2019
Annual Security Report

Secure Link
Part of Orange Cyberdefense

SAFELY ENABLING BUSINESS

The data for this report has been extracted by analyzing more than 260,000 incidents in our own Cyber Defense Centers across Europe. Our experts have studied these findings to bring you conclusions that will help you better understand the 2019 cyber security landscape.

Welcome to the second Annual Security Report published by SecureLink.

Information overflow is one of the key problems in the digital age. So why publish another report? Why read it? What do you get out of it?

The short answer: this is information you need.

Cyber security is crucial to you, because your business, and your job, depends on it. The facts you can find in this report cannot be found anywhere else. The data for this report has been extracted by analyzing more than 260,000 incidents in our own Cyber Defense Centers across Europe. Our experts have studied these findings to bring you conclusions that will help you better understand the 2019 cyber security landscape. Once again our best engineers and researchers have torn up elaborate malware samples, extracted indicators of compromise and endured the dangers of the darknet for you. We do this to help you prepare for the future.

However, this is not just about business. For instance: even before a tremendous leak of healthcare data affecting about 16 million datasets from 50 countries was discovered in September, we had already investigated the availability of such data in darknet markets. You can read a summary of what we found in its own chapter in the report.

Throughout the report you will find statistical data obtained from real world incidents, a timeline of remarkable cyber-related events which happened throughout the year, and several more feature articles written by authorities in their respective domain.

This report is dedicated to our faithful customers. Without your trust in us to defend your most valuable digital assets and to route terabytes of data through our various defense systems, this report would not have been possible. So ultimately this report is for you. Thank you!

The SecureLink Team

Table of Contents

2019 Timeline

Franz Härtl
Marketing Manager
SecureLink

Cyber Defense Center 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 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 five cyber defense centers. Once again we have decided to delve into this and extrapolate the figures required to get a better understanding of the ever-evolving threat landscape.

As a result, we can now share with you a very real, first-hand picture of the events and trends over the past year.

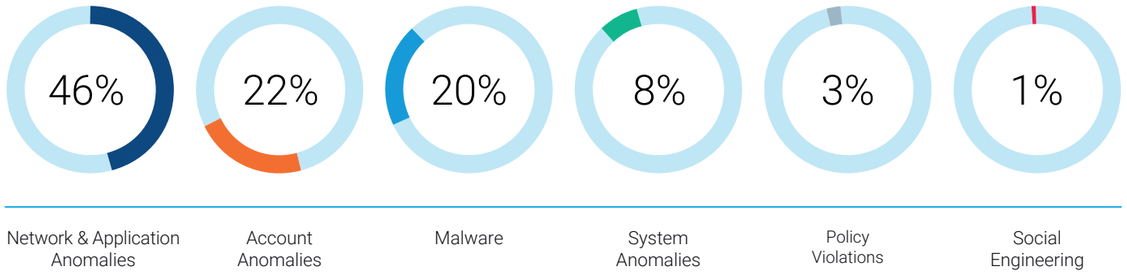
About the data

- Grand total of events analysed: 263,109
- Out of these events, 11.17% (29,391) are considered security incidents by SecureLink data classifications.
- Period analyzed: ten months commencing January 1, 2019.
- If data from the final two months of 2019 break existing trends, an addendum will be released in February 2020.
- Data sources: firewalls , directory services, proxy, endpoint, EDR, IPS, DNS, DHCP, SIEM and our SecureDetect platform.

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 2018 Annual Security 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. Last year, this rate was 8.31%, which means we saw an increase of 38%. 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 the ongoing effort of our engineers and analysts to eliminate false positives in collaboration with our customers. But it also shows that the heat is still on. Attackers will take any opportunity to exploit a weakness.

Have you been Pwned?

Another trend we consider significant is the increase of Account Anomalies. Last year 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 keyword 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.

Social engineering remains hard to detect

As mentioned last year, 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.

JAN

Z-WASP allows hackers To bypass Office 365 e-mail protection

Researchers at Avanan successfully use 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].

Endpoint protection works

Another noteworthy change we observed is that malware related incidents had the most impact last year with a share of 45%, compared to Network & Application Anomalies which ranked second with 36% at the same time. This has fundamentally changed, with malware declining to 20% while Network & Application anomalies have increased to 46%.

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-gen preventive endpoint protection. And we see the results quite clearly: malware rapidly loses its tooth 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.

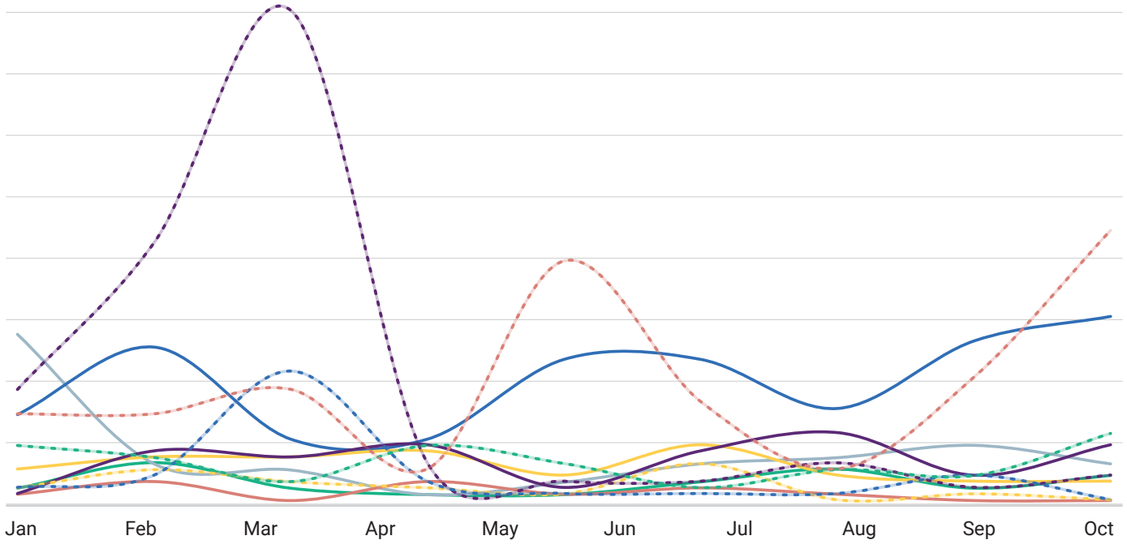
Malware Trends

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 and the end of July. The latter is likely due to a trend we already observed during 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 also explain the drop in April, when attacks slowed due to an early Easter holiday.

Another difference in comparison to previous years, is the new rise of attacks considered "old school" like trojans and classic viruses. This was most noticeable at the beginning of the year.

As shown in our research from last year, Ransomware has its highs and lows. What is interesting is the repeated correlation with Cryptocurrency miners. 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 a new peak in May/June. 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.

