Orange
Cyberdefense

Security Navigator

Research-driven insights to build a safer digital society

Hugues Foulon
Executive Director
of Strategy and
Cybersecurity activities
Orange Cyberdefense

Michel Van Den Berghe
Chief Executive Officer
Orange Cyberdefense

In 2019 through our 16 CyberSOCs, we analyzed more than 50 billion security events daily, solved over 35,000 security incidents, and led in excess of 170 incident response missions.
Our world-class experts have digested all this unique information and synthesized our key findings in this report, to the benefit of our clients and of the broader cybersecurity community.

We are very pleased to release the first edition of the Orange Cyberdefense Security Navigator. Thanks to our position as one of the largest telecom operators in the world as Orange, and as the European leader of cybersecurity services as Orange Cyberdefense, we have a unique vision of the threat landscape.

The COVID-19 pandemic has disrupted the physical and digital society and economy on an unprecedented scale. It has fundamentally shifted the way in which we work and do business. A lot of these changes are going to outlast the crisis. Boosted demands for secure cloud services, reliable remote network connections via SSL and videoconferencing – the new home office world is going to stay.

This crisis also proves that digital freedom is not a given. Malicious players increasingly use new and old spaces of connection and progress as opportunities for harm and disruption. Anyone can be a victim on an individual or collective level. This can lead to a breach in digital trust. At Orange Cyberdefense, we believe that the digital world can remain a trusted means of leisure, professional opportunities and services that make everyday life easier, more prosperous and fulfilling.

That's why we strive to create lines of defense and protect freedom in the digital space, not only in crisis, but on our way into the future. Our purpose is to build a safer digital society.

In the past year through our 16 CyberSOCs, we analyzed over 50 billion security events daily, solved in excess 35,000 security incidents, and led more than 170 incident response missions.

Our world-class experts have digested all this unique information and synthesized our key findings in this report, to the benefit of our clients and of the broader cybersecurity community.

We are proud and humbled everyday to be trusted with the security of our clients' most important assets, and are deploying the best expertise and technology in all domains to protect their business.

Thanks for your trust!

Hugues Foulon
Michel Van Den Berghe

Table of contents

2019 Timeline ▸

COVID-19 & Cybersecurity

As the COVID-19 coronavirus pandemic continues to spread worldwide, cyber-threat actors are trying to capitalize on the global health crisis by creating malware or launching attacks with a COVID-19 theme. However, this kind of exploitative behavior by the cybercrime ecosystem is only one part of a bigger cybersecurity picture. Orange Cyberdefense is releasing this information in order to draw attention to a diverse set of facts that should be considered now.

Download the full report on https://orangecyberdefense.com/global/covid-19/

The COVID-19 pandemic has changed security threat models in five important ways:

- Your employees are more vulnerable to social engineering and scams than normal.
- You have less control and visibility over the IT systems you protect than you are used to.
- Your users may be connecting from systems and environments that are fundamentally insecure or poorly configured.
- You may have rushed to implement remote access systems without having the time to plan and execute as well as you would like.
- You, your team and your providers may be operating with diminished capacity.

Effects on the digital world

Some of the tendencies we observed during the lockdown phase:

1. Malware and phishing using COVID-19 as pretext
2. General misinformation/fake news campaigns
3. Some ransomware groups have called a "ceasefire"
4. Targeted attacks aiming at healthcare and research institutions
5. Increased geopolitical tension might spark more cyberwarfare
6. Attacks against remote access technologies and VPN gateways
7. Visibility through SIEM was impaired
8. Computing activity was extensibly moved to the cloud
9. Accelerated move to e-commerce
10. Increased permanent strain on internet infrastructure can lead to degradation

The perfect lure

On March 24 alone, our CERT team in France tracked 23 unique COVID-19-based phishing mails over a 24-hour period. Our CERT team also reported that during the same week, customers reported more than 600 potentially fraudulent emails, 10% of which has proven to be malicious.

Suspected phishing mails reported by customers

The number of confirmed fraudulent emails was 4 times higher than in the previous week.

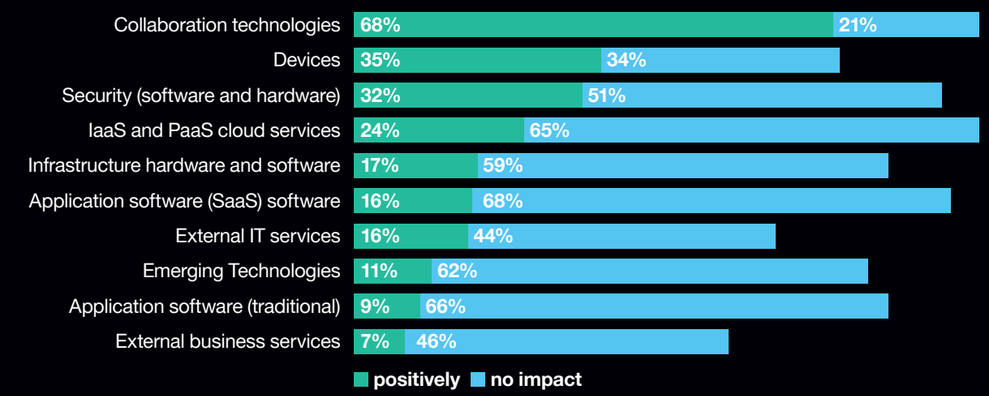
Recommendations summary

During a crisis like COVID-19 we recommend that you focus on the following responses, in order of importance:

- Establish emergency response procedures and systems.
- Establish a security support hotline and prepare to expand the team providing support.
- Review backup and Disaster Recovery (DR).
- Equip your users with the information they need to make good security decisions.
- Provide secure remote access.
- Establish visibility over remote endpoints.

How will COVID-19 change technology?

An IDC survey asked 180 organizations across Europe for the impact of the crisis on technology investment.



https://www.idc.com/getdoc.jsp?containerId=EUR146175020

Lessons learned during the crisis

Advice is cheap in time of crisis. But every business is different, and we won't pretend to know how individual businesses should respond to their particular security threat. We would however offer the following high-level guidelines to businesses who are evaluating the security threat and considering their response to the threat in times of crisis:

1. Understand that we were experiencing a state of heightened threat, but only slightly increased vulnerability. We cannot control the threat, but we can control the vulnerability, so let's focus on that.
2. Understand what has changed and what hasn't. Your business's threat model may be very different today than it was yesterday, but it may also not be. If it hasn't changed, then your strategy and operations don't have to either.
3. Form partnerships but avoid mobs. Your suppliers, service providers and even competitors are all in the same boat, never more so than during crisis. They may not have all the answers either, but it might be time to reach out and find partners that have balanced and rational views and avoid communities that are promulgating hype and hysteria.
4. Maintain context. IT and the internet have survived for twenty years despite our various security failures. There is no doubt that a situation of crisis is worrying, and that the risk of a fundamental cybersecurity crisis is real and can't be ignored. However, this time, the crisis is medical and human. Don't let the hype about cybersecurity distract you from that.
5. Work smart, not hard. You will be able to achieve very little during times of diminished capability, so spend time and energy on considering what your primary concerns are and focus on those.

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Introduction

The state of the threat

“There is too much spending on the wrong things. Security strategies have been driven and sold on fear and compliance issues with spending on perceived rather than genuine threats”.

Art Coviello, RSA Chief Exec (2017)

A war of attrition

Cybersecurity is a problem of resources. Both the attacker and the defender have limited resources in terms of time, money and skill, which they must apply strategically to achieve their objectives.

In a complex and evolving landscape, telling the difference between 'perceived' and 'genuine' threats is very difficult. As Art Coviello points out, this lack of certainty has led to doubt and resulted in too much fear-driven buying. But what are the “genuine” threats? And how do we identify and track them as the threat landscape changes over time?

Allow us to tap into the vast collection of data that we have at our disposal, and the deep skills and experience of our specialists, to help you learn from the past and plan, where possible, for the future.

The state of the threat emerges through the relationship between three primary components – structural forces, inflationary factors and the evolution of technology.

Structural forces

Structural forces include the systemic elements that create enablers and constraints that shape the threat and our ability to respond to it. These factors are woven into our contexts and environments and have a fundamental impact on the shape the threat takes and our ability to respond to that threat.

An example of such structural force is innovation by criminals. It's not the 'cyber' in cyber-crime that is evolving; it's the 'crime'. New ways of monetizing existing attack methods - for example through crypto-mining and ransomware – are changing the nature of the threat at a very rapid rate and thus continually reshaping our threat models.

The key market trends affecting CISOs include:

- Cybersecurity regulation and laws;
- Executive management responsibility vs. Lack of visibility; and
- Market shortage (growth in requirements vs. increasing talent demand).

Nadav Shatz /
Director of Advisory, Consulting and Architecture,
Orange Cyberdefense

Another example is that cyberdefense has become a core business function and senior leaders and boards are much more cyber-aware. But boards, being concerned primarily with regulation, compliance and their fiduciary responsibilities as directors, are also now putting pressure on CISOs to evolve how they work. This distracts the CISOs from understanding and addressing the threat because they are focused instead on understanding and addressing the requirements of the board.

Inflationary factors

As we've noted, the threat landscape we face today emerges first and foremost from a context that is shaped by powerful structural forces. These forces can be military, political, economic, social or legal and they originate at a national or international level.

Once the shape of the threat landscape is initially defined, the challenges we face are amplified by equally powerful and even less controllable 'inflationary factors'. We can picture these inflationary factors as having the effect of blowing air into a balloon.

A major set of inflationary factors are the result of the ambivalence that governments worldwide feel toward fundamentally solving the security problem, and the continued investment by governments in building and using sophisticated hacking tools and techniques to pursue their political objectives. We believe the investment by military forces in computer hacking to be the most significant factor in this area.

As conflicts between nation states in cyberspace inevitably grow in scale and intensity, the key point worth noting is that those conflicts occur on the internet that all of us share. Their impact cannot be restricted to 'government' targets and the rest of us will all inevitably be impacted by these conflicts in one way or another. Think of it as collateral damage.

Eventually government technology, training, skills and experience will find their way into the civilian ecosystem, where it can have a highly disruptive impact, as the WannaCry and notPetya outbreaks clearly illustrated. The scope and scale of government-funded initiatives have the potential to totally subvert everything we hold to be 'true' in our industry.

From a cyberdefense perspective, these powerful geopolitical forces are like the weather. They have an enormous impact on our daily reality. While we can observe these forces and even attempt to predict them, we have no real way of controlling them. Our only choice here is to observe them and orient our own strategies accordingly.

In today's world, not a single military operation proceeds without an implication of cyber defence capacity, either in intelligence, psychological operations, targeting, destruction or post-strike evaluation.

Laurent Célérier / EVP Technology & Marketing,
Orange Cyberdefense

Former senior officer, French Ministry Of Defense

Evolution of technology

It stands to reason that the evolution of technology, along with the new business models and process it enables, would have a meaningful effect on the threat landscape. Both the attacker and the defender are impacted by even the smallest changes to the systems and tools both sides use.

There are some consistent principles that describe how technology evolution affects the state of the threat.

One such principle is that for most businesses, new technologies seldom completely replace old technologies, rather they simply add to them. Therefore, over time, a business becomes burdened with a deep pool of security 'debt' that never goes away, but rather increases. We can assert with confidence that the security challenges we struggled with yesterday will probably still challenge us tomorrow, and that new and evolving technologies will probably not reduce the risk, but only add new threats.

An obvious example of the principle above is the introduction of 5G. The new technology is undoubtedly more secure than its predecessor and promises to be a powerful enabler for next-generation technologies and business opportunities. However, it will undoubtedly also multiply the security debt the technology industry is building up in the rush to develop, market and sell various new forms of technologies. IoT systems are clearly already being plagued by the same security issues that have characterized desktop computers for decades now, but they also bring their own challenges (like remote firmware patching at scale). These problems are massively magnified by the scale of IoT deployments.

From a cyberdefense point of view, however, technology is something we can exert control over. We can choose not to adopt a new technology, and when or how we deploy others to address emerging security threats.

Since these efforts are completely under our control, it makes perfect sense for us to use recognized best practices to do so.

The impact of a new technology is always over-estimated in the short term, and under-estimated in the long term.

We don't know what's going to change, but we can confidently guess what's going to stay the same.

Etienne Greeff / CTO Orange Cyberdefense

Weighing our options

Reflecting again on the three key factors that comprise the emergent threat landscape, we consider how we as cyber defenders can control or influence these forces to our own advantage.

Since there is only one contributing element of the emerging threat landscape that we truly have control over – the technology element – this must clearly be our immediate short-term focus. This effectively requires the smart deployment of technology, people and best practice processes to counter threats and reduce risk.

While our efforts at the technology level are clearly necessary the three elements unfortunately do not all have equal impact on the emergent state of the threat.

The emerging threat landscape is influenced more by the factors we don't control, than by the factors we do control. This suggests that, while it's imperative we continue to improve our technology, people and processes, we also need to accept and anticipate that this alone will not be enough to achieve the level of resilience we desire in the face of current and 'genuine' threats.

Structural forces
Systemic forces that create the enablers and constraints that shape the threat and our response

Influence
We cannot control these factors, but influence them. Influencing the landscape is the most far-reaching way of adressing threats in the long run.

Inflationary forces
the threat emerges out of a political, economic, social, legal & regulatory context

Observe and orient
These forces are like weather: they have an enormous impact but we cannot control them. Our only choice is to observe and adjust accordingly.

Evolution of technology
As technology changes so does the threat

Control
We can reduce the size of our attack surface, find and mitigate vulnerabilities. These efforts are under our control, so it makes sense to do so.

> Bad guys will continue to innovate. We need to accept that there will be breaches and think about detection and response.
>
> Stefan Lager / SVP Global Service Lines, Orange Cyberdefense Nordics

A crisis of compromise

One could argue that the role of security within technology is to create and assert trust. The three pillars of the 'CIA Triad' – confidentiality, integrity and availability – define for us how this should be done: by ensuring the that the data and systems we use can be trusted to keep secrets, ensure accuracy and be available when we need them. When security fails, trust is compromised. Once trust is lost it's very difficult to regain. Indeed, so important is trust to the systems our businesses, societies and very lives depend on, that to sacrifice trust in a key technology would be nothing short of a crisis.

The lesson for those of in technology here is simple and clear: our stakeholders need to be able to trust the systems and data we're responsible for.

When attacks, breaches and compromise happen, that trust is damaged, and the consequences are far-reaching. In a complex system with multiple factors we don't control, we can't prevent crises from emerging. We can nip them in the bud, however, and to do that we need to have good visibility, early detection, and clear and confident response capabilities. Beyond preserving trust, we need to focus on restoring trust when bad things happen. Detection, response and recovery play an essential role.

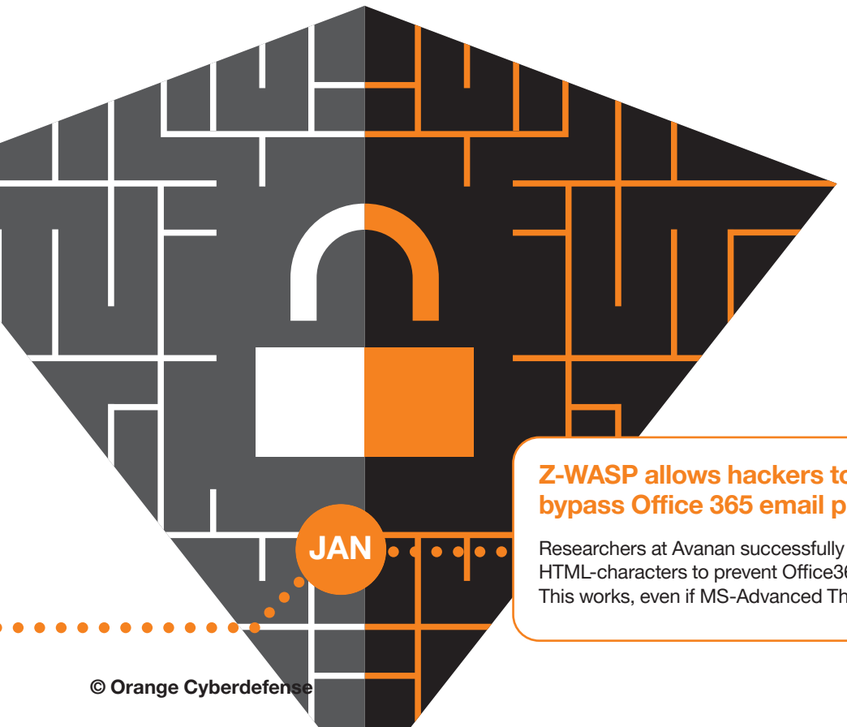
Balancing the scales – detect, respond, recover

Our paradigms clearly need to change, and Dominic White, CTO of Orange Cyberdefense's elite attack and penetration testing unit, offers some insight into where we need to go.

> If they detect us, they burn us, and that has consequences. Attackers also have a boss and a budget.
>
> Dominic White / CEO, SensePost

This insight from a team of seasoned attackers illustrates that while the various preventative controls we implement may impose a cost on the attacker, effective detection and response by an elite attack and penetration testing unit has the effect of truly setting them back. It is from this lesson that our beliefs on 'engagement' emerge: The adversary can no longer be held back at the gates.

We need to anticipate the adversary being active behind our perimeters, and on our systems. We must find them there and counter them there, often system by system, until they are driven out. Like all prior security doctrines before it, "Detect, Respond & Recover" is not a silver bullet. It cannot be deployed in isolation and it will not overcome the systemic structural and inflationary forces we face. It is, however, a necessary tactical response in a contemporary reality that still overwhelmingly favours the attacker.



Z-WASP allows hackers to bypass Office 365 email protection

Researchers at Avanan successfully used non-printable zero-width HTML-characters to prevent Office365 from recognizing malicious links. This works, even if MS-Advanced Threat Protection (ATP) is enabled[t1].

Conclusion

What becomes clear from considering the emerging state of the threat is that businesses, no matter how large or small, are going to find themselves in a state of constant conflict with adversaries that are buoyed by large, systemic factors and forces over which we have very little control. These factors and forces collectively outweigh all the resources we as defenders can hope to bring to bear.

The COVID-19 lockdown with its impact on global business is a perfect example of such an uncontrollable factor. It is clearly having an impact on the focus and attack schemes of threat actors, both positive (some hacking groups have declared a ceasefire) and negative (increased pressure on healthcare institutions and massive attempts to profit from the COVID-topic for phishing and fraud).

Without neglecting the basic security best practice required to counterbalance these threats (without which they would simply overwhelm us), we must recognize that attacks, compromises and breaches are inevitable and prepare to engage our adversary in an active and continuous manner behind the traditional perimeters of our environments.