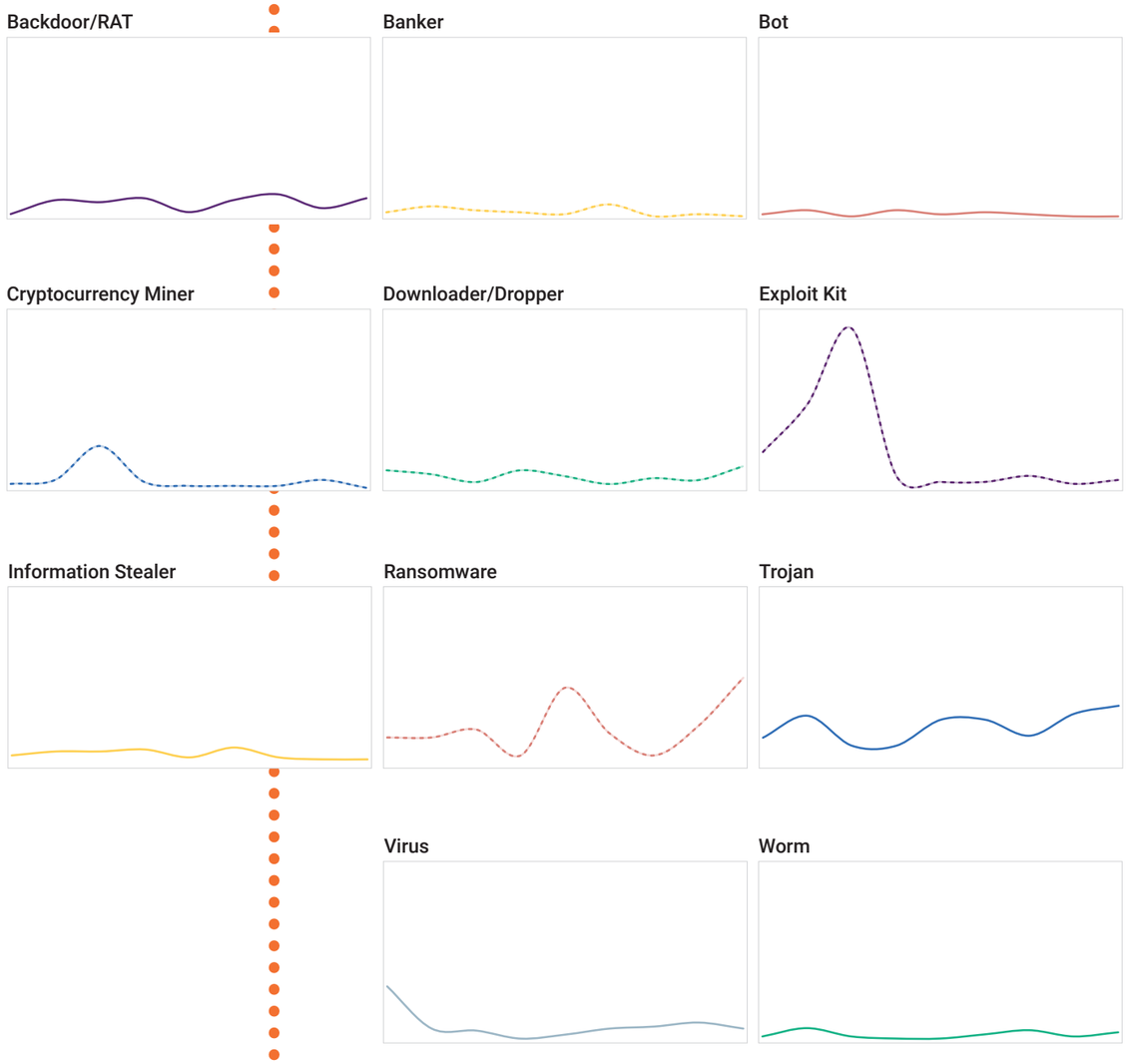


Hacktivist sentenced to 10 years for DDoSing hospital

Martin Gottesfeld attacked several institutions, but most notable was his 2014 attack against the Boston Children's Hospital using a botnet of 40,000 routers. He allegedly did this to protest the abusive treatment of Justina Pelletier[t2].

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 (PNR) as well as flight details, names and other personal info[t3].



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

Australian researcher Troy Hunt discovers a massive collection of credential records (e-mail addresses & passwords). The records originate from several different data breaches[t4].

Bing "accidentially" blocked in China

MS search engine Bing is blocked for two days by the "Great firewall of China", in spite of censoring its search results. According to "sources" this was due to a technical error[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 e-mails with malicious Word-attachments[t6].

xDedic shut down by Police

Law enforcement from the US and Europe shut down xDedic market, mainly trading remote access to hacked computers and servers as well as stolen personal information[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 was the CEO and founder, Gerry Cotton, who unexpectedly died in December 2018[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 trigger the break, accelerate or shut down the scooter from up to 100m away[t9].

Organization size

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

A significant shift has occurred when it comes to medium and large organizations. Last year we found large companies 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.

What we saw this year is a dramatic rise in attacks on medium -sized businesses. 2019, we tracked 31% of the incidents here, which is a significant increase from last year's 19%. At the same time, incidents in large organizations dropped from 73% to 58.8%.

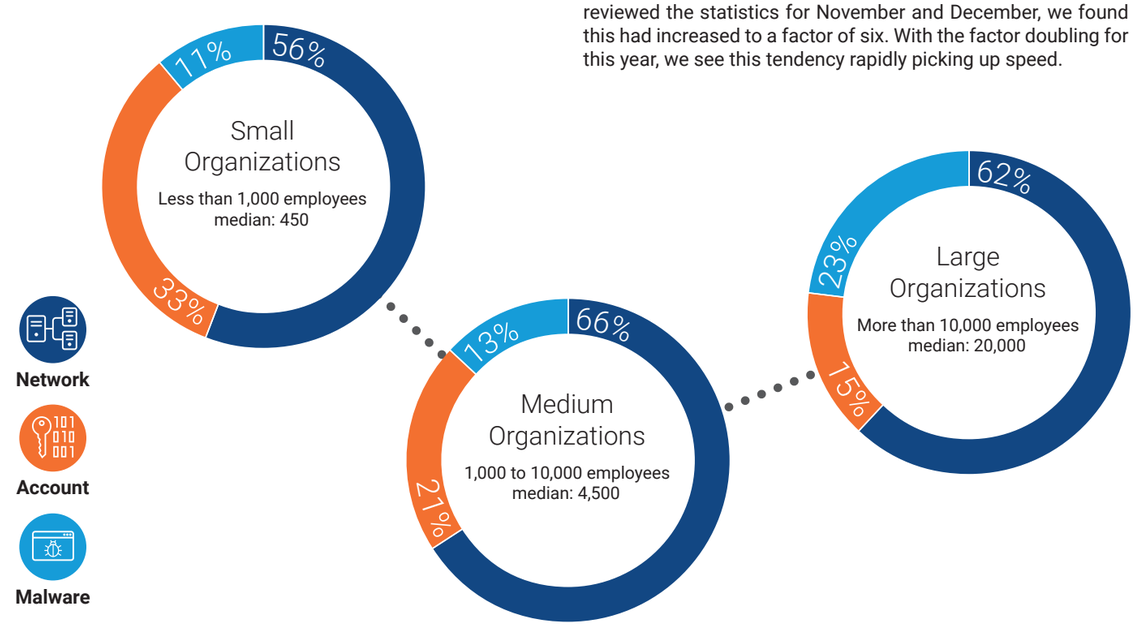
Apparently threat actors have massively shifted their focus, now targeting medium-sized businesses with 1,000-10,000 employees, much more than the big players.