Not only are mature and effective detection and response capabilities an existential requirement in light of contemporary threats, effect detection and response programs also help us to counter-attack some of the very advantages that give our adversaries a systemic advantage, namely by minimizing their element of surprise, inflicting real costs and consequence for their mistakes, and extending the time they require to learn and improve, while simultaneously reducing the time for us to do the same.

Most importantly however, effective detection, response and recovery are vital to restoring trust when the inevitable compromise happens.

The threat is evolving, attack is inevitable, engagement is essential.

Hacktivist sentenced to 10 years for DDoSing hospital

Martin Gottesfeld had attacked the Boston Children's Hospital and another institution in 2014 via a botnet of 40,000 routers, allegedly to protest the abusive treatment of Justina Pelletier[t2].

The Fondation du Patrimoine and the Notre-Dame fire

After the roofs of the Notre-Dame de Paris Cathedral burned down on 15th of April 2019, the Fondation du Patrimoine faced another crisis. Empowered by the State to collect solidarity funds for the reconstruction of the edifice, this entity was quickly overwhelmed by a problem it had not anticipated: the proliferation of fraudulent fundraising and the registration of parasitic domain names.

"Many sites were trying to pass themselves off as legitimate collections, and the Heritage Foundation site was offline for two hours [...] It was of a rare magnitude, I'd never seen anything like it. The foundation was not ready to face such a situation."

Jean-Michel Livowski, DPO, Fondation du Patrimoine

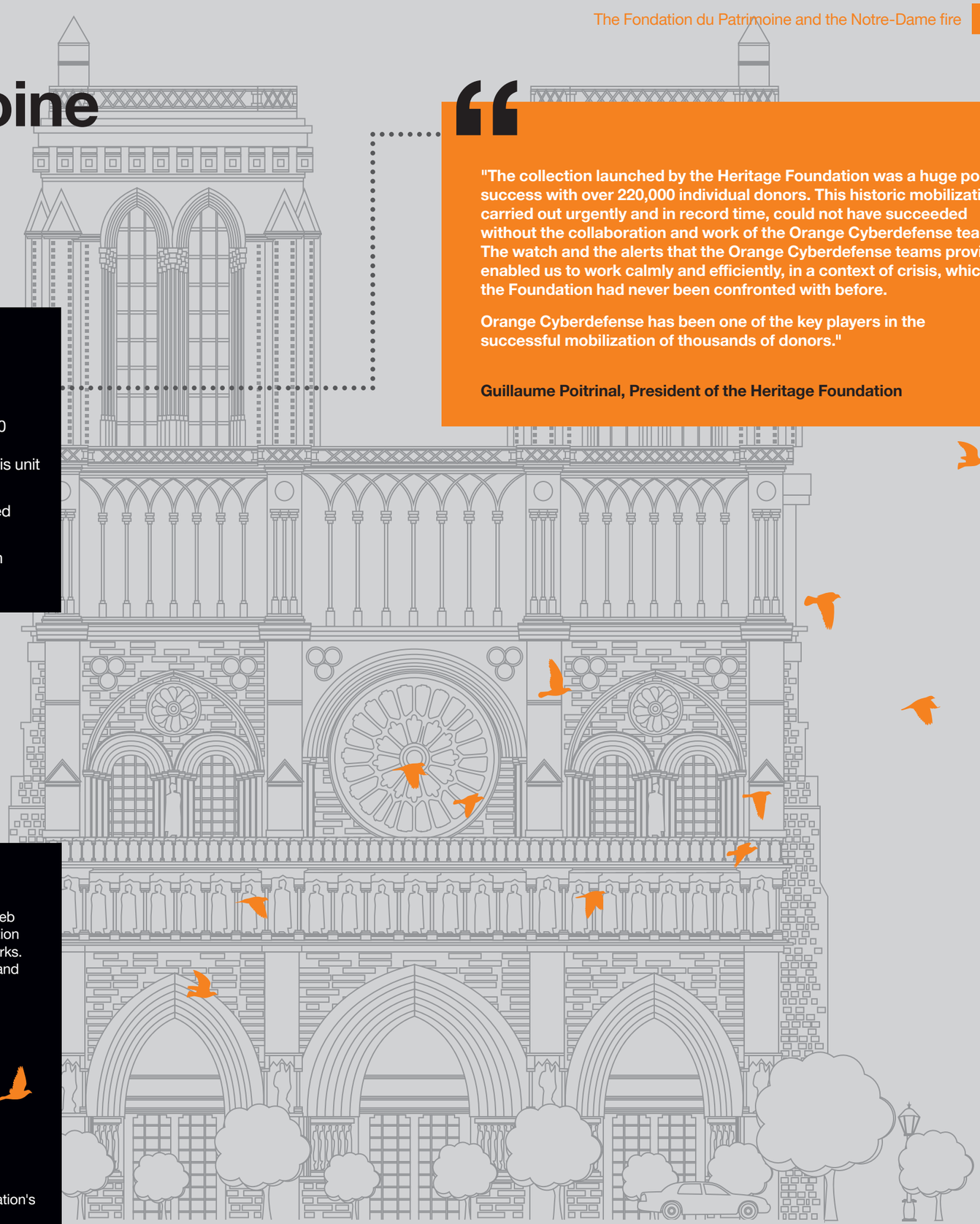
Crisis management key figures:

- Nearly 50 days of surveillance
- Approximately 20,000 items of information passed on to the crisis unit
- Nearly 400 identified parallel pools reported to authorities
- More than 20 domain names under watch

"The collection launched by the Heritage Foundation was a huge popular success with over 220,000 individual donors. This historic mobilization, carried out urgently and in record time, could not have succeeded without the collaboration and work of the Orange Cyberdefense teams. The watch and the alerts that the Orange Cyberdefense teams provided enabled us to work calmly and efficiently, in a context of crisis, which the Foundation had never been confronted with before.

Orange Cyberdefense has been one of the key players in the successful mobilization of thousands of donors."

Guillaume Poitrinal, President of the Heritage Foundation



Concerned about the situation and a possible intensification of attacks due to the upcoming Easter weekend, the press contacted Orange Cyberdefense on the evening of April 19th, the eve of a long weekend that would help malicious actors. Orange Cyberdefense's Incident Response Team (CSIRT) and Alerts Center (CERT) teams decide to deploy a crisis management system without delay.

Crisis management in record time

As donations flow in, the first actions are taken by the Heritage Foundation, including the creation of an official web page dedicated to donations, supported by a communication campaign taken up by the various media and social networks. This one, as well as the websites of Notre-Dame de Paris and the Fondation du Patrimoine are under observation by Orange Cyberdefense analysts.

In addition to this first safety measure, there is also a monitoring system for:

- domain names
- mobile applications
- profiles on social networks
- the official fundraising on the specialized platforms

A crisis unit sends alerts in real time to the Heritage Foundation's managers, lawyers and judicial authorities via an extranet.

Sara Puigvert
EVP Global Operations
Orange Cyberdefense

Franz Härtl
Head of Global Content Marketing
Orange Cyberdefense

CyberSOC statistics

This is what happened

Protecting IT assets, systems and infrastructure in order to safely enable business is our daily bread. As we monitor security devices, endpoints, cloud applications, operational technology (OT) environments and networks for our customers worldwide, we see a lot of what ends up on the news with our own eyes.

A continuous stream of data passes through our 10 CyberSOCs and 16 SOCs. As we have done in our previous Annual Security Reports, we decided to delve into this data and extrapolate the figures to get a better understanding of the ever-evolving threat landscape.

So as part of the new Security Navigator, we can again share with you a very real, first-hand picture of the events and trends over the past year.

This data was collected before COVID-19 began to affect both the business- and threat-landscape and as such can serve as an important baseline for comparison with future data.

About the data

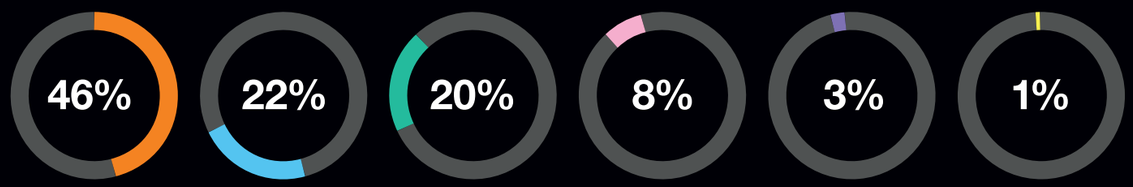
- **Grand total of events analyzed: 263,109**
- **Out of these events, 11.17% (29,391) are considered security incidents by Orange Cyberdefense* data classifications.**
- **Period analyzed: complete data for the entire year of 2019.**
- **Data sources: firewalls , directory services, proxy, endpoint, EDR, IPS, DNS, DHCP, SIEM and our managed threat detection platform.**

*includes alerts from part of our operational scope for this special edition

Funnel:
Alert to incident

263,109
Alerts • Use Cases • Events

29,391
11.17% Security Incidents



Types of incidents

In 2019, we detected the following incident types:

Network & Application Anomalies, such as tunneling, IDS/IPS alerts and other attacks related to network traffic and applications.

Account Anomalies, such as brute force attacks, reusing credentials, lateral movement, elevation of privileges or similar kinds of incidents.

Malware is malicious software such as ransomware.

System Anomalies are events directly related to the OS and the components around it like drivers that stop working or services that are terminated unexpectedly.

Policy Violations, such as installing unsupported software or connecting an unauthorized device to the network.

Social Engineering is any attempt to fool users; including, but not limited to, phishing and spoofing.

Totals

In comparison to our previous report, we recorded an increase of alerts. We had more onboardings this year, so this discrepancy was expected. Having said that, it is noteworthy that the number of events we identified as security relevant has increased more than predicted.

Among the 263,109 events in total, we identified 11.17% (29,391) as verified security incidents. In the previous year, this rate was 8.31%, which means we saw an increase of 34.4%. This is quite significant considering that the total number of alerts grew by less than 3%.

This change in ratio can partly be explained by better finetuning of the platform to avoid false positives in collaboration with our customers. Still it is a fact that the number of security incidents grew significantly. Attackers will take any opportunity to exploit a weakness.

Have you been pwned?

Another trend we consider significant is the increase of Account Anomalies. In the previous report 15% of our incidents were classified as account anomalies and it was ranked in third place. This year, it has jumped up to second place at 22%. What happened?

A possible explanation could be the unusual frequency and sheer magnitude of this year's data leaks. As you can find in several items of the 2019 timeline, literally hundreds of millions of accounts and credentials have been breached and sold on the darknet. Adding the fact that people tend to reuse passwords, especially when they have to be renewed every 100 days, it is obvious that we run into problems here.

The keyphrase is 'credential stuffing'. And, this increase may just be the tip of the iceberg, as even criminals need some time to process and abuse data on that scale. You can read more on Data breaches, their causes and impact in the chapter "Databreaches on the rise".

Social engineering remains hard to detect

Social engineering statistics are tricky. Social engineering encompasses all sorts of activities which usually precede the actual attack. It starts with researching target account owners or key management roles in different social media like LinkedIn or Facebook. For instance, targets could be manipulated to reveal details of operating systems, network setups or even credentials via fake phone calls from fake-service employees.

All of this can happen outside of the company perimeter and as such is outside of our direct tracking capabilities. Targeted threat intelligence can in some cases help identify such occurrences but generally we only see the results.

Damage resulting from social engineering might still be prevented, depending upon the nature and sophistication of the real attack. However, related incidents are likely counted into their respective categories like account anomalies or malware, even though they are an immediate effect of social engineering.

Critical Vulnerability in "Amadeus" online booking platform fixed: almost half of all airlines worldwide affected

Just by injecting some simple commands into the browser it was possible to get the passenger name records and following that, flight details, names and other personal info[13].

Endpoint protection works

Another noteworthy change we observed is that malware incidents declined significantly. Previously we had classified 45% of the incidents to be malware-related. During 2019 this dropped to 22%. During the same period Network & Application Anomalies increased from 36% to 46%, making it the new top incident category in 2019.

Does that mean malware is not a threat anymore? Generally it doesn't, but it shows that endpoint-centered prevention can significantly reduce the risk. What we see here is very likely the immediate result of next-generation endpoint protection.

While AI-based solutions have been around for a while now, their widespread application has taken some time. Now, more and more customers have started investing in next-generation preventive endpoint protection. And we see the results quite clearly: malware rapidly loses its teeth as a threat, moving down in ranks to third place, after account anomalies.

While elaborate malware and APTs used in targeted attacks still do pose a serious threat, the skill level of the common cybercriminal does not match up-to-date endpoint protection anymore. And that is good news.

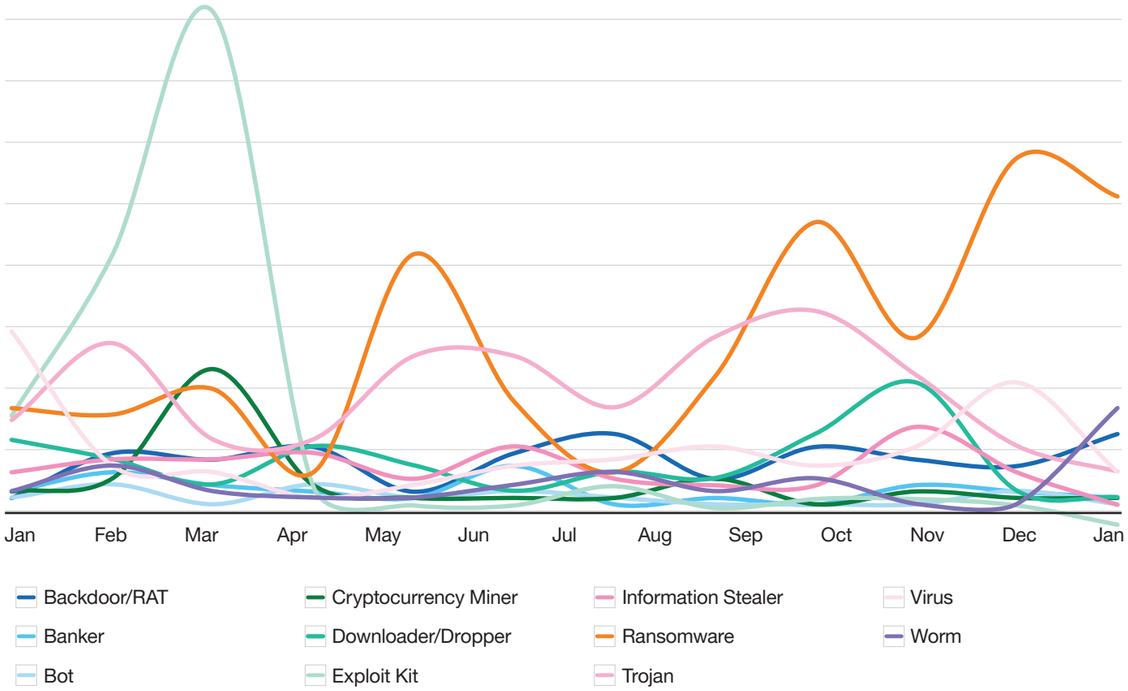
Malware trends

When looking at overall malware trends, we notice some striking patterns.

The first two notable tendencies are the drops in attack activities during the beginning of April, mid-July and early December. These are likely due to a trend we already observed in previous years: with cybercriminals getting more professional we see them adopting a nine-to-five-mentality. As odd as this seems: hackers now take regular holidays. This may explain the drop in April, when attacks slowed due to an early Easter holiday, as well as summer vacation and Christmas at the end of the year.

Ransomware had its highs and lows, but remains a popular attack. For mining attacks it's different. While both attack types showed a rise at the beginning of the year, mining attacks dropped and stayed low from April onwards. Ransomware dropped in April as well, but rose to new peaks in May, October and December. It is also remarkable that Monero[2.1], Ethereum[2.2], Litecoin[2.3] and Bitcoin[2.4] prices reached a new peak in early summer, but there was next to no effect on the frequency of mining attacks, while we had previously seen mining directly following the trade value of cryptocurrencies. This indicates that Cryptomining as a threat is gone for good and likely will not return in widespread campaigns.

Malware Trends overview



„Collection #1“: 773 million records found on the darknet

Australian researcher Troy Hunt discovered a massive collection of credential records (email ad-dresses & passwords). The records originate from several different data breaches[t4].

Altran Technologies hit by cyber attack that affected operations in several European countries

The French engineering consulting firm was apparently struck by a targeted campaign that hit operations in several European countries[t5].

GandCrab/Ursnif

Beware of Word macros: Ursnif is a trojan set to exfiltrate critical data, while GandCrab is a classic ransomware. Both spread via phishing emails with malicious Word attachments[t6].

European joint multinational Airbus under attack

Airbus and its suppliers have been hit by a whole series of attacks aiming to steal intellectual property[t7].

FEB

$145 million gone after CEO dies with only password

QuadrigaCX , the largest bitcoin exchange in Canada, claims to have lost access to its offline storage wallets, as the only person with access to these was CEO and founder Gerry Cotton who had unexpectedly died in December[t8].

E-Scooter password override allows life-threatening hacks

Electric Scooter M365 by Xiaomi comes with an apparently vulnerable Bluetooth app. As the scooter does not validate the password, attackers can apply the brakes, accelerate or shut down the scooter from up to 100m away[t9].

Secure email provider VFEmail.net wiped

In a catastrophic security breach hackers completely destroyed all data on both primary and the backup servers. This included the entire infrastructure with email hosts, virtual machine hosts and an SQL server cluster. This was purely destructive, there has been no ransom demand[t10].

Hacker sells 839 million accounts in the darknet

Hacker “Gnosticplayers” published three rounds of accounts from dozens of hacked websites and services on Dream Market adding up to 839 million credential sets. Many of the sites did not even know they had been breached[t11].

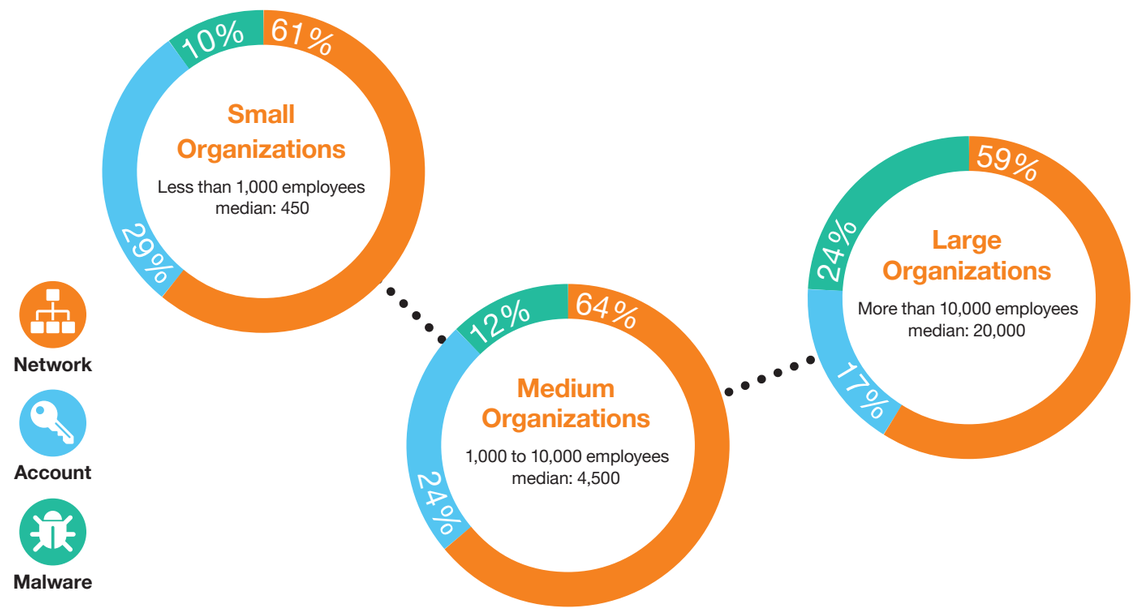
Organization size

The big picture has changed somewhat. Considering previous numbers the smallest change was that 9.72% of the incidents were tracked in small businesses. That’s a minor increase from last report's 8%.

A significant shift has occurred when it comes to medium and large organizations. Last year we found big players were the ones hit the most by far. Generally, it is still true that most incidents occur in companies with more than 10,000 employees.

But what we also saw this time is a dramatic rise in attacks on medium-sized businesses. In 2019, we tracked 31% of all recorded incidents here, which is a significant increase from the previous 19%. At the same time, incidents in large organizations declined from 73% to 58.8%.

Apparently threat actors have partly shifted their focus, now targeting medium-sized businesses with 1,000-10,000 employees much more than previously observed.



Types of incidents versus business size

We see the same tendency as in the averages of the funnel on page 16. The major change in comparison to the previous report can be observed in large organizations, who had to deal with extensive amounts of malware last year. This year, all business sizes had network & application anomalies as the top-ranked incident type.

Two factors stick out, though: small organizations suffer much more from Account Anomalies (29% as compared to 24% for medium/17% for large) and large ones still have to fend off more than twice as many malware attacks as smaller ones.

On average, the incident count per head in small businesses is about fourteen times higher than in large organizations. This is confirming a trend we observed in previous reports. In our last update report we found this factor to be six times higher. With the factor doubling for 2019, we see this tendency rapidly picking up speed.

Incidents

Per 100 employees

For organizations with under 1,000 employees, we once again observed a sharp increase in the incident ratio. On average, the incident count per head is about fourteen times higher than in large organizations.

By now, almost one person in three working in a smaller organization is directly affected by a cyber threat.

Small Organizations	Medium Organizations	Large Organizations
29.5	6.4	2.1

Criticality

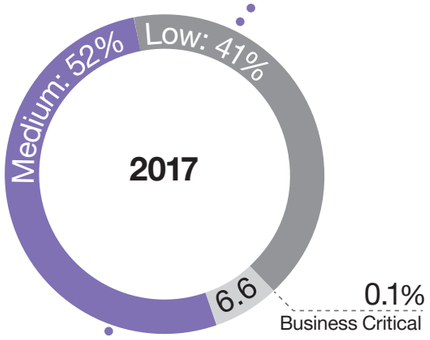
Incidents are not equal. At Orange Cyberdefense, we have defined four levels:

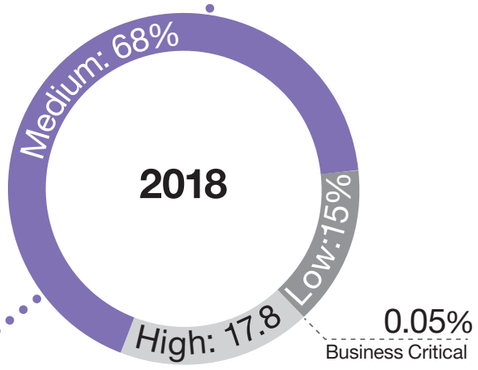
- **Business critical:** Critical business impact, business processes grinding to a halt
- **High:** Significant business impact, incidents that must be handled immediately
- **Medium:** Limited business impact, acceptable workarounds may exist
- **Low:** Minimal business impact, does not significantly impact operations

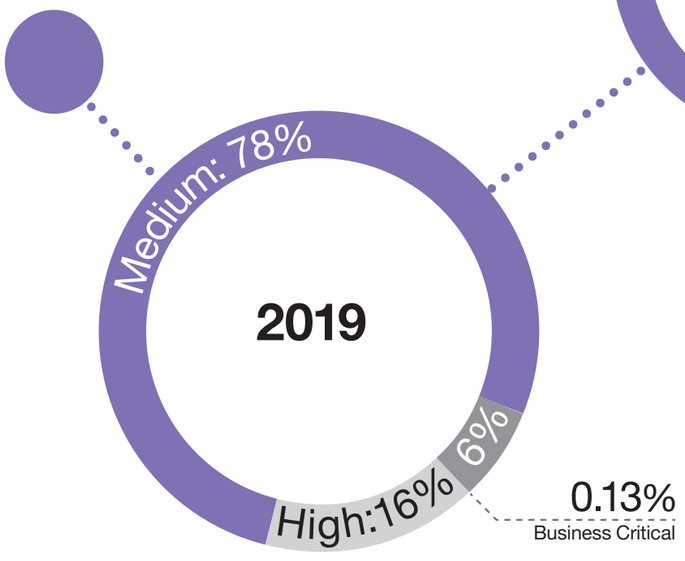
	Business Critical	High	Medium	Low
2016	0.50%	8.2%	53%	38%
2017	0.10%	6.6%	52%	41%
2018	0.05%	17.8%	68%	15%
2019	0.11%	16%	76%	7%

In 2019 we see two trends continue from the previous two years: incidents ranked medium again gained almost 10% as compared to last year. Meanwhile, incidents with low criticality have about halved, indicating again that the "base noise" of uninspired mass attacks is rapidly losing ground to an increasing level of baseline security.

Attacks classified as high have remained stagnant at 16.04%. From 2017 to 2018, high impact attacks tripled, so it's a relief that that didn't occur again. What leaves an uneasy feeling however, is that the number of attacks deemed business critical, while not being dramatically high at 0.11%, has nonetheless doubled compared to 2018. This is comparable to the status of 2017.







Operation "Sharpshooter" linked to North Korea

The global espionage campaign was aiming at critical infrastructure like government institutions, power stations and financial organizations. Potential false flags made attribution difficult, but now researchers at McAfee officially credited the campaign to the North Korean state sponsored Lazarus group[t12].

Mozilla introduces Firefox Send, a free encrypted file transfer service

It allows users to upload files of up to 1GB (up to 2.5 GB for registered users) and share the download link[t13].

MAR

Round 4 — Hacker puts 26 million new accounts up for sale on dark web

"Gnosticplayers" strikes again: 26 million new records on sale[t14].

Mirai is back

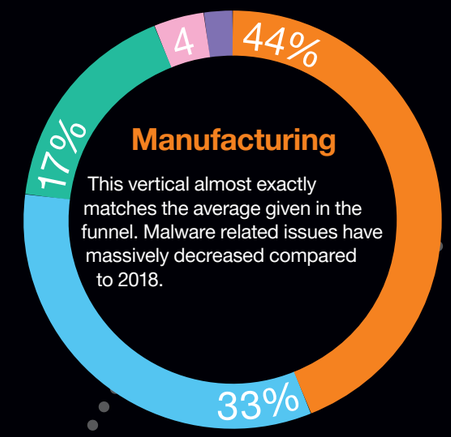
IoT-botnet Mirai resurfaced as "Enterprise Edition", now aiming specifically at turning corporate smart devices like wireless presentation systems and routers into DDoS bots[t15].

Incidents in different verticals

How are the incidents distributed within different verticals? We analyzed seven industries and were surprised by the differences we spotted.

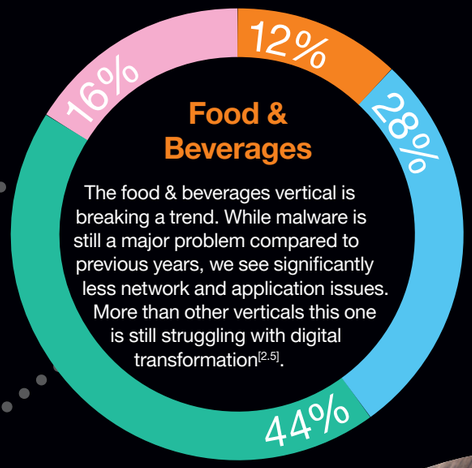
Higher percentages in these graphs do not just mean that incidents are occurring more frequently, and that the industry is more 'vulnerable'. In fact, they can indicate quite the opposite. The ability to identify an incident may indicate a high security maturity. For example, in finance there are high volumes of social engineering for fraudulent purposes because financial organizations are more mature in dealing with these incidents and are able to detect and report more of them.

	Network	Account	Malware	System	Policy	Social
Professional Services	59.93%	22.68%	10.85%	5.50%	0.94%	0.10%
Financial Services	45.06%	26.48%	11.76%	6.19%	0.11%	10.41%
Manufacturing	44.38%	32.63%	16.94%	4.39%	1.63%	0.03%
Food & Beverages	12.13%	27.62%	43.51%	16.32%	0.00%	0.42%
Government&Public	49.17%	41.72%	5.30%	1.16%	2.65%	0.00%
Healthcare	83.19%	5.75%	9.02%	1.84%	0.03%	0.19%
Education	39.25%	57.01%	0.47%	0.00%	2.80%	0.47%
Biotechnology	42.37%	49.57%	4.76%	3.30%	0.00%	0.00%
Retail	34.33%	18.49%	27.84%	12.11%	5.77%	1.46%



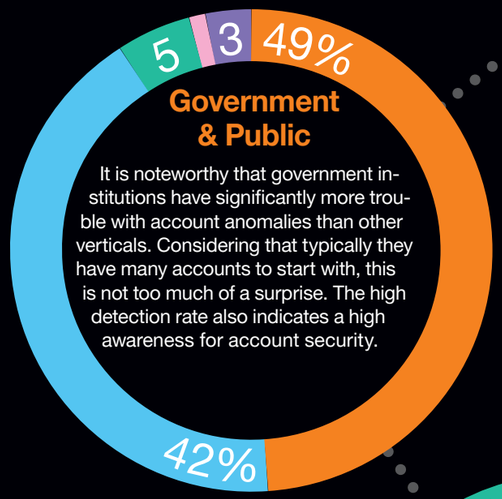
Manufacturing

This vertical almost exactly matches the average given in the funnel. Malware related issues have massively decreased compared to 2018.



Food & Beverages

The food & beverages vertical is breaking a trend. While malware is still a major problem compared to previous years, we see significantly less network and application issues. More than other verticals this one is still struggling with digital transformation[2.5].

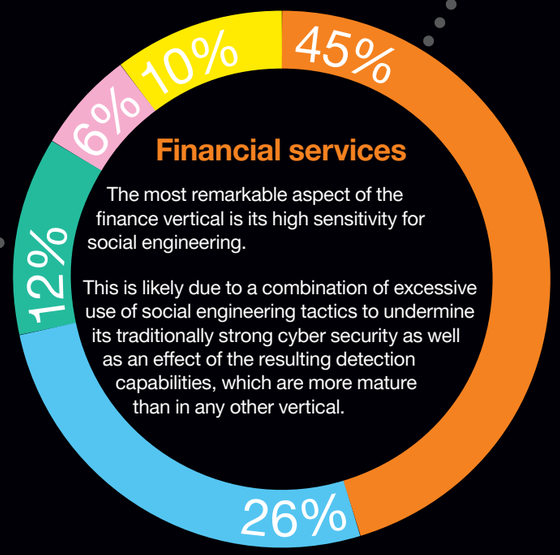


Government & Public

It is noteworthy that government institutions have significantly more trouble with account anomalies than other verticals. Considering that typically they have many accounts to start with, this is not too much of a surprise. The high detection rate also indicates a high awareness for account security.

Professional services

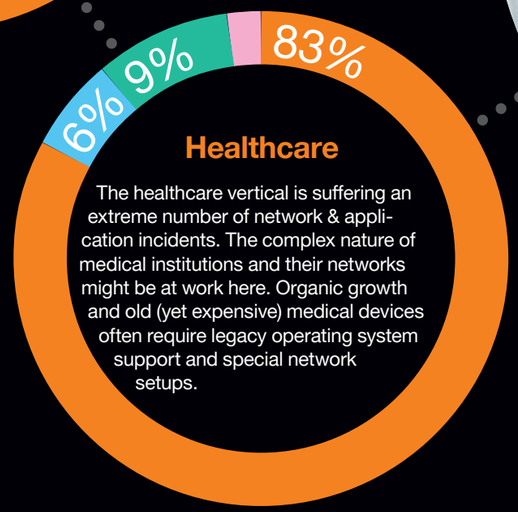
We find this vertical closely matches the profile observed for organizations with up to 1,000 employees.



Financial services

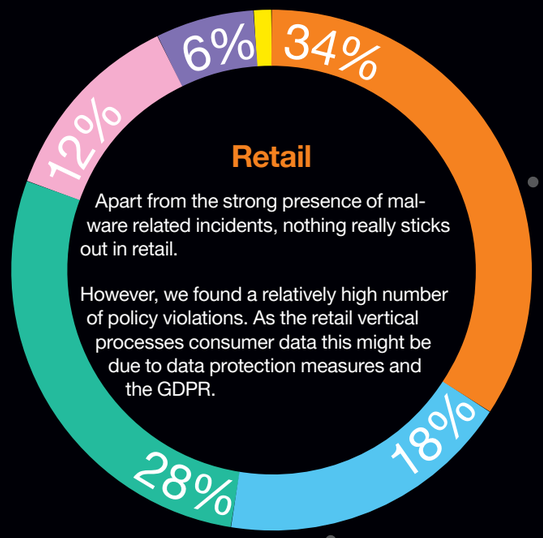
The most remarkable aspect of the finance vertical is its high sensitivity for social engineering.

This is likely due to a combination of excessive use of social engineering tactics to undermine its traditionally strong cyber security as well as an effect of the resulting detection capabilities, which are more mature than in any other vertical.



Healthcare

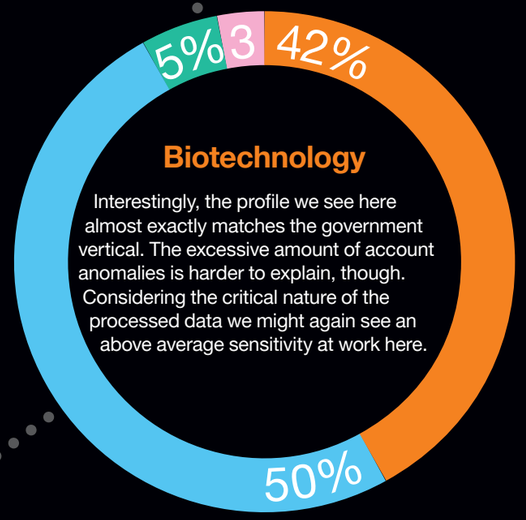
The healthcare vertical is suffering an extreme number of network & application incidents. The complex nature of medical institutions and their networks might be at work here. Organic growth and old (yet expensive) medical devices often require legacy operating system support and special network setups.



Retail

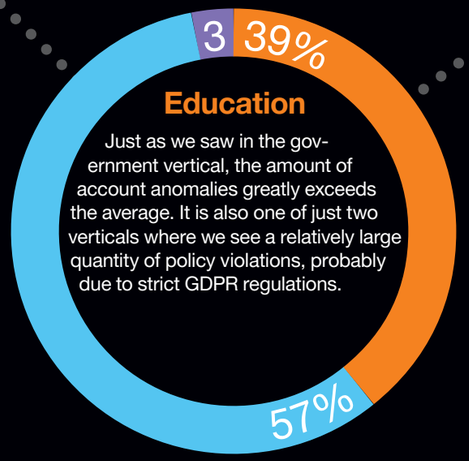
Apart from the strong presence of malware related incidents, nothing really sticks out in retail.

However, we found a relatively high number of policy violations. As the retail vertical processes consumer data this might be due to data protection measures and the GDPR.



Biotechnology

Interestingly, the profile we see here almost exactly matches the government vertical. The excessive amount of account anomalies is harder to explain, though. Considering the critical nature of the processed data we might again see an above average sensitivity at work here.



Education

Just as we saw in the government vertical, the amount of account anomalies greatly exceeds the average. It is also one of just two verticals where we see a relatively large quantity of policy violations, probably due to strict GDPR regulations.

Conclusion

The tension has increased. Considering the relation between total alerts and security-relevant incidents we see a tendency for the worse. This change is partly due to the ongoing work invested in the fine-tuning of alerts (eliminating false positives), but it also shows that threat actors are still on our heels.

In the previous report, the major source of incidents was malware, accounting for almost half of the attacks we had detected in our CyberSOCs. This year, network-related incidents take the crown.

The reduction of malware has been achieved thanks to the implementation of the newest generation of endpoint protection by many of our customers.

Nonetheless, account anomalies and malwares should not be underestimated. They remain relevant potential threats with significant impact to the victims when they hit. Endpoint detection and response could help reducing the risk further, as from a certain point, detection yields better (and more cost-efficient) results than over-spending on prevention alone. Additionally, Network Traffic Detect and Respond technologies thoroughly complement endpoint and SIEM-based detection coverage.

A considerable shift of attacks that target small and medium-sized organizations clearly indicates that the midmarket would best increase their sensibility to cybersecurity threats.

This investment is not limited to technology: having access to experts with the right skills is essential. And in a market where cyber expertise is scarce – up to 2.9 million vacancies are open today according to non-profit ISC2 – managed detection and response is ever more compelling as an answer. Large enterprises and multinationals were the early adopters, we expect to see mid-size enterprise interest picking up rapidly as well.

It will be very interesting to review how figures have changed due to the massive impact of the COVID-19 crisis in the next Security Navigator in December. Both the exceptional move towards home office during the lockdown phase and the changed attack patterns within the community of threat actors could have a significant effect.

Norsk Hydro shuts down global network due to ransomware attack

Several plants in different countries had to be shut down or emergency operated in manual mode due to an infection with LockerGoga spreading from the US sites[t16].

Implanted defibrillators vulnerable to hacking

The devices manufactured by Medtronic operate on a proprietary radio-based connection protocol whose implementation is fundamentally flawed: it does not include any encryption, checks for authentication or data validation[t17].