Types of incidents versus business size

We see the same tendency as in the averages of the funnel on page 8. The major change in comparison to 2018 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 (33% as compared to 21%/15%) and large ones still have to fend off almost twice as many malware attacks as smaller ones.

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 twelve times higher than in large organizations. This is confirming a trend we observed last year. By October we found the incidents per head in small businesses four times higher than for large ones, and by the time we reviewed the statistics for November and December, we found this had increased to a factor of six. With the factor doubling for this year, 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 twelve times higher than in large organizations.

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

SMALL ORGANIZATIONS	MEDIUM ORGANIZATIONS	LARGE ORGANIZATIONS
18.5	4.3	1.6

Criticality

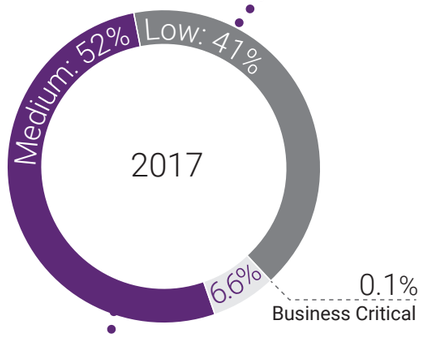
Incidents are not equal. At SecureLink, we have defined four levels:

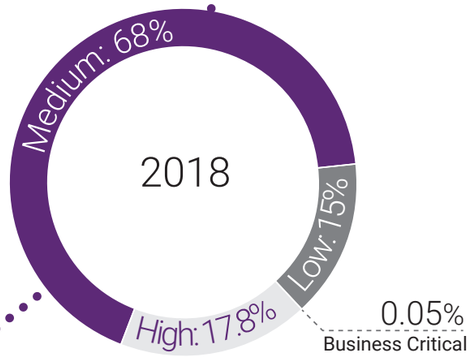
- **Business critical:** Critical business impact, business processes grinding to a halt
- **High:** Significant business impact, incidents that must be handled immediately
- **Medium:** Limited business impact, acceptable workarounds may exist
- **Low:** Minimal business impact, does not significantly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

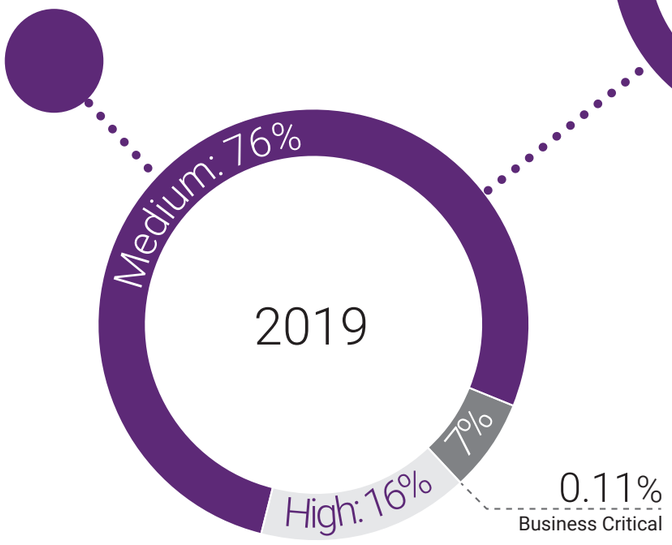
	Business Critical	High	Medium	Low
2016	0.50%	8.2%	53%	38%
2017	0.10%	6.6%	52%	41%
2018	0.05%	17.8%	68%	15%
2019	0.11%	16%	76%	7%

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. In this regard we are actually back to the status of 2017.







Secure e-mail provider VFE-mail.net wiped

In a catastrophic security breach hackers completely destroy all data on both primary and backup servers. This includes the entire infrastructure with e-mail hosts, virtual machine hosts and an SQL server cluster. The attack is purely destructive in nature, apparently there was no ransom demand or data theft[t10].

Hacker sells 839 million accounts in the darknet

Hacker “Gnosticplayers” publishes 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].

MAR

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 credit the campaign to the North Korean state sponsored Lazarus group[t12].

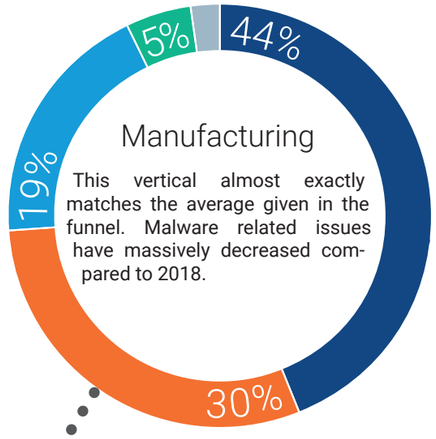
Incidents in different verticals

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 large amounts 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.

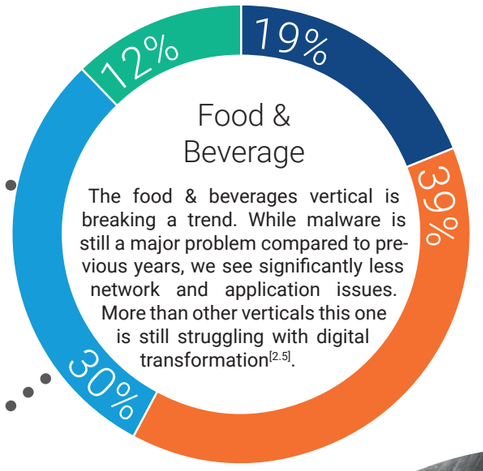
You can find more on the maturity of different verticals in the Security Maturity Report we published earlier this year. More details on *https://securelink.net/sma/*

	Network	Account	Malware	System	Policy	Social
Business Services	59.64%	23.57%	11.67%	4.67%	0.30%	0.15%
Financial Services	43.81%	25.90%	12.59%	5.97%	0.06%	11.66%
Manufacturing	44.40%	30.45%	18.97%	4.67%	1.49%	0.02%
Food & Beverages	18.59%	39.15%	29.86%	12.11%	0.00%	0.28%
Government/Public	37.87%	53.85%	5.33%	2.07%	0.89%	0.00%
Healthcare	83.97%	3.79%	10.00%	2.02%	0.04%	0.18%
Education	52.50%	37.50%	1.25%	1.25%	6.25%	1.25%
Biotechnology	44.66%	45.02%	5.69%	4.63%	0.00%	0.00%
Retail	33.74%	16.77%	29.97%	12.43%	5.81%	1.28%



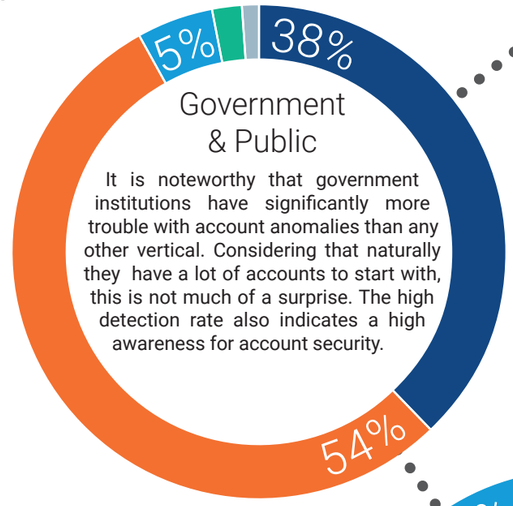
Manufacturing

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



Food & Beverage

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].

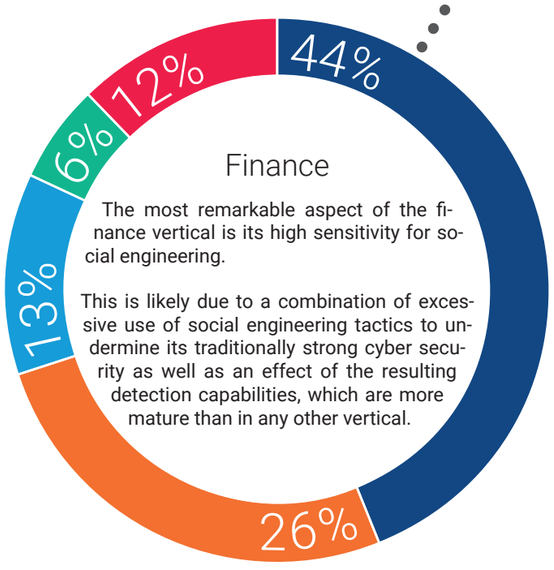


Government & Public

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

Business services

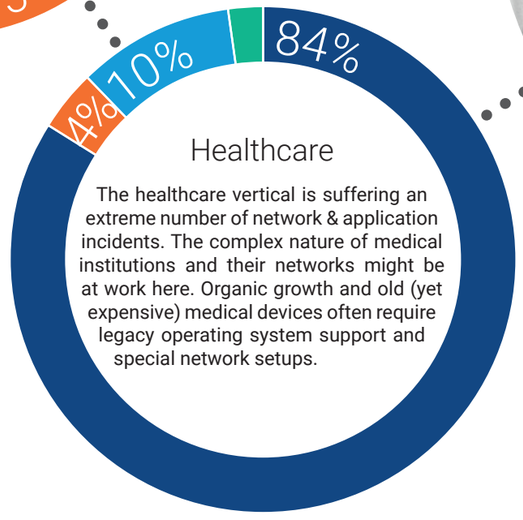
We find this vertical closely matches the profile observed for organizations with up to 1,000 employees.



Finance

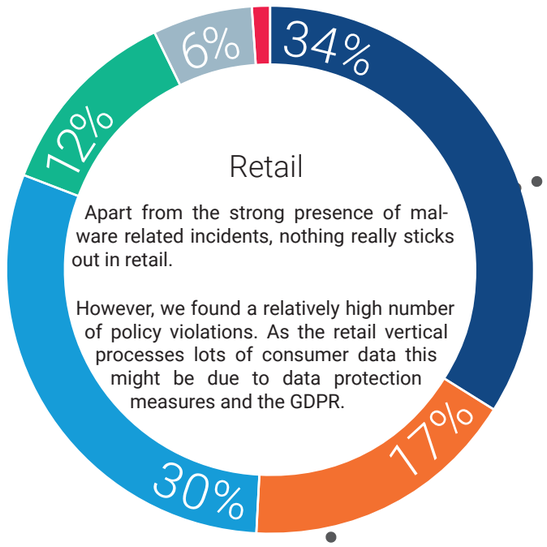
The most remarkable aspect of the finance vertical is its high sensitivity for social engineering.

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

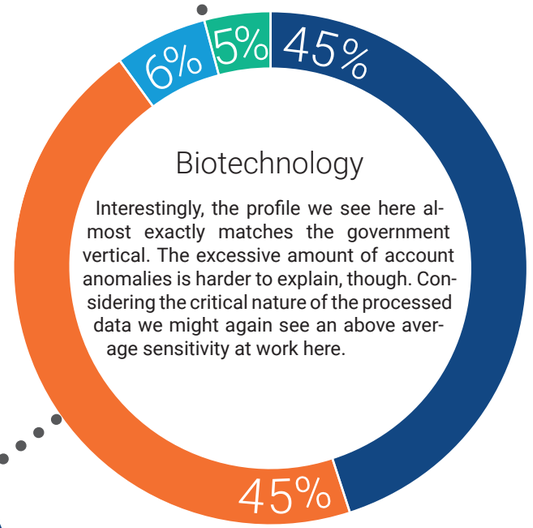
The healthcare vertical is suffering an extreme number of network & application incidents. The complex nature of medical institutions and their networks might be at work here. Organic growth and old (yet expensive) medical devices often require legacy operating system support and special network setups.



Retail

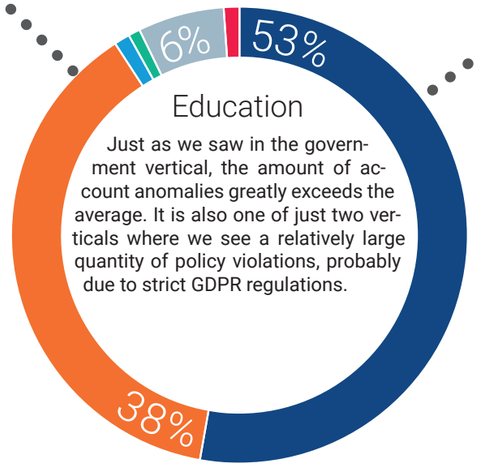
Apart from the strong presence of malware related incidents, nothing really sticks out in retail.

However, we found a relatively high number of policy violations. As the retail vertical processes lots of 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 elimination of false positives, but it also shows that threat actors are still on our heels.

In 2018 the major source of incidents was malware, accounting for almost half of the attacks we had detected in our cyber defense centers. Network & application anomalies came in second with a difference of 10% between the two.

This year network related incidents take the crown. Due to many of our customers implementing the newest generation of endpoint protection, malware rapidly loses in relevance, ending up ranked third after account anomalies.

This is a good thing, as some of the most devastating attacks in the past have been malware related.

It is also noteworthy that the increase in prices of Bitcoin, Monero and other cryptocurrencies apparently did not inspire new waves of cryptomining.

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].

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

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

Mirai is back

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

Norsk Hydro shuts down global network due to ransomware attack

Several plants in different countries have 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].

Electrum wallet infection rapidly spreads, steals $4.6 million

The attack consists of a group of hacked servers pretending to be part of the Electrum peer network. These respond with a falsified error message to legitimate requests, tricking Elektrum Wallet apps to download a malicious update which then steals wallet funds and additionally contains a botnet infection which is used to DDoS legitimate Electrum servers[t23].

French government chat "Tchap" hacked

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

Bayer detects Winnti in their network

Multinational chemical corporation Bayer fell victim to an elaborate, long-term infiltration attempt hosted by renowned Chinese APT group "Wicked Panda" using Winnti. Bayer claims no actual data has been stolen[t20].

TajMahal: New APT framework discovered

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

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].

Bithumb hacked [again]: $19 million stolen

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

Paul van der Haas
Lead Engineer Operations SLI
SecureLink

Thomas Eeles
CSIRT Manager
SecureLink

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

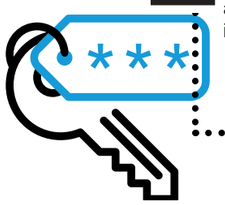
A new assignment arrived from a customer, one with specific objectives: identify vulnerabilities on the internal network and proceed to exploitation and penetration further into the network. A typical assignment but permission was granted to exploit and explore; something we do well.