APR

Bithumb hacked (again): $19 million stolen

3 million EOS and 20 million XRP were stolen from compromised wallets. Just last year Bithumb had already lost $32 million worth of EOS which were stolen from many of its users wallets[t18].

540 Million Facebook user records found on unprotected Amazon servers

Mexican media company Cultura Colectiva had gathered 146GB of data containing comments, likes, account names and user IDs from Facebook and left them on public access on AWS servers. Apparently Facebook has already lost control of its data on millions of users to third parties[t19].

TajMahal: New APT Framework discovered

TajMahal is a toolkit containing an astonishing set of 80 modules and contains tricks “never seen before”. It has apparently existed for at least five years, but has never been detected until now[t21].

French government chat “Tchap” hacked

Due to improper validation of allowed email addresses, French security researcher Elliot Alderson could log into the app which should have been restricted to government officials[t22].

Electrum Wallet Infection rapidly spreads, steals $4.6 million

In nature the attack was a group of hacked servers pretending to be part of the Electrum peer network. These responded with a falsified error message to legitimate requests, tricking Elektrum Wallet apps to download a malicious update which then stole wallet funds and additionally contained a botnet infection which was used to DDoS legitimate Electrum servers[t23].

MAY

Fleury Michon stopped production for five days due to a computer virus

11 production sites as well as the logistics unit were shut down. Management claims that the costs of the outage are covered by a cyber insurance. [t24].

Mysterious database found containing data on 80 million US citizens

Known hacktivists Noam Rotem and Ran Locar discovered an unprotected database containing information on up to 65% of US households hosted by a Microsoft cloud server. It is yet unknown who owns this database or what purpose it serves[t25].

City of Baltimore shut down by ransomware

While emergency lines like 911 stayed unaffected, most civil services like the departments for public works, finance and transportation suffered outages of email and telephone lines[t27].

Europol shuts down Wall Street Market and Silkkitie (aka Valhalla)

International law enforcement took down two infamous darknet marketplaces. Wall Street Market used to be the second biggest worldwide with some 5400 vendors and millions of users trading goods like drugs, stolen data, hacking services and malware code[t26].

Aéroports de Lyon’s website targeted by a cyber attack

Customers booking services such as parking lots and lounges at the airport homepage found themselves redirected to a phishing site trying to steal their credentials and data[t28].

Paul van der Haas
Lead Engineer Operations SLI
Orange Cyberdefense

Thomas Eeles
CSIRT Manager
Orange Cyberdefense

Pentesting & CSIRT stories

Tales from the low-level

Once upon a penetration test

Over time, penetration testers have acquired a certain reputation and a very special set of skills. These skills are not too dissimilar from the bad guys which organizations are so desperate to keep at bay; albeit we are trusted to disclose our findings in a responsible manner. But we do drink coffee, lots of it, and enjoy doughnuts. The ones with sprinkles!

Reputation equals trust. Customers get to know us, they admire our skills and establish trust with us, and they invite us to identify weaknesses and often exploit them. What better way to demonstrate true cyber risk?

Our reputation precedes us. Our own sales team would often boast of our abilities: regaling about the brief time it would take to compromise a domain administrator account, and all before the first coffee was finished and the customer had returned with the sprinkled doughnuts.

Times have changed, stories like this are committed to cyber history. Fables will soon include such tales, and our children's bedtime stories will popularize the penetration testers of old.

So grab the marshmallows and follow us to the low-level of security!

Story 1: De-faulty security

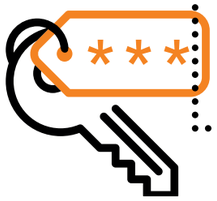
A new assignment arrived from a customer, one with specific objectives: identify vulnerabilities on the internal network and proceed to exploitation and penetration further into the network. A typical assignment but permission was granted to exploit and explore; something we do well.

Coffee arrived and so did the doughnuts, and we set about discovering the customers network with scanning software.

1 Scan

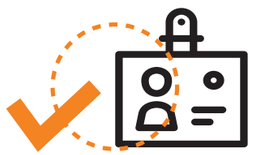
The coffee was still warm, the scans were still running, and a member of our team declared he'd already discovered a web application that looked like an administration portal for the customer's Active Directory.

Reminiscing about times gone by, surely it couldn't be possible to log in with admin/admin, right?



2 Login with default credentials

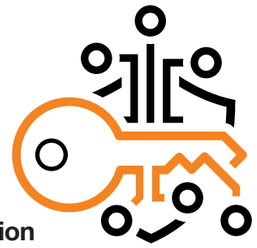
Finish your coffee, pack the laptop away, there is a new domain admin in the house!



3 Gaining privileged access

As you might have guessed, it was possible to log in with these credentials. The application was using an account with privileged access to the customer's Active Directory.

Designed to make administration of the domain easier; allowing helpdesk admins to manage user accounts.



4 Obfuscation is not security

With good intentions, the customer had configured the domain administrator account to achieve this. The application was hiding the password of the account with basic obfuscation, but only in the client side.

5 Exploiting the weakness

Exploiting the client-side weakness, it was possible to change the password field to show the password in plaintext, in essence revealing to the penetration tester the domain administrator credentials.

6 Full compromise

With slightly more than half of a doughnut still to eat, he had revealed the most privileged account in IT.

The flag was captured, the finish line had been crossed, anything the customer had considered secure was now considered compromised.

JUN

GoldBrute targets 1.5 million RDP servers

The ongoing botnet campaign aims to brute force logins at open Windows RDP servers. To avoid detection each bot only sends one credential set to lots of different servers so each request originates from a different IP[t29].

Lessons learned

Although this penetration chapter is only a brief extract of the customer's IT story, many lessons can certainly be learned. What really went wrong for this customer? Was it the default credentials, or was the application failing to sufficiently protect the Domain Administrator credentials?

We need to go back a little further to understand. Information security acknowledges that security controls will fail, therefore reliance upon a single control is simply not effective. Following the story from the beginning you will notice weak or even absent controls, starting with:

- **Network Access Controls (NAC):** the testers were able to connect to the network without any challenge. NAC could have made the penetration tester work harder to simply connect to the network and its services.
- **Principle of Least Privilege:** overly permissive credentials. The Domain Administrator account has one purpose: to manage the domain (from the domain controller). Access to this account should be extremely limited.
- **Segmentation and filtering:** the application found was used for managing user accounts. There was no reason for a non-administrative device to be accessing the application. Functional segmentation should be in place and filter allowed access to the application. Always keep the least privilege principle in mind!
- **Default credentials:** Always change system and application default credentials. Default credentials are deliberately weak and often publicly known. Policies and procedures should be established that require default credentials to be changed.

CSIRT stories

This year has seen the CSIRT at Orange Cyberdefense handle unprecedented levels of cyber security incidents. A steady flow of Microsoft Office 365 email hacks have been abused in large-scale ransomware attacks. None of them have been "nation-state attacks", and the majority have not been what we would classify as overly sophisticated. However, they were all causing severe damage before we were called in. This section will look at a tiny selection of some of the mistakes that we have seen in 2019 and the damage they have caused.

Story 2: The million euro flat network breach

This is the stuff of IT nightmares. The fable as old as IT: "no one will hack us, we don't have anything worth stealing". So why bother doing the most basic of industry best practices?

That is exactly what we found. A totally flat network, with no backups, over 30 domain admin accounts, and no centralized logging.

1 Word macro from hell

The latter meant that when someone opened a macro loaded Word document no one spotted that their antivirus had alerted (but not blocked) a download of Emotet, nor did anyone spot that shortly after a local admin account was used to install some network mapping tools.

3 Jackpot for hackers

The attackers were lucky: protection of the local admin account on the endpoint they had access to was, to be polite, very weak.

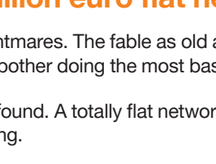
Worrying on its own, this gets terrifying when you factor in that the local admin password was the same on every endpoint of the network, including servers and hypervisors.

This gave the attackers total access to the entire network, with no one watching what they were doing.

2 No alerts

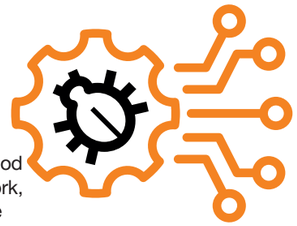
A good Security Operations Centre (SOC) could have issued an early warning to any one of those incidents. It could have all been cleaned up and the end user could have had some training to try and prevent such incidents from happening again.

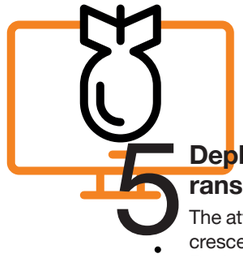
But that's not what happened.



4 Lateral movement & destruction

So off the attackers went: deleting backups, disabling AV, creating domain admin accounts, using Blood Hound to map out the entire network, and opening up firewalls to outside Remote Desktop (RDP) connections.





5 Deploying ransomware

The attack reached a devastating crescendo when the ever-popular Ryuk ransomware was placed in a hidden share folder on the client's domain controller. Accompanied by a list of over 4,000 Microsoft Windows endpoints in a simple ".txt" file, a lone ".bat" file, and a copy of the legitimate Windows "PsExec" binary.

With one click the bat file unleashed Ryuk on the network encrypting every usable file and grinding the business to a total standstill.

6 Recovery

In total the Orange Cyberdefense CSIRT worked for four weeks to get the network back up and running.

Against all advice from Orange Cyberdefense, the client paid half a million Euros to the attackers to get decryption keys. On top of that, they had to pay a law firm hundreds of thousands in fees to handle the payment (begs the question who the real criminals are in this), and well over half a million more in network upgrades and policy changes to get the damaged network to a clean and trustable state.

Lessons learned

So what should you take away from this tale of horror?

The majority of weaknesses in the network could have been easily changed: network segmentation is probably the most basic of security measures, as well as strong password policies and user rights restrictions. These measures have some impact on how IT staff work, but don't cost a lot to implement. Admittedly, retrofitting a SOC is a big project, but that's why you ensure that your network implements best practices to begin with.

The scariest part of this story: we have left a lot of the details out for privacy purposes.

In real life, it was much worse.

GandCrab encryption broken

A free decryption tool for the GandCrab Ransomware discovered earlier this year has been released[t30].

Story 3: A delicate email affair

While this attack didn't bother the CFO of the client as much as the first story, it did keep the PR team awake at night and worried for a few weeks. It is nothing newsworthy to talk about how more companies are now putting faith in the cloud. Especially when it comes to email and file shares, with Microsoft Office 365 (O365) taking the lion's share of email hosting for big business.

As with a lot of IT, this shift in practice has resulted in some security gremlins.

1 High-level spam

In early 2019 a client contacted us with a "sensitive" matter relating to an O365 email hack.

To keep the PG rating of this report, all I will say is spam emails of a rather adult nature had been sent to hundreds of thousands of accounts, from a high up individual in the organization.

2 Bad PR is not the only problem

This raised two problems for the client; the most obvious is the public relations nightmare of having a board-level member of an organization spamming so many people with such unadulterated filth, the second is that someone had access to highly sensitive emails held within the client's O365 environment.

Did they forward or download a copy of any of these emails? It became quickly apparent that the user in question had been the subject of a password stuffing attack.

3 Password stuffing

As it turned out the attack was far larger than first indicated.

Thousands of username and password combinations had been pointed at the organization's O365 infrastructure. From logs obtained from Microsoft, we managed to work out that the list used was probably the LinkedIn password database from 2016. The user of the first hacked account had the same email and password combo for both LinkedIn and their corporate email.

4 Banning insecure passwords

We found that well over a hundred accounts had been accessed from four suspicious-looking IP addresses that we could link to similar ‘smut' based spamming campaigns.

This is the first stage the client could have implemented protections to mitigate the risk of such an attack succeeding. Stopping users from reusing passwords is hard, but not impossible. Known leaked passwords can be blocked from use on corporate networks, services like “Have I Been Pwned” allow you to match password hashes to known leaked lists, meaning you can have a huge banned password list.

5 Tracking back the attack path

Once we were happy that we had identified all accounts that had been ‘popped' during the attack we started to map out what had happened, and what access to data the attackers might have had.

6 Automated hack but no data breach

We could see from timestamps that the attack was automated. The time delay from the time of access to the time of the first emails being sent was just a few seconds, and the volume of emails sent in such a short time frame matched other campaigns that had been proven to be automated.

We also didn't find any signs of emails being synched or down-loaded, nor did we identify any forwarding rules across any of the affected accounts.

7 Recovery

All we could see were hundreds of email accounts were being accessed, then sending out millions of top-shelf emails that swiftly got deleted.

This made the data protection officer happy but put the PR and marketing team in a bad mood.

Lessons learned

As with the first story, some easy changes could have been made to the setup to stop this early. Users tend to access emails from the same devices, and same IP addresses (at least the same country IP block), so alerting on email access from abnormal IP addresses is a great tool for early warnings. Especially if you can then correlate those IP addresses to other authentication attempts.

The one big remedy though, is two-factor authentication (2FA). In 2019 any organization that has internet-facing infrastructure/services without 2FA enforced is asking for trouble. 2FA stops the majority of "drive-by" or "opportunistic" attacks that cause so much damage. While scanning IPs is easy and free to roll out, 2FA can be a bit more tricky. But look at the advantages gained from the week or two worth of effort to get it set up. No doubt about it, everyone should be using 2FA.

So there you have it, three stories from the Pentesting- and CSIRT trenches showing you what you should do to stop financial and public relations disasters. By simply sticking to industry best practices a lot of clients could drastically reduce the threat of these specific attacks, and once you have the basics covered you can look at stopping super-sexy-targeted hacking attempts or sophisticated nation-state attacks.

Facebook announces Libra, its own cryptocurrency

Followed by a very mixed set of reactions the world’s most powerful social media network announced it would start its own blockchain-based cryptocurrency in 2020[t31].

Laurent Célérier
EVP Technology & Marketing, Orange Cyberdefense
Former senior officer, French Ministry Of Defense

Databreaches on the rise

Where has all the data gone?

If history is to be believed, 2017 was a standout year for ransomware. Our poor colleagues down in IT (and even more so our CSIRT!) are still experiencing anxiety burdened memories of the highly damaging campaigns from WannaCry, Petya and NotPetya.

Digital extortion was nothing new, but the success of the 2017 ransomware campaigns was certainly newsworthy. Unprecedented media attention coupled with crippled businesses. It was a year that we won't soon forget..

The year 2018 brought a new plague, not quite of biblical proportions, but cryptomining certainly hurt many IT digital wallets (and electricity bills). Highly dependent upon the street value of Bitcoin and other cryptocurrencies, rogue miners had a boom throughout the first half of the year, employing several new successful attacks. Botnets globally had a new mission, their compute muscle was switched from traditional spamming and DDoS attacks to digital revenue generation.

So what was the “big thing” in 2019? The year may not be an Olympic year, but it will be remembered as a year of record breaking data breaches!

Timing is everything

Time, and the lack of it, is always a crucial factor when managing data breaches. Many breaches are only discovered years after they first occurred. On occasion data breaches are even committed over a number of months or even years before being detected. More often than not, organizations are informed of their breach by authorities or security researchers discovering data linked to the organization on the darker parts of the internet; much too late to prevent harm to the impacted individuals, and baffling organizations. It is often difficult to trace back and figure out how the data actually got leaked and when.

Billions not millions impacted

An eyewatering 4,174,339,740 leaked datasets were discovered in 2019. Consider this: the earth's population was estimated to have reached 7.7 billion in April this year[4.29], that means that potentially one in two people has had personal information unlawfully disclosed. This figure should be alarming, not only to data protection enthusiasts and fans of the GDPR.

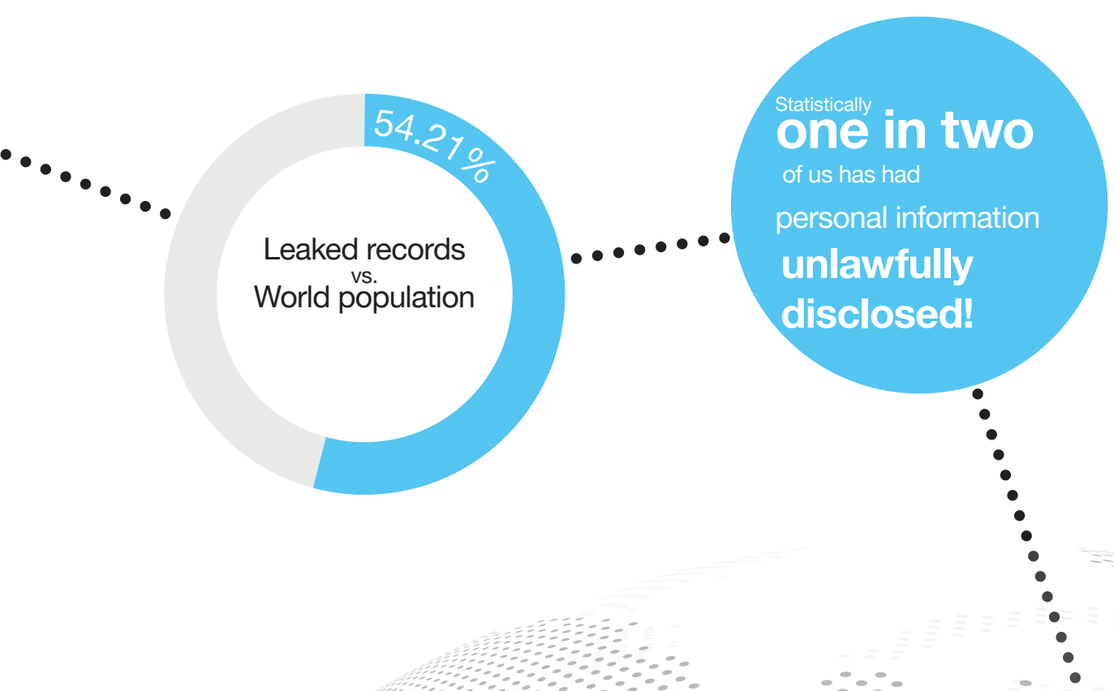
And those are just the breaches we know about.

Businesses under siege

According to the Midyear Data breach Report[4.30] there were 3,813 data breaches reported in the first half of 2019, an increase of almost 54% as compared to the same time in the previous year. In the same period, eight breaches were reported as exposing over 100 million records.

At 84.6%, the vast majority of those originate from the business sector. It also comes as no surprise that criminals primarily seek email addresses, which were found in 70.5% of the breaches and passwords (64.2%)[4.30]. Obviously valid credentials can be abused in numerous ways.