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

1 Scan

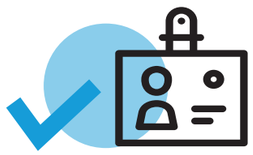
The coffee was still warm, the scans were still running, and a member of our team declared he'd already discovered a web application that looked like an administration portal for the customer's Active Directory.

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



2 Login with default credentials

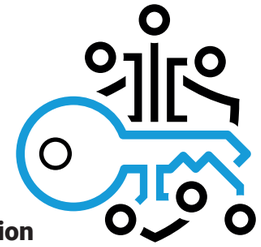
Finish your coffee, pack the laptop away, there is a new domain admin in the house!



3 Gaining privileged access

As you might have guessed, it was possible to login 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.

PGP implementations severely flawed

Until E-Fail OpenPGP and S/MIME seemed to provide a good level of security in business communication. Researchers now uncover severe flaws in the implementations in Thunderbird, Microsoft Outlook, Apple Mail with GPGTools, iOS Mail, GpgOL, KMail, Evolution, MailMate, Airmail, K-9 Mail, Roundcube and Mailpile[t24].

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 SecureLink handle unprecedented levels of cyber security incidents. A steady flow of Microsoft Office 365 e-mail 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 chapter 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 centralised 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.

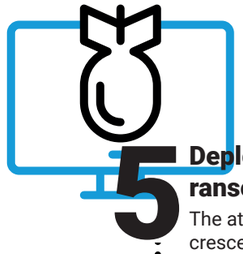
Worrying on its own, this gets terrifying when you factor in that the local admin password was the same on every endpoint of the network, including servers and hypervisors.

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.



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 loan ".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.

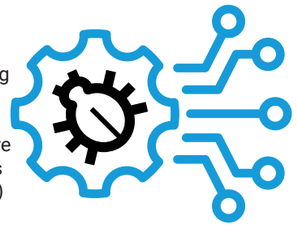
6 Recovery

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

Against all advice from SecureLink, the client payed 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.

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.



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.

Story 3: A delicate e-mail 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 e-mail and file shares, with Microsoft Office 365 (O365) taking the lion's share of e-mail 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 e-mail hack.

To keep the PG rating of this report, all I will say is spam e-mails 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 e-mails held within the client's O365 environment.

Did they foreward or download a copy of any of these e-mails? 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 organizations 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 e-mail and password combo for both LinkedIn and their corporate e-mail.

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 databreach

We could see from timestamps that the attack was automated. The time delay from the time of access to the time of the first e-mails being sent was just a few seconds, and the volume of e-mails 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 e-mails being synched or downloaded, nor did we identify any forwarding rules across any of the affected accounts.

7 Recovery

All we could see where hundreds of e-mail accounts were being accessed, then sending out millions of top-shelf e-mails that swiftly got deleted.

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

Lessons learned

As with the first story, some free changes could have been made to the setup to stop this early. Users tend to access e-mails from the same devices, and same IP addresses (at least the same country IP block), so alerting on e-mail access from abnormal IP addresses is a great tool for early warnings. Especially if you can then corelate 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 are 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 vs the week or two of effort to get it set up. No doubt about it, everyone should be using 2FA.

So there you have it, two 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.

Mysterious database found containing data on 80 million U.S. citizens

Known hacktivists Noam Rotem and Ran Locar discover an unprotected database impacting up to 65% of U.S. households, hosted by a Microsoft cloud server. It is yet unknown who owns this database or what purpose it serves[t25].

Franz Härtl
Marketing Manager
SecureLink

What really disrupted Europe

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..

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? This year may not be an olympic year, but it will be remembered as a year of record breaking data breaches!

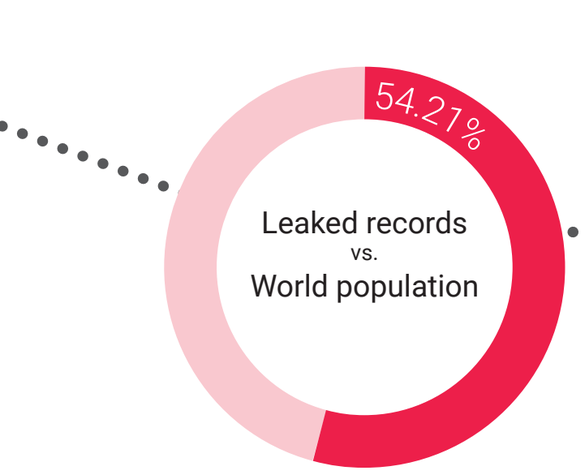
Timing is everything

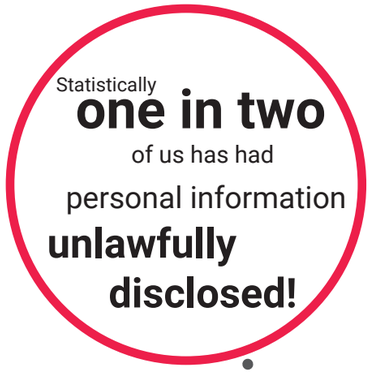
Time, and the lack of it, is always a crucial factor when managing data breaches. Many breaches are only discovered years after they first occurred. On occasion data breaches are even committed over a number of months or even years before being detected. More often than not, organizations are informed of their breach by authorities or security researchers discovering data linking 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 it actually got leaked and when.

Billions not millions impacted

An eyewatering 4,174,339,740 leaked datasets have been discovered throughout 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 the year, an increase of almost 54% as compared to the same time last 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 e-mail-adresses 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 databreaches, often without even knowing it.

Databreaches by number of records[4.30]

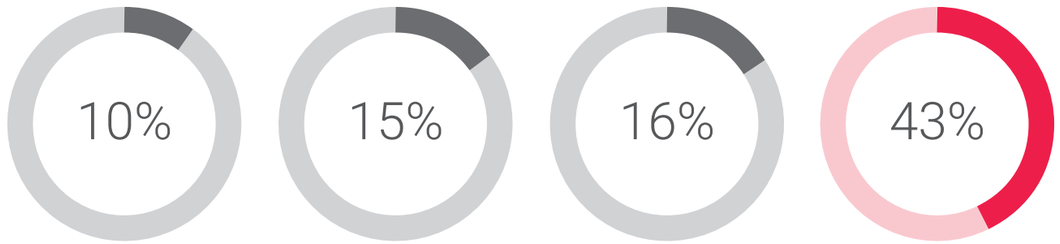
Why climb the tree...

... 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, webservices 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 databreaches 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)	Mrz 15	808,000	poor security	[4.7]
GnosticPlayers, Round 4	Mrz 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	Mai 22	299,055,000	unknown	[4.13]
First American Corporation	Mai 24	885,000,000	poor security	[4.14]
Canva	Mai 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.

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.

Diana Selck-Paulsson
Threat Research Analyst / TDMC
SecureLink

Databreaches in healthcare

A VISIT TO DR. BLACKHAT

Why healthcare data is so attractive to cybercriminals

Targeted cyberattacks against various industries have become increasingly common in recent years. The healthcare sector is no exception. In 2015, this reached its peak, especially affecting United States (U.S.) based healthcare companies, with more than 113.27 million records being exposed.

In September, it was discovered that 16 million datasets of medical images like x-rays and MRT scans, along with the accompanying personal data (name, address, date of birth), had been commonly available for years on unprotected servers.

According to a study that collected data on breaches between 2010 and 2017, 2,149 breaches were reported to the US Health and Human Services Office for Civil Rights with a total amount of 176,4 million compromised health records (McCoy TH, Perlis RH, 2018).

Digitization with side effects

The healthcare sector, as any other vertical, is undergoing immense changes towards digitalization. The intent of the industry is to increase information sharing and collaboration for better patient care. The side effect is an extended attack surface.

Knowledge and awareness, as well as budget, are not always sufficient for securing health data and addressing security issues.

Critical conditions for data

Health data is a very special kind of data. It can be used, and abused, for many purposes due to the variety of information within one health record. Attackers could leverage the PII data, the financial data or the medical history part of the record for purposes like fraud, identity theft or even doing physical harm.

What makes this worse is the fact that data regarding medical conditions, social security number, or date of birth cannot be changed. This data is connected to a patient for a lifetimelifetime, and once it is compromised it will always be compromised.

What are the most common causes of health data compromise?

According to the 2019 Data Breach Investigations Report from Verizon, the healthcare sector is listed as number two, where 15% of the breaches occurred. The top three patterns for causes of health data leakage are miscellaneous errors, privilege misuse and hacking/web applications[5.1].

This is interesting because some say that the healthcare industry is one of the few that struggles with experiencing more insider threats than threats from the outside. Often the healthcare sector is able to detect hacking incidents quicker than insider threats, where detection occasionally happens years after the actual breach.

Actions involved	Incidents	Data Breaches
Error	124	110
Misuse	110	85
Hacking	100	78
Social	91	78
Malware	85	7
Physical Theft	47	17

Why is the healthcare vertical such an attractive target?

Financial motivation

While most of the sources differ in the actual value of a health data record, they all agree that medical records are typically worth more than financial data on the markets[5.2]. Health data cannot as easily be blocked and changed as, for example, credit card information. Secondly, banks have taken some precautions over the years, and are faster in their response towards theft, while the health sector is in the middle of digital transformation and will most likely need more time to set up detection and response capabilities.

Identity theft to commit fraud

If they have family history, demographic data and insurance information, it is easy for an attacker to steal the victims identity. A fraudster can use PII data to apply for loans, credit cards, tax returns. Or the stolen identity could be used to fraud insurances and receive payments of treatments and prescribed medications. The same can be applied for medical equipment acquired through a patient's prescription.

Physical harm, targeted assassination, blackmail

Gaining access to someone's health data and conditions such as allergies, medication and other dependencies is life critical. In July 2018, 1.5 million patient records were stolen from SingHealth. Among the records was medication details of Singapore's prime minister. It was later concluded that the attack seemed well-planned, sophisticated and targeted, potentially even nation-state sponsored[5.3].

Data collection - where to look when looking for health dumps

Initially, finding market listings consisted mainly of going through online sources such as Reddit threads, hidden wiki-links, dark.fail links and reaching out to other researchers. We experienced the most success when looking through the dark.fail list and forum references.

An unexpected limitation we found was extensive law enforcement activities in the first half of 2019 that shut down many referenced marketplaces. For example, DreamMarket was referenced a lot. When trying to find the marketplace however, it had been closed just one month prior to our investigation[5.4]. Wallstreet Market was shut down in May 2019 by law enforcement[5.5]. Valhalla (also known as Silkkitie), one of the oldest marketplaces, had just been taken down when we started with the data collection[5.6], as well as DeepDotWeb in May 2019[5.7]. The Nightmare market has been unavailable since July 2019, likely due to an exit scam carried out by its operators.

During a period of three months, we visited nine marketplaces and five paste sites and forums.

Overview of relevant market listings

Darknet Marketplace	Listing	Price/Unit
Cryptonia	*Kidz Fullz* • SSN DOB	$20/1 (USD)
Cryptonia	*Partial data from Hospital breach* • SSN DOB	$50/50 (USD)
Empire	*Kidz Medical Fullz* • SSN DOB	$24/1 (converted to USD)
Empire	*Prescription Fraud Course* • Script templates • How to fool pharmacist guide • Quick ways to make money guide	$16.97/1 (converted to USD)
Empire	*Medicare Card (Australia)* • 1x HQ Australian Driver License DL photo scanned • Medicare Card • both valid	$97.84/1 (converted to USD)
Empire	*Healthcare Fraud Package* • Bachelor Diploma • Bachelor Medical Technology • Resume • Malpractice Insurance Document • Medical Diploma & Board Recommendation • DEA License • Medical Technologist Certification (ASCP) • New Mexico MD License • Driving License Scan • Passport Scan	$500/1 (USD)
Empire	*Medical Form Fullz* • Date Info updated • Home Phone • Name • Social Security Number • Address • E-mail • Sex • Employer & Employer Address • Business Phone • Emergency Contact • Closest Relative Living with you • Will • for some patients, ID scans available	$12/1 (USD)

Findings

This research is in no way meant to be representative and only serves to give some insights and "reality check" towards the assumptions we raised earlier. In the above overview, we provide listings we came across that we deemed as relevant to this research.

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

International law enforcement takes 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].

Conclusion

There is no doubt that healthcare data is being sold and traded in underground circles. Due to the volatile nature of the darknet and presumably, limited visibility, it's hard to judge exactly how widespread the activity is.

As we have shown, our biggest limitation was accessing marketplaces. Nevertheless, we can definitely see why someone would be attracted to buying medical records. Because the possibilites of leveraging health data are extensive, it can serve several purposes to defraud or harm a victim.

If you are interested in the full details of our research: You can find much more in the Whitepaper "Databreaches in healthcare"! The download is available for free on https://securelink.net/healthcare/

City of Baltimore shut down by ransomware

While emergency lines like 911 stay unaffected, most civil services like the departments for public works, finance and transportation suffer outages of e-mail and telephone lines[t27].

New sidechannel vulnerabilities affect intel CPU'S

Microarchitectural Data Sampling (MDS attacks) make it possible to steal information from priviledged OS processes or enable breaking into virtual machines. Almost every processor since 2011 is affected[t28].

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].

Facebook announces Libra, its own cryptocurrency

Followed by a very mixed set of reactions, the world's most powerful social media network announces it plans to start its own blockchain based cryptocurrency in 2020[t31].

GandCrab encryption broken

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

JUL

Double-Dip: million fines for breached institutions

British Airways is 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].

Ransomware eCh0raix/ QNAPCrypt targets networkstorages

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].

Michael Haugland
Threat Research Analyst
SecureLink

The PKI and digital trust

I SPY WITH MY DIGITAL EYE

The public key infrastructure (PKI) we use today facilitates many of our secure, everyday internet activities: e-commerce, internet banking, instant messaging and confidential e-mail. 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 noone 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 CA's 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 CA's 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 CA's 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, this real issue, is a conceptual dilemma rather than a technical flaw in the PKI, which makes it incomparably harder to fix.

CA's 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.