The methods used by attackers to obtain large quantities of data are nothing new: tactics like phishing and skimming remain popular.



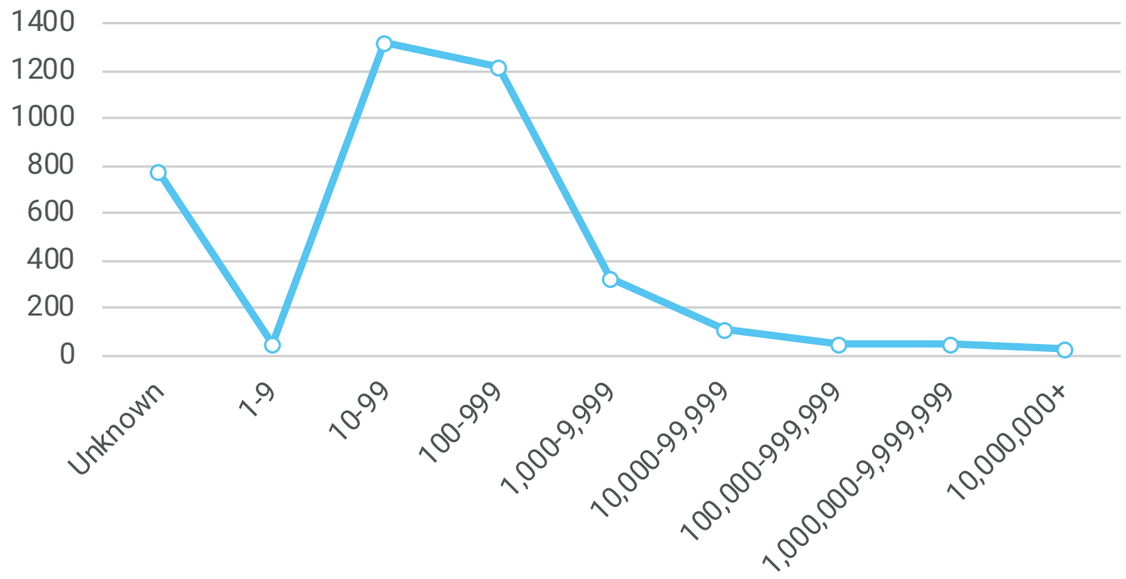
There is no "too small"

Media coverage embraced the opportunity to sensationalize the breaches of larger organizations, and rightly so! This may take the heat away from small and mid-sized businesses. However, this might also lead to a false sense of security especially for mid-market organizations. Considering the actual numbers, this is a dangerous misconception: more than two-thirds of the data was exposed in small quantities of 1,000 records or less. It appears all fruit is good fruit for criminals, regardless of size.

Data from one breach soon meets data from another. Data enrichment creates new opportunities for criminals, providing a sustainable business model for reliable, quality data to those wishing to monetize it.

So, what later is found for sale is often an accumulation of thousands of smaller businesses having suffered data breaches, often without even knowing it.

Data breaches by number of records[4.30]



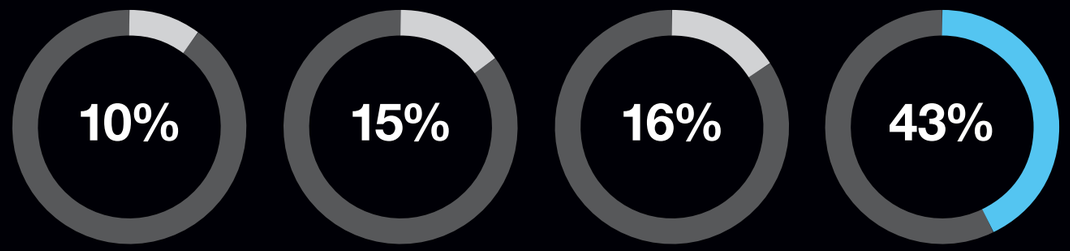
Why climb the tree...

... when fruit can be harvested from the ground?

Ok, fruit found on the ground is often considered inedible, but data has no bacteria. Hacking still monopolizes the statistics when accounting for the most incidents (82%), but not for the largest amount of records. In fact, the numbers are misleading. When we take a closer look we find that 79% of the actual data exposed required little to no effort for harvesters; with misconfigured databases, web services and apps, or insecure cloud storage accessible over the web contributing to the data hauls. Insider actions, both malicious and accidental are another major source of fruit picking.

Victims of data breaches

Source: Verizon data breach report 2019[4.31]



Remarkable data breaches in 2019

Breach	Date	No. of records	Method	Source
Collection 1	Jan 17	773,000,000	hacked	[4.1]
Universiti Teknologi MARA	Jan 25	1,164,540	hacked	[4.2]
Ministry of Health (Singapore)	Jan 28	14,200	poor security/inside job	[4.3]
GnosticPlayers, Round 1	Feb 11	617,000,000	hacked	[4.4]
GnosticPlayers, Round 2	Feb 15	127,000,000	hacked	[4.5]
GnosticPlayers, Round 3	Feb 18	92,000,000	hacked	[4.6]
Health Sciences Authority (Singapore)	Mar 15	808,000	poor security	[4.7]
GnosticPlayers, Round 4	Mar 17	26,000,000	hacked	[4.8]
Facebook	Apr 04	540,000,000	poor security	[4.9]
Facebook	Apr 18	1,500,000	accidentally uploaded	[4.10]
Justdial	Apr 18	100,000,000	unprotected api	[4.11]
Mystery Database	Apr 30	80,000,000	unprotected	[4.12]
Truecaller	May 22	299,055,000	unknown	[4.13]
First American Corporation	May 24	885,000,000	poor security	[4.14]
Canva	May 28	140,000,000	hacked	[4.15]
Westpac	Jun 03	98,000	hacked	[4.16]
Australian National University	Jun 04	200,000	hacked	[4.17]
Quest Diagnostics	Jun 05	11,900,000	poor security	[4.18]
Desjardins	Jun 20	2,900,000	inside job	[4.19]
2019 Bulgarian revenue agency hack	Jul 16	5,000,000	hacked	[4.20]
Capital One	Jul 29	106,000,000	hacked	[4.21]
StockX	Aug 03	6,800,000	hacked	[4.22]
Health Care Image Leak	Sep 17	16,000,000	unprotected	[4.23]
Novaestrat	Sep 18	20,000,000	unprotected	[4.24]
Mobile TeleSystems (MTS)	Sep 20	100,000,000	misconfiguration/poor security	[4.25]
Amazon Japan G.K.	Sep 26	unknown	accidentally published	[4.26]
DoorDash	Sep 26	4,900,000	hacked	[4.27]
Zynga	Sep 30	218,000,000	hacked	[4.28]
Total:		**4,174,339,740**		

Conclusion

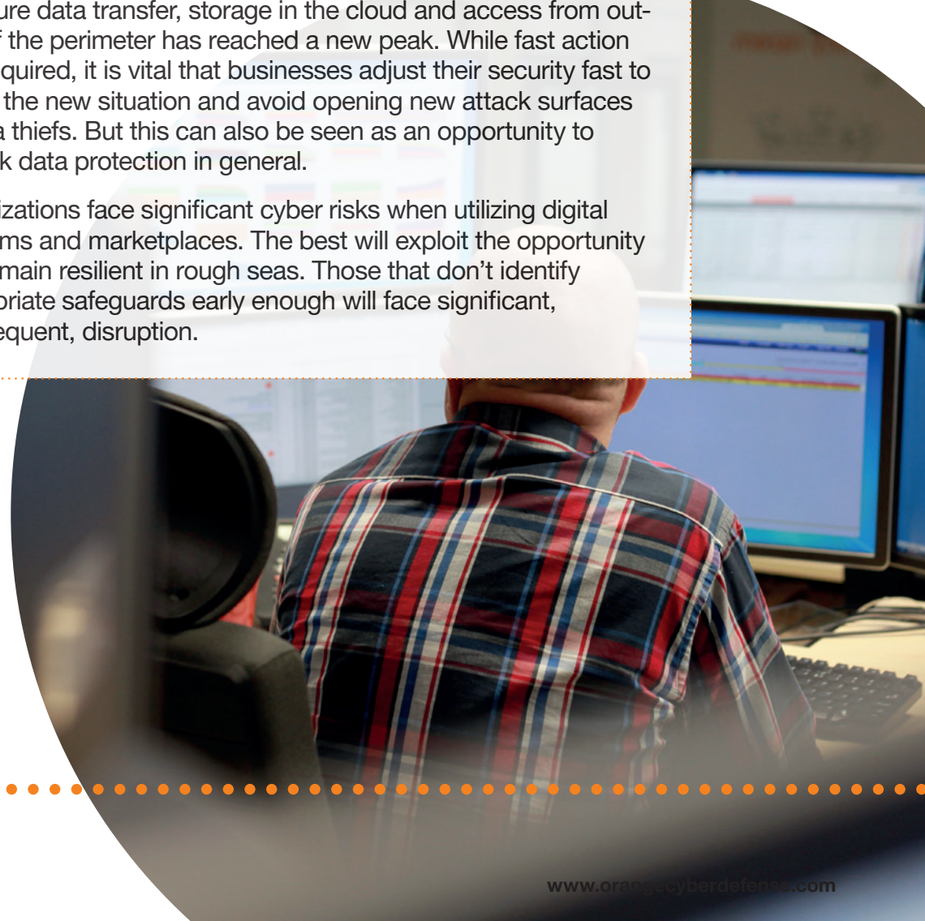
Despite new regulations, the availability of state-of-the-art technology and a greater understanding of cyber risk, 2019 has seen an incredible number of high profile data leaks. With more information than ever before available on criminal marketplaces, data protection is a top priority issue facing the vast majority of organizations.

With 80% of data breaches resulting from unintentional or accidental causes, organizations need to take a close look at their data processing to identify the root cause. Employee awareness training, monitoring and inside threat analytics are key to preventing data leaks.

High profile cases such as Marriott, British Airlines and Facebook create new landmark consequences for organizations. Not just reputational impacts, but regulatory bodies flexing their muscles to deliver heart-stopping fines. The ripples from these events don't stop with the organizations, cyber harm is now a reality for many people; people who find themselves chasing control of their own digital identities.

The COVID-19 lockdown has forced a significant part of the service industry into home-office. As a consequence the importance of secure data transfer, storage in the cloud and access from outside of the perimeter has reached a new peak. While fast action was required, it is vital that businesses adjust their security fast to match the new situation and avoid opening new attack surfaces to data thiefs. But this can also be seen as an opportunity to re-think data protection in general.

Organizations face significant cyber risks when utilizing digital platforms and marketplaces. The best will exploit the opportunity and remain resilient in rough seas. Those that don't identify appropriate safeguards early enough will face significant, and frequent, disruption.



Charl van der Walt
Head of Security Research
Orange Cyberdefense

Technology review

How safe are VPNs?

Virtual private networks (VPN) are considered a safe means of communication and data transfer, especially in business. We took a closer look to check for weaknesses.

Enterprise businesses equip staff with mobile devices such as laptops and smart phones to perform daily tasks. This makes the workforce much more mobile but places an implicit burden on the staff to ensure that they are always online. Security is handled by the underlying operating system and supporting solutions, such as VPN. Commercial VPN technology has been around since at least 1996. Recently this technology reached a new level of importance due to millions of service employees worldwide having to access corporate network resources remotely because of the COVID-19 lockdown.

VPN solutions, especially enterprise grade, can be complicated and nuanced with several configuration options. Remotely supporting users with technical issues can result in overheads when trying to resolve technical issues that are caused by misconfigured solutions.

In this section we will reveal the findings from the research we have conducted into the effectiveness of modern commercial VPN solutions in respect to contemporary mobile worker use cases, typical endpoint technologies, and contemporary threat models.

Talking about VPNs - do they actually still work?

What is a VPN supposed to do?

A VPN should afford its users confidentiality and integrity of network connectivity, guarding against data sniffing and tampering. In corporate environments authentication and access control are added to ensure that only legitimate users gain access to corporate resources. In this sense modern enterprise VPNs are fulfilling at least two, separate, use cases.

The words virtual private and network capture exactly what their purpose is. “Virtual” refers to the fact that the construct it emulates resembles and behaves like a physical equivalent. The word 'private' lays claim to confidentiality and implies trustworthiness.

We can thus infer that a VPN is a logical extension of a private network to another location giving the experience that a distant computing device resides on the local network segment. This network extension can span across public internet.

VPN is not simple

The reality of VPN solutions is that they are rarely deployed in a simple way with all the traffic going down the VPN towards the enterprise. For example, most deployments allow for some traffic to be directed down the VPN tunnel while some traffic is sent directly to the internet. This facility is often called split tunneling and has become more and more prevalent as internet speeds have increased.

Another complex example involves remote workers that connect to complimentary internet hotspots typically offered by coffee shops, airports, hotels, etc. Hotspots are Wi-Fi access points that offer free internet bandwidth. Most hotspots today feature a captive portal that requires either a password, a voucher code, or some form of consent before allowing a connected computer access to the internet.

A robust VPN implementation should not allow a user to interact with a network resource that bypasses the VPN tunnel. In most modern deployments however, this creates a catch 22 scenario because the user must first connect to the hotspot Wi-Fi and then process the request of the captive portal before the VPN software can connect to the server and establish the tunnel.

What happens in the timeframe between connecting to the Wi-Fi hotspot and activating the VPN, while the user is dealing with the captive portal?

How vulnerable is the user during this time? The Wi-Fi hotspot will securely isolate guests while the local firewall on the laptop will protect the user from any attacker; but does this work even if the hotspot is fully under the control of an attacker? Let's take a closer look.

VPNs & security

For this research, its important to understand the basic threats against confidentiality, integrity and access control that the VPN is supposed to protect the typical corporate user against. We focused on the following:

DNS ‘person in the middle’ (PiTM) or spoofing

The attacker somehow feeds fake DNS responses to legitimate requests from the client, thereby controlling where the subsequent connection ultimately terminates. This is a precursor to several other attacks, like spoofed websites for credential harvesting or 'responder' attacks (see below).

Harvesting credentials using spoofed website

Once the attacker controls DNS and routing (as they would with a malicious AP) they can present the user with a fake login page to valuable resources like O365 to harvest login credentials.

Capturing Windows hashes via responder

So-called ‘responder’ attacks involve tricking Windows systems into connecting to a fake Windows service, which in turn requests authentication and then captures the password hash that is sent. This enables further attacks against Active Directory resources, like connecting to the VPN gateway itself, which commonly uses Active Directory for authentication.

Using the Browser as a tunnelling proxy

Once the attacker controls DNS and routing (as she would with a malicious Access Point) they can inject JavaScript code into other legitimate websites to exert some remote control over the victim’s computer, for example using it as a pivot point to tunnel traffic into the corporate network.

Using IPv6 to interact with host

Most enterprise VPN technologies are designed to protect IPv4 traffic, but many endpoints now also run IPv6 stacks that can be used to communicate on the LAN and internet. If the VPN doesn’t control IPv6, that presents the attacker with an open channel for communicating with the computer.

All the attacks described above could be considered feasible when a corporate computer is connected to a public Wi-Fi access point (AP) controlled by a hacker. Businesses therefore depend to a great extent on VPNs to protect their roaming endpoints. Given the ambiguous state captive portals place the endpoint in, we want to know to what extent VPNs still offer the kinds of protection we expect.

Introducing captive portals

Captive portals are commonly used by Wi-Fi internet access providers like hotels, airports and coffee shops. A device requiring internet access will be able to connect to the Wi-Fi network but will generally not have internet access until the demands of the captive portal for payment, personal details or consent are met.

Once connected to a Wi-Fi AP the operating system (OS) of most modern devices will generally test for internet access by making an HTTP request to a URL of its choosing. If the HTTP response matches to what it expects then the OS assumes the device is connected to the internet

If a captive portal is encountered, however, the OS will prompt the user, usually by presenting a web browser interface that shows a message from the portal in form of a web form. In the case of Android and iOS, the user is informed that a captive portal is present and asked if she wishes to interact with it.

Android and iOS have special web browsers built in that that are called captive portal mini-browsers. These are separate from the full-fledged web browser apps. macOS has a similar concept in the form of a Captive Network Assistant.

Windows and Linux however rely on the default web browser to interact with the captive portal, and Windows can automatically start the default web browser when it detects the captive portal. Linux is silent and relies on the user to start a web browser, such as Firefox, that can detect a captive portal.

In all cases however, the use of a captive portal on a ‘free’ Wi-Fi network creates a significant window of time in which the device is connected to the Wi-Fi AP, has its network configuration controlled by the Wi-Fi AP, but cannot connect to the internet, and therefore cannot establish the VPN.

Introducing VPN split tunnelling

Another common, though not mandatory, VPN configuration setting used by enterprises is called ‘split tunneling’. Split tunneling is when a VPN is configured, once connected, to route specific network requests through the VPN tunnel while other traffic follows default network routing rules. This is done so that only traffic destined for the corporate network is encrypted and subject to access control, while regular local network or internet-bound traffic can traverse directly and in the clear. The reasoning is obvious – to allow access to resources on the local network and improve performance when accessing public internet sites and services.

The implications of this configuration choice may not be so clear, however, as it also implies a computer ‘captured’ by a malicious Wi-Fi network could be forced to make connections or send traffic via unencrypted and unprotected routes.

In our testing of two major enterprise VPN products the default deployment, once the VPN was established, involved split tunneling. This is the model we used in our tests and which we report on below.

Test A: standard mode

As suspected, in this state the typical Windows machine is completely vulnerable to all the threat vectors we outlined, for both enterprise VPN products that we tested. More worryingly, when used in split tunneling mode, both VPN products remained vulnerable to these attacks even after the VPN was fully established. (✓ = protected, ✗ = no protection)

Attack	Captured		Online	
	VPN1	VPN2	VPN1	VPN2
DNS ‘person in the middle’ or spoofing	✗	✗	✗	✗
Harvesting credentials using spoofed website	✗	✗	✓	✓
Capturing Windows hashes via responder	✗	✗	✗	✗
Using the browser as a tunneling proxy	✗	✗	✓	✓
Using IPv6 to interact with host	✗	✗	✗	✗

The findings above represent the results of a simplified and discrete version of each case. There may be instances, for both the failed and successful tests, where the results may differ based on other circumstances that fall beyond the scope of this test.

JUL

Double-Dip: massive fines for breached institutions

British Airways was fined £183 million under GDPR for its 2018 data breach[t32], Equifax has to pay up to $700 million in 2017 data breach settlement[t33] and Marriott faces a $123 million fine following the Starwood data breach[t34].

VPN improvements – lockdown mode

Modern VPN technologies have responded to the challenge of captive portals as described above by introducing a set of features generally known as ‘captive portal remediation’ or ‘lockdown mode’ which are supposed to provide better protection in certain untrusted environments.