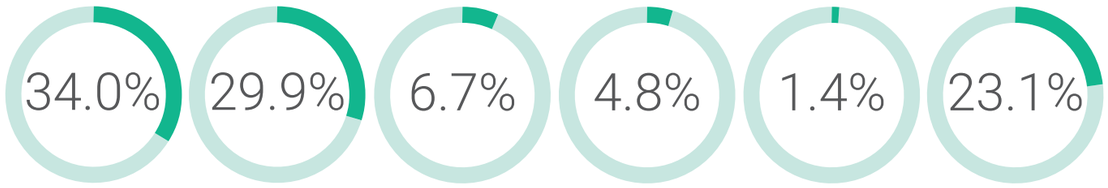
Which is the most trusted CA?

Figuring out which CA is the most trustworthy depends on many factors, but primarily your geolocation. However, our dependency on two standout CA's is clearly who we trust the most.

The two major CA's 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
AddTrust AB

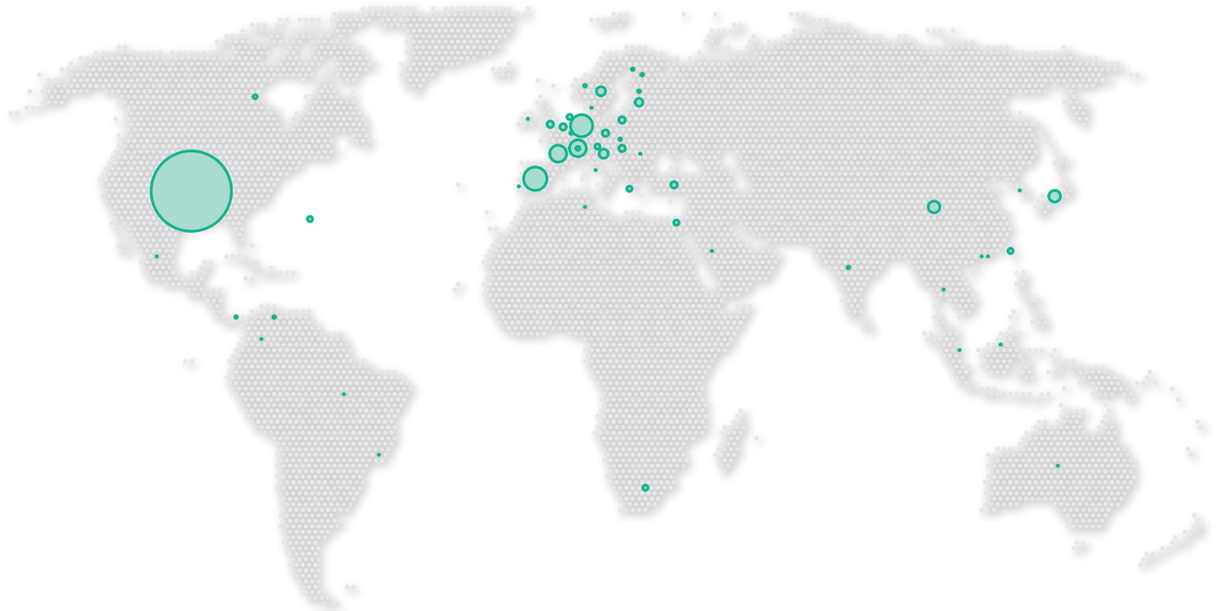
DST Root CA X3
Digital Signature Trust CO

Go Daddy Secure Certificate Authority - G2
Go Daddy Group Inc.

DigiCert Global Root CA
Digi Cert Inc.

Self signed

Others (<5%)

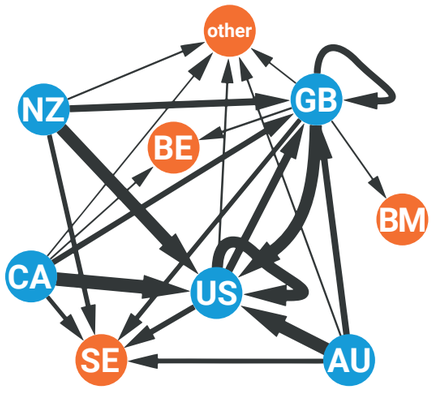


Trust store certificate distribution by geolocation

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.

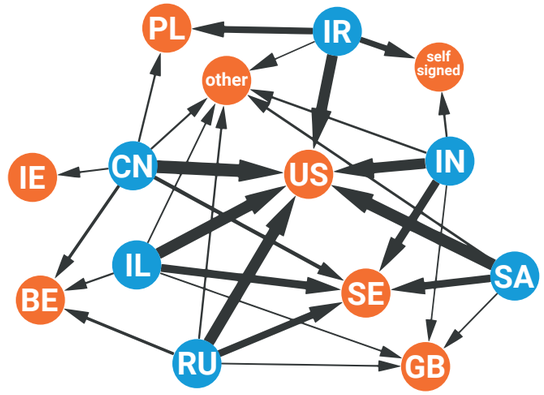
Geographical patterns: Who do the "Five Eyes" trust?

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.



Geographical patterns: Who do the "bad guys" trust?

While this trust distribution exhibits a similar pattern to that of Five Eyes, with the U.S. 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 CA's 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 CA's and Root CA's available in the vendors implemented Trust Store
- The CA's and Root CA's we identified as "used" after analyzing the The List

"Orphaned" CAs lingering in the system

We found that large amounts of the trusted CA's 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 CA's?

As previously mentioned, the root certificates that identify CA's are privately owned. Apparently, there is no regulatory instance deciding which CA's 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 intransparency, is the fact that CA's can (and do) transfer their authority to issue certificates to subordinate CA's (which in turn may pass it on to subsidiaries), resulting in a certificate chain. 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 CA's from geolocations you might hesitate to trust, if you had known.

CA's 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?

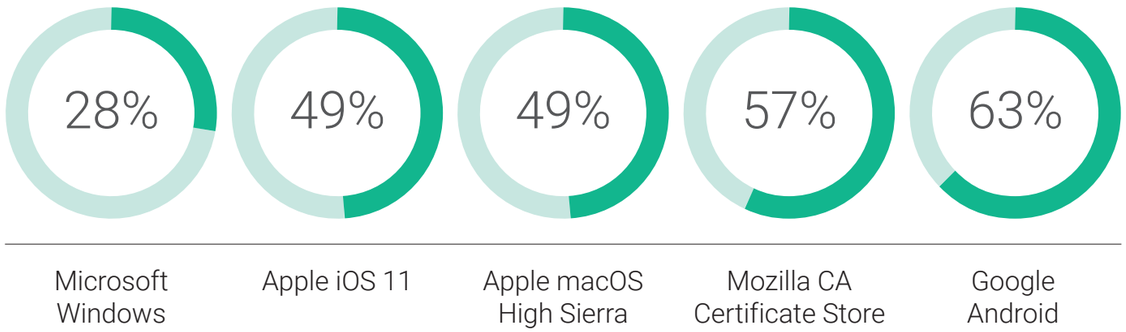
The core of the problem is that it is highly intransparent to end users who they actually trust at all.