Lockdown mode can be thought of as a set of VPN features that are designed to limit the amount of traffic that leaves the endpoint while it is on the WLAN, dealing with the captive portal.

The specifics of these features vary from product to product, but generally come down to

- protecting the browser that connects to the portal and
- limiting the amount of traffic that’s allowed to leave the computer.

We therefore proceeded to test the two VPN products that offered these features with the full capabilities enabled, to determine how effective their protection was.

Test B: lockdown mode

In summary, our testing shows that even the so-called ‘Lockdown’ capabilities provided by VPN vendors to mitigate against the risks introduced by captive portals do little to mitigate against contemporary technical threats. (✓ = protected, ✗ = no protection)

Attack	Captured		Online	
	VPN1	VPN2	VPN1	VPN2
DNS ‘person in the middle’ or spoofing	✗	✗	✗	✗
Harvesting credentials using spoofed website	✗	✗	✓	✓
Capturing Windows hashes via responder	✗	✓	✗	✗
Using the browser as a tunneling proxy	✓	✗	✓	✓
Using IPv6 to interact with host	✗	✗	✗	✗

The findings above again represent the results of a simplified and discrete version of each case. There may be instances, for both the failed and successful tests, where the results may differ based on other circumstances that fall beyond the scope of this test.

Summary of findings

In summary, our experiments demonstrate that our initial concerns about the failure of VPNs to protect machines in captive portals all hold true. This is not to say that these VPNs don’t ‘work’, or that they have ‘bugs’, but rather that captive portals present a use case that VPNs were simply not originally designed to deal with.

Under the assumption that any ‘free’ Wi-Fi service should reasonably be considered malicious, and with an appreciation of contemporary attack vectors and tools, this inability to deal with a significant new use case represents a serious limitation. It forces us to depend on secondary mechanisms like SSL/TLS, firewalls and endpoint protection to defend the mobile endpoint.

We were further disappointed to discover that even once fully established, a carelessly configured VPN barely does better at mitigating these very real threats.

In response to the challenges introduced by captive portals, enterprise VPNs have introduced a set of ‘lockdown’ features that are intended to ‘mitigate’ the captive portal problems. These features do indeed address some issues, but unfortunately barely put a dent in the full set of threats we considered for our experiments.

While the behavior of some of these features have at times perplexed us, we must emphasize that this is once again a fundamental function of how captive portals work, rather than a problem with the products themselves.

The threats we considered in our experiments are by no means catastrophic in nature. Several factors must coincide for the weaknesses to be exploited, and several external factors could prevent such attacks from succeeding.

However, we assert that there is a realistic set of conditions under which modern VPNs fundamentally cannot fulfill their declared objective of securing confidentiality, integrity and dependable access control.

As our own first-hand experience illustrates, the conditions required to maliciously exploit this weakness in VPN technologies can occur under common real-world circumstances and is probably much more common then we realize.

We would assert that the threat is serious and realistic enough to warrant a serious response by enterprise IT teams, as we will discuss below.

Recommendations

We believe that the vulnerabilities and threats described in these experiments are serious enough to warrant an urgent response, though this need not be expensive or disruptive.

Our technical recommendations can be summarized as follows:

Configuration changes:

- Avoid using split tunneling in your VPN configuration. Rather have corporate users tunnel through the enterprise network where they can be subject to egress filtering, monitoring and other protections the internal network offers.
- Use your VPN configuration to enforce an internal DNS server under your control, and to hardcode the DNS domain search suffix. Both the enterprise VPN products we tested offered this feature, and we expect other serious products to do so also.
- Understand and implement whatever ‘lockdown’ and ‘captive portal mitigation’ features your VPN offers. This will not be a simple change and will require careful testing and deployment.

Other technical controls:

- Ensure that all the internal Windows systems your users access use fully qualified host names. For example, consistently use ‘ocd-src-server.ocd.local’ and not just ‘ocd-src-server’.
- Local host firewalls and sophisticated Endpoint Detection & Protection programs, properly used, can offer significant defence against the attacks described here.

Strategic thinking:

“If you’re not the customer you’re the product” is a saying that’s frequently used these days.

We believe it holds true for so-called ‘free’ Wi-Fi services also. The cost to privacy and security that must be offered in exchange for free internet for mobile users is to our thinking too high for modern businesses who must take both essentials seriously. We therefore recommend that businesses equip mobile workers with appropriate mobile data technologies and bandwidth so that they can connect via a relatively trustworthy, visible and accountable mobile network provider, rather than a veritable smorgasbord of wholly unknown free internet providers whose integrity and motives can never be fully trusted.

Consider Zero Trust.

Zero Trust is an emerging security paradigm in which all networks are considered equal, and untrusted, where there is no internal or external space, and where security must therefore be achieved on the endpoint and on the server without requiring a VPN. Zero Trust is a security ideology conceived for the modern internet and being adopted by leading thinkers like Google in their own security strategy. We recommend our customers seriously engage with the Zero Trust concept and the new set of technologies and approaches it advocates if security is to remain relevant in the face of changing technologies and emerging threats over the next five to ten years.

Conclusion

Security technologies emerge onto the market in response to a specific set of threats.

As the needs of the client and the technology landscape evolve, however, so must the security product. Ensuring continued alignment between evolving threats and the technologies we use to mitigate them requires constant vigilance.

The COVID-19 lockdown has proven once more how reliant we are on secure networking technology. This has brought VPN into the focus of both potential attackers and responsible security representatives.

Our investigation regarding the effectiveness of VPN products in the context of modern internet configurations raises significant cause for concern. The issue is really a larger one, however, regarding the constant effort required to understand the threat, the difficulty of understanding how our security tools align to the threat, and ultimately ensuring that we are using those tools to their full effect. No technology on its own makes a problem go away.

That's our responsibility, and it hasn't gotten any easier.

Ransomware eCh0raix/QNAPCrypt targets network storages

In Linux based networks the malware targets NAS servers produced by QNAP Systems either by brute forcing weak SSH credentials or exploiting known vulnerabilities[t35].

State of Kazakhstan could launch PiTM attacks on all citizens

Kazakh ISPs are forced to require their customers to install a government-issued root certificate labeled "national security certificate", hence enabling authorities to intercept and censor all encrypted HTTPS and TLS connections[t36].

Ransomware causes power outages in Johannesburg

South AfriCAs biggest city, with a population of more than 5 million, suffered power outages for several days due to its major power supplier, City Power, being hit by a ransomware attack[t37].

AUG

European Central Bank shuts down 'BIRD portal' after getting hacked

"Unauthorized parties" had managed to breach the Banks' Integrated Reporting Dictionary (BIRD) website, which was hosted by a third-party provider, eventually forcing the ECB to shut down the site[t39].

POC: Ransomware can spread to DSLR cameras

Researchers at Check Point have discovered severe vulnerabilities in the firmware of Canon cameras. A POC demonstrated these could easily be exploited to infect a camera with ransomware via USB or Wi-Fi[t38].

French police remotely removed RETADUP malware from 850,000 infected PCs

France's National Gendarmerie took out a RETADUP botnet using a flaw in the malware's CNC-communication. The cybercrime division (C3N) ceased control of the CNC-server and triggered a self-destruct of the malware on infected clients[t40].

Ransomware protection service hit by ransomware

DDS Safe, a cloud-based data backup system popular among dental practice offices in the US (to safeguard medical records from cyberattacks) has been hit by Sodinokibi ransomware[t41].

Michael Haugland
Threat Research Analyst
Orange Cyberdefense

Technology review

The PKI and digital trust

The public key infrastructure (PKI) we use today facilitates many of our secure, everyday internet activities: ecommerce, internet banking, instant messaging and confidential email. PKI can be used in different ways to provide the four ingredients for trust, namely: confidentiality, authentication, integrity, and nonrepudiation. It is something we take for granted and we hardly ever question it.

In blissful ignorance we accept it simply works. But does it?

We have analyzed the fundamental building-blocks of PKI to understand who we actually trust when using encrypted data transmission, such as secure hypertext transfer protocol or HTTPS for short.

What we found is alarming: digital trust is not only distributed very unevenly in a geographical sense (it is largely fixed in the US), but you also trust countries you would probably be concerned about.

Apparently, the basis of secure online communication is our trust in largely unmonitored, intransparent private organizations. And no one ever even thinks about it.

In certificates we trust

The use of encryption predates the Romans, and was even popularized by Caesar. The basic concept is simple and hasn't changed for millennia: using a secret key to convert a message into cipher text, rendering it useless for anyone who is not in possession of the secret key to decipher it.

Using the PKI we can easily achieve this for HTTPS traffic:

- We connect to a web server which identifies itself using a digital certificate;
- Our browser verifies that the digital certificate is valid (domain, date and signed by a Certificate Authority (CA));
- If validated, cryptographic keys are exchanged, and the resulting communication is encrypted.

Allowing parties to identify one another with digital certificates is the basis for reliable communication, providing confidentiality through the use of encryption, data integrity and a reasonable foundation for nonrepudiation.

When trusting digital certificates, we rely upon independent CAs who distribute them. We trust they meet certain principles and criteria to become a CA. We (end-users) play no part in the selection of CAs and rely upon the digital certificate subscriber (owner) to choose an appropriate CA when we use their product or service for our communication. The devices we use and the software we choose come preloaded with CAs ready to establish trust on our behalf, displaying the padlock to indicate trusted and secure communications.

So, who do you implicitly trust? And what does this mean for secure business communication?

The implications of enforcing trust

A PKI consists of all the roles, policies and procedures needed to manage (create, distribute, store and revoke) digital certificates. The implementation of these is usually governed by a territory or region, often fracturing their very principles.

Trust, however, requires reliability, consistency and transparency: the direct opposite of the evolving PKI implementation. This conflict is a conceptual dilemma rather than a technical flaw in the PKI, which makes it incomparably harder to fix.

CAs are at the root of this problem. Certificates are the ID cards of the internet. But, imagine what would happen if ID cards were not issued exclusively by trustworthy government organizations, but instead by a non-transparent set of private institutions, each according to their own set of rules and agenda?

Some of them might not even exist as separate legal entities anymore, but their ID cards would still be commonly used. What would be the impact on the trustworthiness of ID cards? Would it be wise to trust a messenger with business-critical information, who relies on such an ID?

Yet this is pretty much how the PKI works today.

Identifying who we trust

Our methodology

We leveraged "The Alexa Top Sites Service", a service that provides access to lists of websites ordered by Amazon's Alexa Traffic Ranking. This list provides a reasonable representation of the web's ecosystem as a whole.

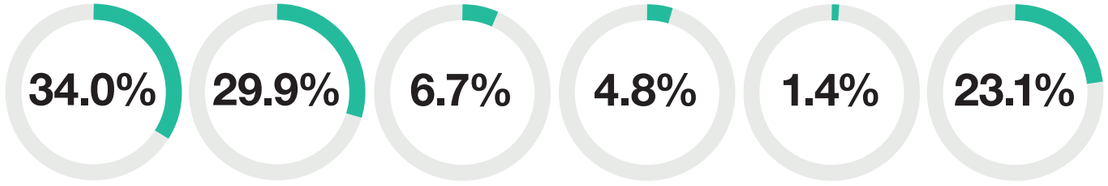
We connected to, and downloaded the full certificate chain, of every site on "The list" (~1 million) by using a proprietary tool.

Which is the most trusted CA?

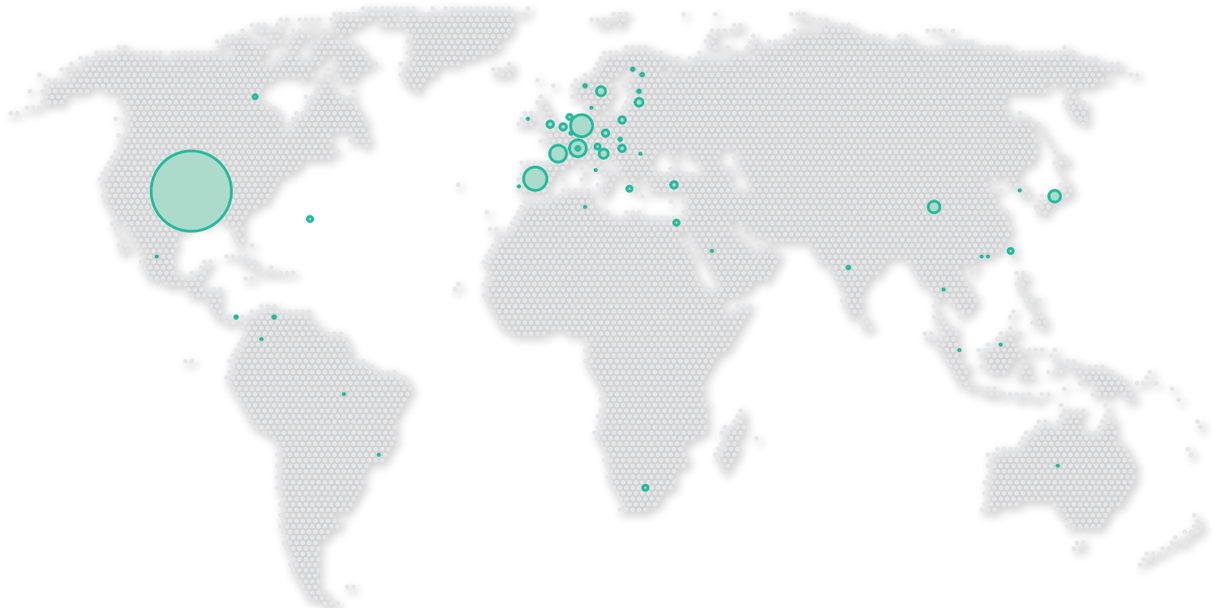
Figuring out which CA is the most trustworthy depends on many factors, but primarily your geolocation. However, our dependency on two standout CAs is clearly who we trust the most. The two major CAs are DST rootCA X3 and AddTrust External. Together, their certificates are used by 64% of the sites in the list.

Certificate utilization

Percentage of the certificate roots used within the list



AddTrust External	DST Root CA X3	Go Daddy Secure Certificate Authority - G2	DigiCert Global Root CA	Self signed	Others (<5%)
AddTrust AB	Digital Signature Trust CO	Go Daddy Group Inc.	Digi Cert Inc.		

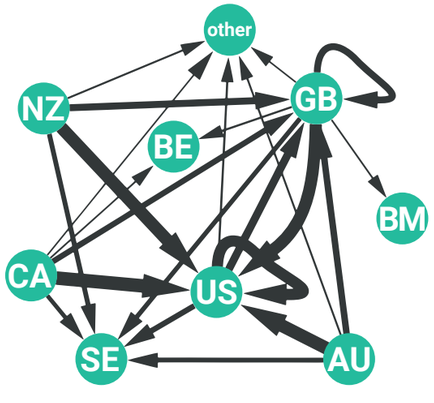


Trust store certificate distribution by geolocation

The map above was produced by looking at the trust store for all sources and grouping the certificates by the country code (attribute C) defined within the certificate itself. Each country was mapped to a coordinate and drawn on the map with a circle size that proportionally represents the number of certificates in each group.

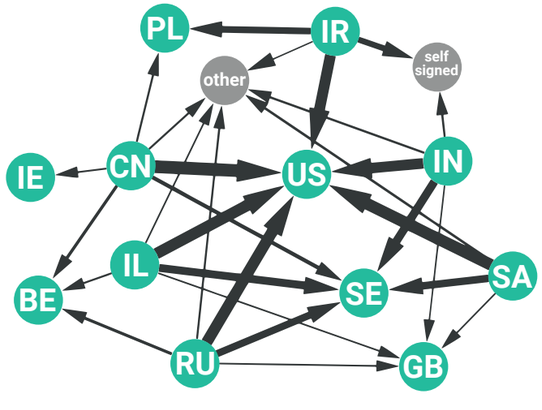
Geographical patterns: who do the "Five Eyes" trust?

The Five Eyes, often abbreviated as FVEY, is an anglophone intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. Trust among the FVEY is very much directed inwards, or rather, directed towards one entity. America is overwhelmingly the most trusted entity. Other important locations include Great Britain, which is not much of a surprise, and Sweden. This seems odd, but the root certs which produced that node in the graph were originally owned by AddTrust, so really the credit should go the U.S. instead.



Who do the 'usual suspects' trust?

While this trust distribution exhibits a similar pattern to that of Five Eyes, with the US being at the epicenter, it does have some deviations. For instance, self-signed certificates are overly prevalent in India and Iran. Furthermore, these countries seem to be more inclined to place their trust in Great Britain, Poland and Belgium than the Five Eyes.



Trust store utilization

So, which automatically trusted CAs are actually in use? We analyzed the percentage of each trust store utilized in the list. In the below chart, green indicates which trust store has been observed in The list. To determine the trust store utilization, we compared two values:

- A list of trusted CAs and Root CAs available in the vendors implemented Trust Store
- The CAs and Root CAs we identified as "used" after analyzing the The list

"Orphaned" CAs lingering in the system

We found that large amounts of the trusted CAs actually are unused. Every additional CA is a potential source of risk, so this is somewhat disturbing. Microsoft, for example, hasn't used about 72% of its trust store.

In contrast, the vendor whose trust store has the highest use percentage from the list, is Android with only 37% left unused. This is still a significantly high percentage.

Who is behind the CAs?

As previously mentioned, the root certificates that identify CAs are privately owned. Apparently, there is no regulatory instance deciding which CAs can be trusted.

While the certificates themselves are subject to a defined standard (X.509 [6.1]), the means by which a public CA authenticates its users is not. These means can vary substantially[6.2]. Two common types of verification are basic domain validation, which only verifies domain ownership. Extended validation would provide more trustworthiness, and digs deeper into the actual company that offers a website or service via HTTPS, but it is rarely used. The only instance that actually provides some kind of control over these practices, and the trustworthiness of CAs are the big four browsers: Google/Chrome, Mozilla/Firefox, Apple/Safari and Microsoft/Edge.

Adding to the lack of transparency, is the fact that CAs can (and do) transfer their authority to issue certificates to subordinate CAs (which in turn may pass it on to subsidiaries). This results in a certificate chain, which can be traced back to the root. However, it does not exactly make it easier to find out if the issued certificates were actually verified to an extent that justifies the trust we place in them. Being private organizations, it would also be interesting to know who actually owns them.

To illustrate the extent of obfuscation we face in that regard, we tried to investigate which company is actually behind AddTrust, the root-CA behind every third certificate we came across in the list (see addendum).

Conclusion

Clearly there is something wrong with the infrastructure we entrust our data connections to use.

More than anything, it is obvious that it is hard to gauge who and what you are actually trusting, even if you were to look into it.

You implicitly trust CAs from geolocations you might hesitate to trust, if you had known.

CAs themselves are organizations who may or may not reliably verify who they issue certificates to, but there is no common control authority beside the major browsers; and they simply use the power of their market-dominance to drop support for dubious CAs. Is this enough, given the critical role certificates play in secure communication?

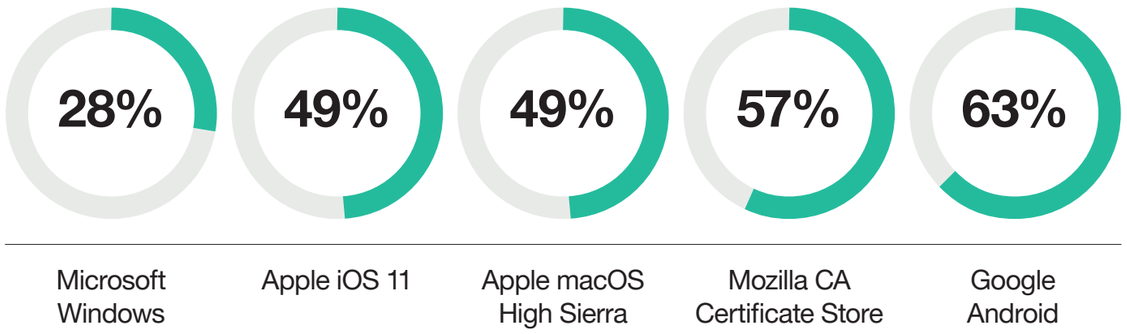
The core of the problem is that it is highly intransparent to end users who they actually trust at all.

For example, when we trust AddTrust, one of the most common CAs, we trust in an authority which doesn't even exist as an organization anymore. Those root certificates were bought by Comodo, now called Sectigo. This perfectly illustrates the lack of transparency of the PKI.

This is most likely just the tip of the iceberg.

Trust store utilization

Percentage of the auto-trusted CAs actually used within the list



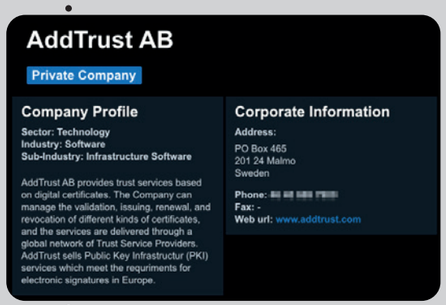
Google, Mozilla, Apple block Kazakhstan's root CA certificate

Major browsers now warn their users, when a website tries to authenticate with dubious certificates issued by the Kazakh government[t42].

Addendum: who is AddTrust?

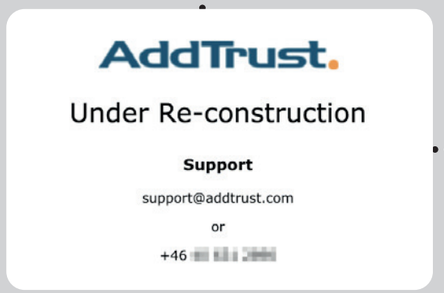
The company “AddTrust” represented more than 30% of all CA-signed certificates gathered from the list. However, there is little information directly available supporting the credibility of the Swedish-based internet company. This doesn't help the already unstable reputation of CAs. Here, we have tried to map out who exactly is AddTrust.

We started by trying to establish the trustworthiness of the purportedly Malmö based company, starting with **Bloomberg**[6.2]:

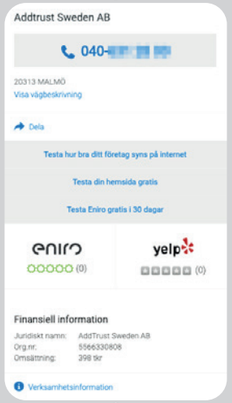


We found a link to the company website, **www.addtrust.com**, but this site cannot be reached.

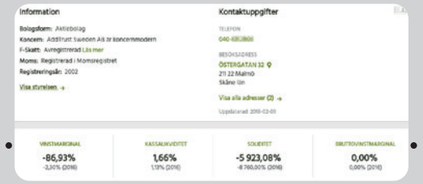
The last entry we can find for the website on internet archives is from January 28, 2011[6.3].
Here we can see a phone number and an email address **support@addtrust.com**

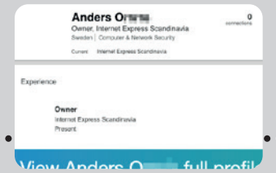


Searching for the company on the Swedish website **Eniro**, reveals more information. In addition to a phone number, we now have a Swedish organization number as well.



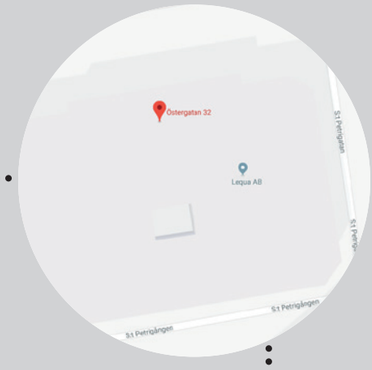
By entering the organization number on **www.allabolag.se** (which lists public information on all companies in Sweden) we can see that AddTrust is registered to **"Anders O."**
The phone number correlates with **Eniro**, and it provides us with another address.





We were able to find **"Anders O."** on LinkedIn, where he states he is the owner of **"Internet Express Scandinavia (IES)"**.

Checking this address in Google maps leads us to a company called **Lequa AB**.



In the "About Us" section of **IES'** website it states that the purpose of **IES** is to work with its 45% share in **Lequa AB.** The domain for Lequa is **www.lequa.com/**

The product they are describing is pointing to this URL: **http://www.lequinox.com/,** but that domain is not available at the time of research.

IES referred us to **Lequa**, who in turn referred us to an organization called **Comodo**, which we already know is a major player in the CA landscape[6.4].

Summary:

After an intensive investigation with obscure clues scattered all over the web, we found that about ten years ago AddTrust was bought by **Comodo CA**, which is now known as **Sectigo**.

They issued their last certificate in 2013[6.4]. Because of the long-lived trust chains we can still see AddTrust is the root of numerous certificates on the internet today.

It is noteworthy that the **AddTrust External CA Root** will expire May 30th 2020[6.5].

Stefan Lager
SVP Global Service Lines
Orange Cyberdefense

Security predictions

Fasten your cyberdefense

In September 2019 NASA "leaked" a Google paper on Quantum Superiority. While there is some speculation on how (or why) exactly this could happen[7.1], one thing is for certain: quantum computing is picking up speed – and it could do more than impact concepts like cryptography. It could, in fact, change the way computers work and how they are used on such a scale that it makes the AI-revolution look like a minor OS update. However, as with everything in quantum computing, there is a great deal of uncertainty involved.

So, let's look at more reliable predictions. What can we say from our data about what 2020 still has in store for us?

A new model for threat evaluation

For a long time cybersecurity has been driven by a reactive approach that focuses on investing in technology to prevent against cyber-breaches.

Unfortunately, this approach has been proven to be unsuccessful as the number of breaches has increased despite higher security spending. We believe it is important to balance spending across anticipating threats, detecting breaches, protecting assets, responding to incidents and recovering from breaches.

Looking at breaches in particular, we believe that moving forward, businesses will need to split up the concept of a cyber-breach into two phases:

1. The infrastructure breach: when devices or workloads are breached;
2. The data breach: when critical data is destroyed, held for ransom or leaked;

Organizations must accept that their infrastructure will be breached, no matter how much they invest in preventative technologies. Once you have acknowledged this, you need to have a plan for how to detect it, how to limit the impact of the infrastructure breach and how to respond to it as quickly as possible. This is the area where we predict investments will shift into during 2020.

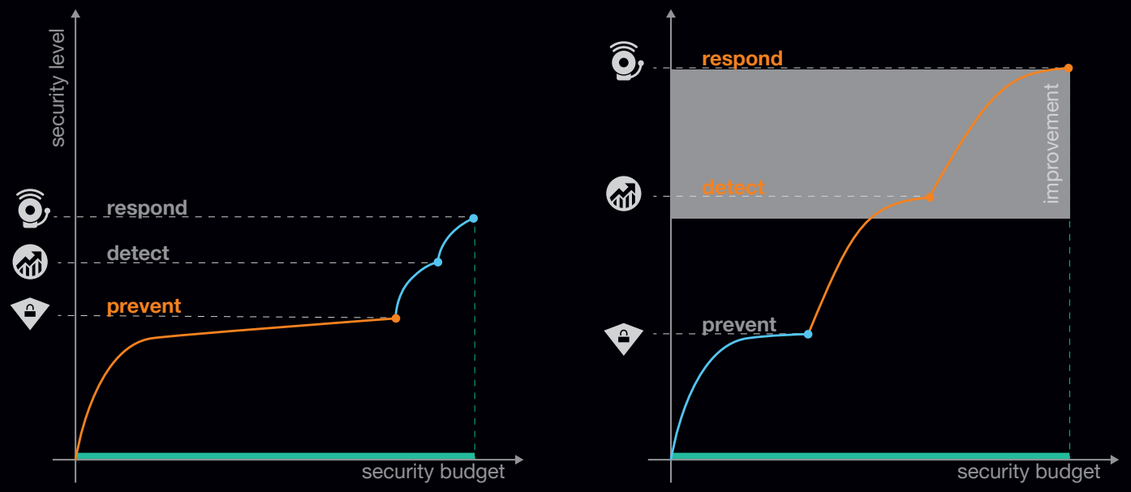
Driving detection

If we accept the hypothesis that we have to increase our ability to detect threats, how can we achieve this? We predict that the focus on just log-based detection will shift, to also include network-based and endpoint-based detection. You should select a detection strategy based on your environment and your requirements.

If compliance-driven detection is most important, then logs are for you. If you want rapid time-to-value and advanced detection and response capabilities, endpoint is for you. If you cannot install any sensors on your endpoints, network-based detection is for you. If you have high requirements of detection, you need a combination of all of the above.

It is now common knowledge that cybersecurity, is truly a “big data” issue. Regardless if you are analyzing endpoint data, network data or log data. To solve this, organizations will need to increase investments in technology that have strong AI/ML implementations, to help analyze this massive amount of data. The key to using AI/ML technologies is to acknowledge that the technologies are not a panacea. To be effective there needs to be a defined problem for which we can use the technology as a tool and not a solution. Good implementations of AI/ML can significantly offload the work of the analysts and are, together with orchestration and automation, the key components for building a SOC for the future.

Allocating a part of your security budget to detection & response will get you further than overspending on prevention alone



Response as added benefit

Now that you have sorted out the technology approach, what’s next? You need people and processes to staff analysis and classification of detections 24x7. Most businesses struggle with the cost and time of building this themselves, so they will buy this as a service (MDR) with the additional benefit that they will also receive 24x7 response.

With any security incident, the amount of damage is inversely proportional to the amount of time before the incident is detected. To be clear: the quicker you can identify a potential incident, the less the damage occurs.

Therefore, the risk created by an incident depends on how quickly you can detect and respond to a threat. But just detecting a breach is only one part of the story, response and recovery are equally important.

During 2019 many customers have called our emergency hotline to get emergency help with incidents. It is our prediction that in 2020 customers will start becoming more proactive and analyze their internal abilities to respond quickly to threats and further complement this with a subscription-based retainer from trusted security providers.

It all starts with visibility

Since cybersecurity budgets are restricted, the investments need to be spent wisely. To make a good decision about where to invest, you need data and visibility to understand where to make the most insightful investments. Therefore, we believe that investments will shift to this area going forward.

Here are some examples or areas that we have seen increased demand for.

Endpoint & network visibility

For decades people have been deploying SIEM solutions as the primary way of detecting and responding to threats. These implementations often take a lot of time, demand, tuning and maintenance. However, in the end they do not perform better than the type of data that is being provided, which in most cases is limited for budget reasons. We still believe that SIEM is a crucial component in your SOC toolbox, but you can maximize your time-to-value and enhance your threat detection capabilities by deploying endpoint-based detection or network-based detection. We see a trend in investing in both these technologies. But also as managed service, for customers that do not have their own 24x7 CSIRT team.

SIEM for machine data visibility

We all know the expression “data is the new oil”. So why not try and make use of all the data that your company creates every day, to help you make data-driven decisions and manage your business more effectively? We believe that just collecting logs for security use cases will shift into leveraging the same (and additional) data for IT and business operations use cases.

Cloud visibility

Everyone is moving to the cloud and devops teams are spinning new environments up and down by the minute. At the same time, we know that all major breaches in cloud infrastructures have been due to misconfiguration or operation practices. We believe that technology, which connects to cloud APIs to extract inventory and security data, will be very helpful for your security team, to get some control of their cloud infrastructure and make the compliance work easier.

OT / ICS visibility

Industrial Internet of Things (IIOT) and Industry 4.0 is all about connecting machines to other machines, and the optimization and productivity that is needed to make 'smart factories'.

The benefits are immense, but the challenges are also significant. A major challenge is to bridge the gap between OT experts and security experts so they have an understanding of the adversities in both areas and can build secure OT environments together. A good start is to get visibility over what is connected to these networks and how they communicate. This knowledge can then enable implementation of protection and threat detection solutions to help safeguard these OT environments.

Privileged account visibility

The majority of data breaches are made by using privileged accounts to do lateral movements and data exfiltration. Why? Because it's easy. Many organizations don't have visibility or control over all the highly sensitive accounts. A common estimation is that the number of privileged accounts is about three times the amount of the normal user accounts. Do you have control on who has access to these accounts, how passwords are shared and rotated and what people actually do when they are logged in as administrators? Getting visibility to your current privileged accounts is a first great step of your plan to implement privileged account security.

Conclusion: what's next?

Once you have visibility into your assets and data, investments have to be made across all areas of prevention, detection and response. We predict:

Prevention will shift from 'all-or-nothing' to a risk-based approach.

Critical data, or employees with access to critical data, should have the appropriate protection needed.

Detection will shift from 'standard' to customer specific detections.

Generic rules in a SIEM are not enough to detect smart opponents.

Response will shift from 'oops-help' to a proactive and planned approach.

Mapping your own capabilities and subscribing to external resources will be a priority.

Many organizations do not have the required abilities in the detection and response areas, so we expect that the market for Managed Detection & Response services will continue to grow significantly.

120 private clinics of the Ramsay group targeted in cyber-attack

The attack caused an IT-blackout in Marseille, but was contained by incident response before it could spread[t43].

SEP

Firefox 69 now blocks 3rd-party tracking cookies and cryptominers by default

By enabling enhanced tracking protection by default for all users Mozilla automatically disables popular tracking cookies like Google Analytics and additionally prevents JS cryptominers from running[t44].

Profile of Twitter CEO Jack Dorsey hacked

Twitter disables 'Tweeting via SMS' after hackers had used SIM swapping to claim Dorseys mobile number they had previously got by social engineering an AT&T employee[t45].

Personal details of nearly every Ecuadorian citizen leaked

General manager of IT consulting firm Novaestrat arrested after personal records of pretty much the entire population were left exposed on an unprotected Elasticsearch server[t46].

More than 16 million patient records from 50 countries left unprotected

The records primarily include medical images and scans, e.g. X-rays, MRIs, CT scans, along with personal data like names, addresses and social security numbers. This was no hack, but rather the "normal" way in which such images were stored for years[t48].

Cryptomining botnet Smominru keeps spreading

According to research from Guardicore the malware infects up to 90,000 clients each month and makes use of the EternalBlue vulnerability known from the infamous WannaCry campaign[t47].

OCT

Password cracked after 39 years

The password belongs to Ken Thompson, one of the fathers of the initial UNIX. Even in 2019, the 8-digit password proved unexpectedly hard to crack. It was found to be short code for a chess move: pawn from Queen's 2 to Queen's 4, or "p/q2q4!a" [t49].

Go Sport and Courir Go Sport hit by ransomware

Distribution group and clothing retailers Go Sport and Courir are knocked out of business by ransomware in late October 2019. Stores have to be closed and the payment system is offline for some time [t50].

The Grand Cognac agglomeration refuses to pay ransom

400 computers including main- and backup servers are infected by email, leading to encryption of 10 years worth of internal working documents. The ransom demanded is €180,000 [t51].

M6, one of France's biggest TV channels, hit by ransomware

France's largest privately-owned multimedia group is hit by ransomware. Due to up-to-date cybersecurity any downtimes in radio- or TV channels can be prevented [t52].

InfoTrax detects ongoing breach only after server runs out of storage

Apparently the breach has been ongoing since 2014 but is only discovered after an archive of stolen data the hackers had created threatens to exceed the company's server storage. InfoTrax provides ERP solutions [t55].

Payment solutions giant Edenred admits cyberattack

The company provides solutions for employee benefits, fleet and mobility as well as corporate payment to 50 million customers worldwide. Due to fast response the impact can be kept relatively limited [t54].

T-Mobile US suffers data breach

Threat actors were able to obtain the personal data of over a million customers. Apparently financial information and password data was left unaffected [t56].

DEC

Newly discovered bug lets attackers hijack encrypted VPN connections

CVE-2019-14899 is affecting most Linux and Unix-like operating systems, including FreeBSD, OpenBSD, macOS, iOS, and Android. It could allow remote 'network adjacent attackers' to spy on (and manipulate) encrypted VPN connections [t57].

Rouen hospital turns to pen and paper after cyberattack

Quick action by France's national cyber-crime agency, ANSSI, helps to limit the scale of the ransomware outbreak and bring systems back shortly [t53].

Snatch ransomware reboots windows in safe mode to bypass antivirus

The ransomware uses a manipulated Windows registry key to schedule a service which starts in Safe Mode and proceeds to run the encryption from there. Snatch specifically targets business and government institutions [t58].

NOV

Report summary:

What have we learned?

Etienne Greef
CTO
Orange Cyberdefense

It is always a challenge to write a conclusion following so many interesting facts and opinions. So I will try to highlight what I believe are the key takeaways from this Security Navigator.

To start off I want to look at the basic principle of digital trust. It is a truism that we live in a very connected world. We have numerous interactions with digital and connected systems in every single aspect of our life. These systems do make our life easier and significantly enhance the quality of our lives. But none of this comes without cost. As consumers, our data, choices, behaviours and interactions with others have become a commodity to be used for good and unfortunately bad at times. I don't believe that most of us made a conscious decision to give free access to our personal data and in effect our lives when we started interacting and using the various online and electronic systems. In other words when we started enjoying the benefits of technology, we didn't fully consider the potential downsides. As this report so vividly illustrates, our data is often compromised, traded and used in ways we never anticipated.

I don't make an argument for not using technology, but I do believe that companies have to up their game and take proper responsibility for the data we entrust them with. I believe that the cybersecurity industry today as a whole is not delivering on the promise of ensuring trust to its customers. Despite the fact that spending is increasing, we are experiencing bigger and bigger breaches more frequently. In a sense there is breach fatigue with most people almost shrugging their shoulders at the latest breach reports.

The news cycle is dominated by big breaches but lessons are often not learned. Our industry is dominated by technology with technology vendors offering more and more solutions to solve essentially the same problem. In my opinion there is not enough focus on understanding risk, looking for potential breaches and building a robust response and recovery capability.

In order to improve the situation from a preventative point of view I want to focus on four basic areas, areas that have been discussed throughout the report.

1 Changing human behaviour

This is often the underinvested part of cybersecurity.

Cyberdefense starts and ends with our users. Our users are often perceived to be the weakest link but they can be our strongest ally, acting as intelligent human sensors. If there is a single bit of advice I would give the typical CISO, it will be to educate and empower their users and to stop regarding them as victims.

2 Focus on authentication and authorization

With the number of compromised user passwords equivalent to half of the population on earth it is clear that only using passwords is simply not good enough. Strong authentication should be a must and should be as transparent and easier to use than passwords. I believe the time has come to put passwords to rest. Beyond passwords it is also important to focus on authorization and put into practice the principle of least privilege. Our ethical hackers love a user account with admin privilege or an admin account with the same password as a user.

3 Putting barriers inside networks

One of the most basic principles of network security is that of zones of trust. A zone of trust is basically grouping together devices or data with a similar level of trust. A lot of companies have a single zone of trust with few barriers inside the network. What is surprising with a lot of compromises isn't the fact that companies have compromises. It is the fact that once compromised, hackers can roam freely within the target network.

4 Understanding your attack surface and vulnerabilities

Hacking is almost never as advanced as the press would lead us to believe. In most cases the vulnerabilities exploited are old and well understood. There is a lot of evidence pointing to the fact that the average age of a vulnerability exploited in major attacks is 90 days. In a lot of recent compromises the miscreants didn't even need to exploit a vulnerability. All they had to do was download a database from a public server without any password. If companies spent as much time trying to understand their attack surface and vulnerabilities as they do trying to implement the latest technological security fad, our report would be much shorter. A well-structured vulnerability management program coupled with a detailed understanding of your environment and where data lives will increase the level of your security exponentially.

We certainly live in interesting times with the COVID-19 pandemic bringing about unprecedented business transformation. The pace of the transformation has been astonishing to say the least with most businesses completely transforming the way they work within a matter of weeks. Obviously this transformation has created some new challenges with regards to security. But one could argue they are not that new after all. Remote work has been a reality for quite some time. The new massive shift to home-office and cloud infrastructure has only strengthened the demand for visibility with the perimeter now truly in every employee's home.

With the classic perimeter gone, smart solutions must be implemented to prevent, detect and respond to threats. It is also important to consider what happens when we go back to work with a number of devices that have not enjoyed the protection of enterprise security re-joining our enterprise networks.

I want to conclude by saying that presently cybercrime does pay, and it pays handsomely. As is discussed in the report, hackers are often paid ransoms and in particular where there is cyber insurance in place. Hackers receiving six figure rewards for hacking is feeding the criminal ecosystem and will most likely lead to a marked increase in hacking activity. In my mind this is the biggest single change in our cybersecurity world during 2019. Criminals are able to monetize their craft using more and more sophisticated tools, often developed by governments. This is worrying and means that businesses have to assume they will become a target at some stage. As Stefan Lager said we need to focus as much attention on understanding our risk, detecting issues, response and recovery as we do on protecting our assets.

Google announces new Patch Rewards Program to encourage open-source security projects

The program includes rewards after completion, combined with upfront financial support to provide an additional resource for open source developers to prioritize security work [t59].

2020 Timeline ▸

Contributors, sources & links

Sources

This report could not have been created without the hard work of many researchers, journalists and organizations around the world. We've gratefully used their online publications for reference or context.

Statistics and numbers

All statistics originate from Orange Cyberdefense's CyberSOCs

Story: The Fondation du Patrimoine and the Notre-Dame fire

[1.1] https://www.zdnet.fr/actualites/notre-dame-de-paris-elan-de-solidarite-et-arnaques-en-tout-genre-39892077.htm

[1.2] Letter dated July 12, 2019 from Mr. Guillaume Poitrinal, President of the Fondation du Patrimoine to Orange Cyberdefense

CyberSOC statistics

[2.3] https://coinmarketcap.com/currencies/monero/

[2.4] https://coinmarketcap.com/currencies/ethereum/

[2.5] https://coinmarketcap.com/currencies/litecoin/

[2.6] https://coinmarketcap.com/currencies/bitcoin/

[2.7] https://www.biznesstransform.com/transforming-the-food-and-beverage-industry-with-digital-technologies/

Databreaches on the rise

[4.1] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

[4.2] https://www.lowyat.net/2019/177033/over-1-million-uitm-students-and-alumni-personal-details-leaked-online

[4.3] https://www.cnn.com/2019/01/28/health/hiv-status-data-leak-singapore-intl/index.html

[4.4] https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

[4.5] https://thehackernews.com/2019/02/data-breach-website.html

[4.6] https://thehackernews.com/2019/02/data-breach-sale-darkweb.html

[4.7] https://www.todayonline.com/singapore/personal-data-808000-blood-donors-compromised-nine-weeks-hsa-lodges-police-report

[4.8] https://thehackernews.com/2019/03/data-breach-security.html

[4.9] https://www.upguard.com/breaches/facebook-user-data-leak

[4.10] https://www.businessinsider.com/facebook-uploaded-1-5-million-users-email-contacts-without-permission-2019-4

[4.11] https://economictimes.indiatimes.com/tech/internet/data-breach-at-justdial-leaks-100-million-user-details/articleshow/68930607.cms

[4.12] https://www.vpnmentor.com/blog/report-millions-homes-exposed/

[4.13] https://www.analyticsindiamag.com/data-breach-truecaller-exposes-indian-users-data-shows-cracks-in-cyber-security-infrastructure/

[4.14] https://gizmodo.com/885-million-sensitive-records-leaked-online-bank-trans-1835016235

[4.15] https://www.cisomag.com/nearly-140-million-user-data-leaked-in-canva-hack/

[4.16] https://finance.nine.com.au/business-news/westpac-data-breach-100000-australian-customers-at-risk/84c91581-90b6-464e-9137-a2d973492614

[4.17] https://www.theguardian.com/australia-news/2019/jun/04/australian-national-university-hit-by-huge-data-breach

[4.18] https://www.publishedreporter.com/2019/06/05/nearly-12-million-quest-diagnostics-patients-medical-info-exposed-in-new-data-breach/

[4.19] https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297

[4.20] https://www.reuters.com/article/us-bulgaria-cybersecurity/hackers-steal-millions-of-bulgarians-financial-records-tax-agency-idUSKCN1UB0MA

[4.21] https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

[4.22] https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/

[4.23] https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet

[4.24] https://www.vpnmentor.com/blog/report-ecuador-leak/

[4.25] https://www.upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure

[4.26] https://japan.cnet.com/article/35143123/

[4.27] https://techcrunch.com/2019/09/26/doordash-data-breach/

[4.28] https://venturebeat.com/2019/09/30/words-with-friends-player-data-allegedly-stolen-for-218-million-users/

[4.29] https://www.worldometers.info/world-population/

[4.30] https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

[4.31] https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

The PKI and digital trust

[6.1] https://docs.microsoft.com/en-us/windows/win32/seccertenroll/about-certification-authorities

[6.2] https://www.bloomberg.com/profiles/companies/108453Z:SS-addtrust-ab

[6.3] http://web.archive.org/web/20110128085641/http://www.addtrust.com/

[6.4] https://en.wikipedia.org/wiki/Certificate_authority

[6.5] https://www.xolphin.com/support/Rootcertificates/Phasing_out_Addtrust_External_CA_Root_certificate

Security Predictions

[7.1] https://towardsdatascience.com/google-has-cracked-quantum-supremacy-cd70c79a774b

Timeline

[t1] https://www.avanan.com/resources/zwasp-microsoft-office-365-phishing-vulnerability

[t2] https://www.justice.gov/usao-ma/pr/jury-convicts-man-who-hacked-boston-childrens-hospital-and-wayside-youth-family-support

[t3] https://www.safetydetectives.com/blog/major-security-breach-discovered-affecting-nearly-half-of-all-airline-travelers-worldwide/

[t4] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

[t5] https://www.reuters.com/article/us-altran-tech-cyber/frances-altran-tech-says-it-was-hit-by-cyber-attack-idUSKCN1PM0IJ

[t6] https://www.carbonblack.com/2019/01/24/carbon-black-tau-threatsight-analysis-gandcrab-and-ursnif-campaign/

[t7] https://www.reuters.com/article/us-airbus-cyberattack-report/hackers-tried-to-steal-airbus-secrets-via-contractors-afp-idUSKBN1WB0U9

[t8] https://thehackernews.com/2019/02/cryptocurrency-exchange-exit-scam.html

[t9] https://blog.zimperium.com/dont-give-me-a-brake-xiaomi-scooter-hack-enables-dangerous-accelerations-and-stops-for-unsuspecting-riders/

[t10] https://thehackernews.com/2019/02/vfemail-cyber-attack.html

[t11] https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/ , https://thehackernews.com/2019/02/data-breach-sale-darkweb.html

[t12] https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=20190303005031

[t13] https://blog.mozilla.org/blog/2019/03/12/introducing-firefox-send-providing-free-file-transfers-while-keeping-your-personal-information-private/

[t14] https://thehackernews.com/2019/03/data-breach-security.html

[t15] https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

[t16] https://www.reuters.com/article/us-norsk-hydro-cyber/aluminum-producer-hydro-hit-by-cyber-attack-shuts-some-plants-idUSKCN1R00NJ

[t17] https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

[t18] https://cafe.bithumb.com/view/board-contents/1640037

[t19] https://www.upguard.com/breaches/facebook-user-data-leak

[t20] https://www.reuters.com/article/us-bayer-cyber/bayer-contains-cyber-attack-it-says-bore-chinese-hallmarks-idUSKCN-1RG0NN

[t21] https://securelist.com/project-tajmahal/90240/

[t22] https://medium.com/@fs0c131y/tchap-the-super-not-secure-app-of-the-french-government-84b31517d144

[t23] https://blog.malwarebytes.com/cybercrime/2019/04/electrum-ddos-botnet-reaches-152000-infected-hosts/

[t24] https://vaaju.com/franceeng/fleury-michon-stopped-production-for-five-days-due-to-a-computer-virus/

[t25] https://www.vpnmentor.com/blog/report-millions-homes-exposed/

[t26] https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

[t27] https://thehackernews.com/2019/05/baltimore-ransomware-cyberattack.html

[t28] https://www.lemondeinformatique.fr/actualites/lire-le-site-des-aeroports-de-lyon-cible-par-une-cyberattaque-75489.html

[t29] https://morphuslabs.com/goldbrute-botnet-brute-forcing-1-5-million-rdp-servers-371f219ec37d

[t30] https://labs.bitdefender.com/2019/06/good-riddance-gandcrab-were-still-fixing-the-mess-you-left-behind/

[t31] https://moneyandpayments.simonl.org/2019/06/perspectives-on-ca-libra-1-first-we-get.html

[t32] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

[t33] https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

[t34] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-internation-al-inc-more-than-99-million-under-gdpr-for-data-breach/

[t35] https://thehackernews.com/2019/07/ransomware-nas-devices.html

[t36] https://www.zdnet.com/article/kazakhstan-government-is-now-intercepting-all-https-traffic/

[t37] https://twitter.com/CityPowerJhb/status/1154277777950093313

[t38] https://research.checkpoint.com/say-cheese-ransomware-ing-a-dslr-camera/

[t39] https://www.ecb.europa.eu/press/pr/date/2019/html/ecb.pr190815~b1662300c5.en.html

[t40] https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/

[t41] https://thehackernews.com/2019/08/dds-safe-dental-ransomware-attack.html

[t42] https://www.theregister.co.uk/2019/08/21/kazakstan_snooping_blockade/

[t43] https://www.tellerreport.com/life/2019-08-13---the-120-hospitals-of-the-ramsay-health-group-in-france-victims-of-a-cyber-attack-.rJQ3yHqg4r.html

[t44] https://blog.mozilla.org/blog/2019/09/03/todays-firefox-blocks-third-party-tracking-cookies-and-cryptomining-by-default/

[t45] https://thehackernews.com/2019/09/tweet-via-sms-text-message-hacking.html

[t46] https://www.vpnmentor.com/blog/report-ecuador-leak/

[t47] https://www.guardicore.com/2019/09/smominru-botnet-attack-breaches-windows-machines-using-eternalblue-exploit

[t48] https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet

[t49] https://thehackernews.com/2019/10/unix-bsd-password-cracked.html

[t50] https://www.lemondeinformatique.fr/actualites/lire-go-sport-et-courir-victimes-d-un-ransomware-77403.html

[t51] http://www.leparisien.fr/societe/cyberattaque-l-agglomeration-grand-cognac-refuse-de-payer-la-ran-con-31-10-2019-8183676.php

[t52] https://www.zdnet.com/article/m6-one-of-frances-biggest-tv-channels-hit-by-ransomware/

[t53] https://www.bbc.com/news/technology-50503841

[t54] https://www.bleepingcomputer.com/news/security/edenred-payment-solutions-giant-announces-malware-incident/

[t55] https://thehackernews.com/2019/11/hacking-file-storage.html

[t56] https://www.techradar.com/news/over-a-million-t-mobile-customers-hit-in-data-breach

[t57] https://thehackernews.com/2019/12/linux-vpn-hacking.html

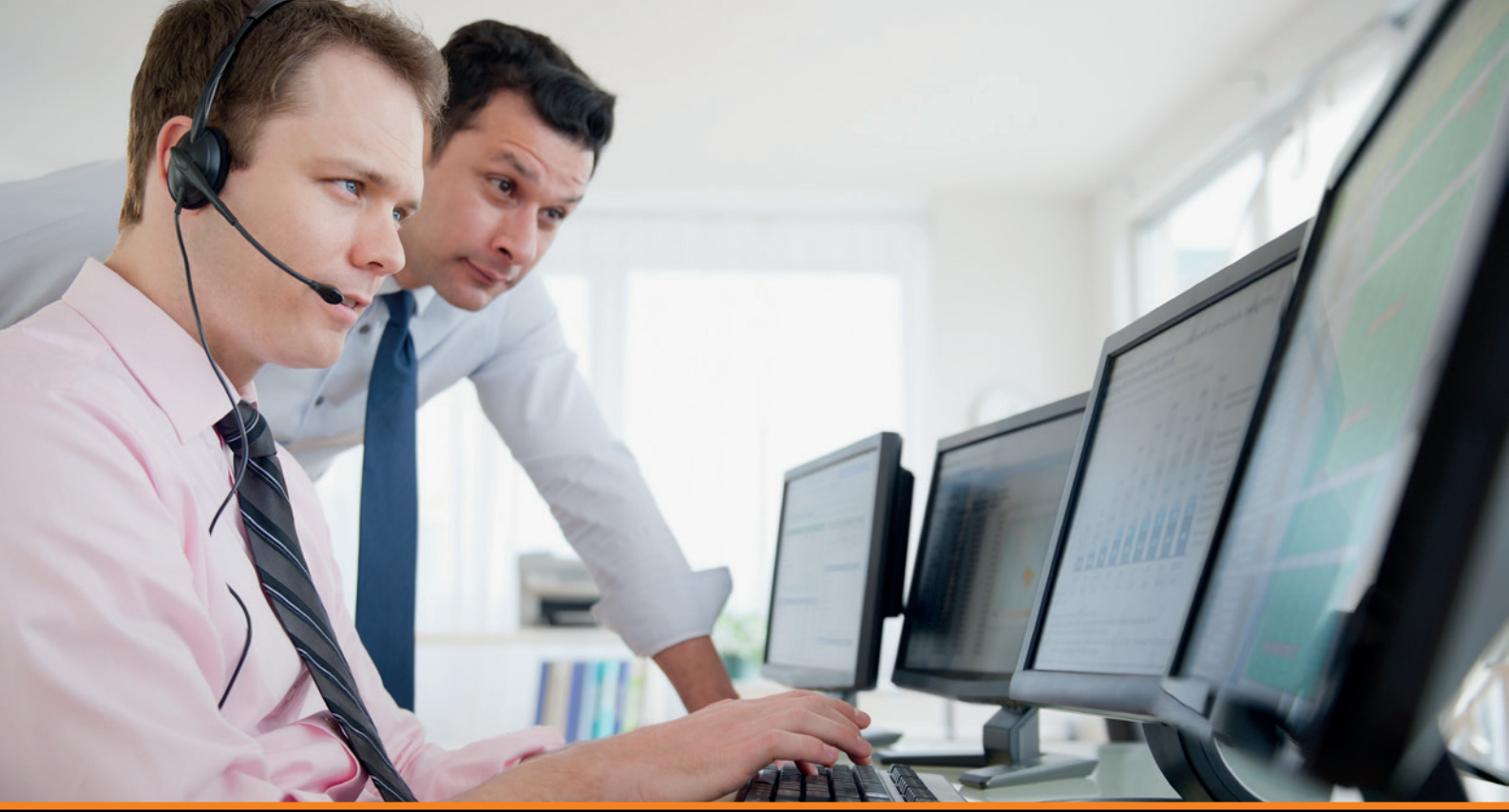
[t58] https://www.zdnet.com/article/snatch-ransomware-reboots-pcs-in-windows-safe-mode-to-bypass-antivirus-apps/

[t59] https://security.googleblog.com/2019/12/announcing-updates-to-our-patch-rewards.html

Disclaimer

In case of emergency you can reach our CSIRT team via your countries hotline 24/7! Find your countries hotline at **orangecyberdefense.com!**

A very special thanks to all cyber hunters, analysts and engineers in our SOCs.



Why Orange Cyberdefense?

Cybersecurity specialists
Orange Cyberdefense specializes in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our services are delivered by our 10 CyberSOCs and 16 SOCs worldwide, delivering immediate, 24x7x365 access to specialists who will deal with incidents and ensure continuous availability.

Vendor insights
Our close partnership with numerous vendors provides superior access to their technical experts and product roadmaps – keeping our Cyber SOC's knowledge ahead of the game.

Extensive security insight
Orange Cyberdefense's Greater Intelligence platform processes over 50 billion events per month, giving us unparalleled access to current and emerging threats. Our elite consulting team is at the forefront of cybersecurity – providing insight into the criminal mindset. We use this information to ensure that our customers are as secure as they possibly can be.

www.orangecyberdefense.com