For example, when we trust AddTrust, one of the most common CA's, 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 intransparency 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



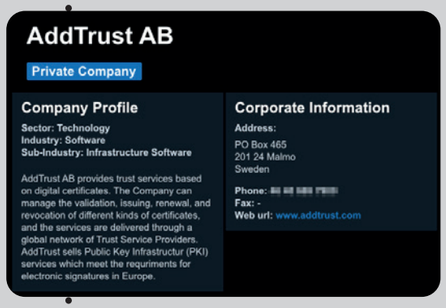
State of Kazakhstan could launch MiTM attacks on all citizens

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

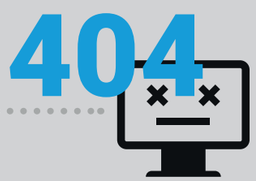
ADDENDUM: WHO IS ADDTRUST?

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 CA's. Here, we have tried to map out who exactly is AddTrust.

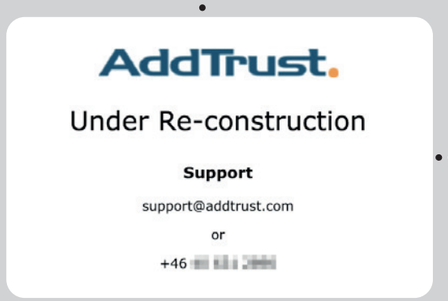
We started by trying to establish the trustworthiness of the purportedly Malmö based company, starting with **Bloomberg**[6.2]:



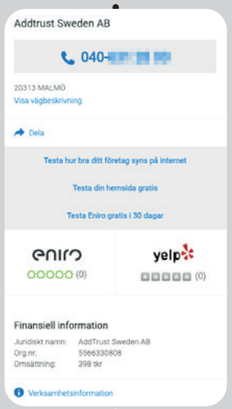
We found a link to the company website, **www.addtrust.com**, but this site cannot be reached.



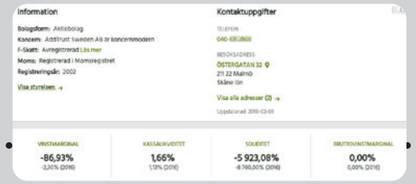
The last entry we can find for the website on internet archives is from January 28, 2011[6.3].
Here we can see a phone number and an e-mail address **support@addtrust.com**



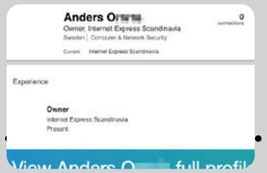
Searching for the company on the Swedish website **Eniro**, reveals more information. In addition to a phone number, we now have a Swedish organization number as well.



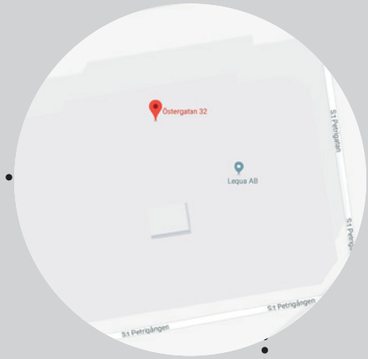
By entering the organization number on **www.allabolag.se** (which lists public information on all companies in Sweden) we can see that AddTrust is registered to "**Anders O.**" The phone number correlates with **Eniro**, and it provides us with another address.



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



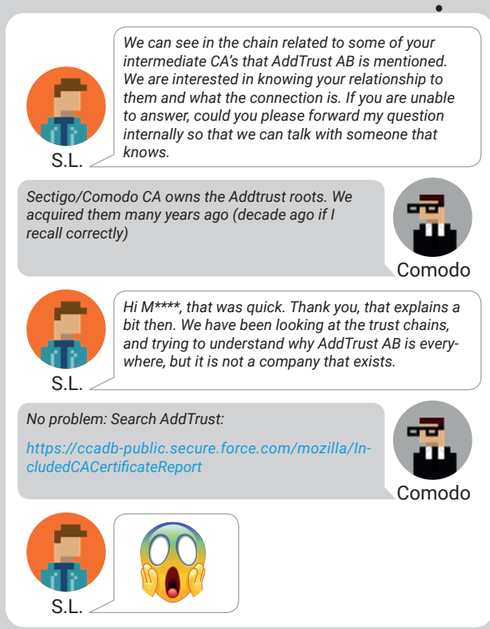
Checking this address in Google maps leads us to a company called **Lequa AB**.



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.

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
Director Group Portfolio Management
SecureLink

Security predictions

FASTEN YOUR CYBER DEFENSE

In September 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 has in store for us?

A new model for threat evaluation

Cyber security has, for a long time, been driven with a reactive approach that focuses on investing in technology to prevent against cyber breaches. Moving forward, customers will need to split up the concept of a cyber breach into two phases :

1. The ***infrastructure breach***, when some devices or workloads are breached.
2. The ***data breach***, when important data is destroyed, held for ransom or leaked.

The security strategy must start with accepting that you will get infrastructure breaches, no matter how much you invest in preventative technologies. Once you have accepted this, you need to have a plan for detecting, limiting the impact of and responding to infrastructure breaches as quickly as possible.

This is the area that we predict investments will shift into during 2020.

Driving detection

So, you know that you have to increase your ability to detect threats, but how do you 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 really 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 or all of the above.

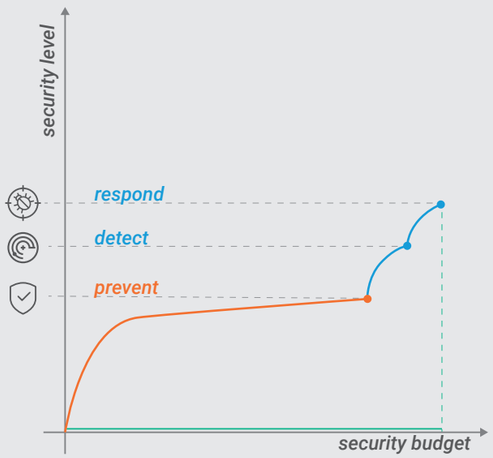
One trend that is very clear when it comes down to it, cyber security is really a big data problem. Regardless of if you are analyzing endpoint data, network data or log data. To solve this, customers will increase investments in technology that have good implementations of AI/ML to help analyze this massive amount of data.

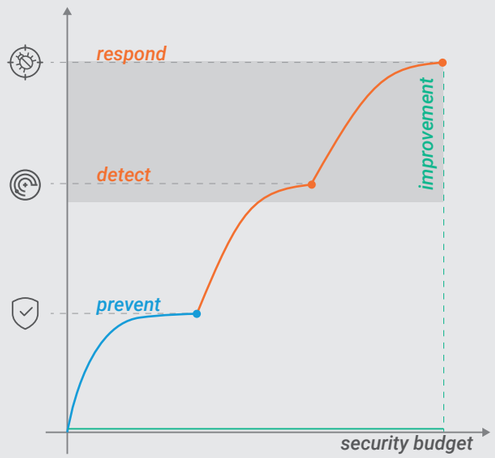
Now you've sorted out the technology approach. What's next? You need people and processes to analyze and classify anything that is detected, 24x7. Most customers struggle with the cost and time of building this themselves, so they will buy this as a service (MDR).

Incident response

As mentioned above, the risk for your business will depend on how quickly you can detect and respond to a threat. Just detecting it will not be enough. During 2019 many customers have called our emergency hotline to get emergency help with incidents. We predict that in 2020, customers will start becoming more proactive, and figure out their internal ability to quickly respond to threats. Then, they will compliment this with subscription based retainer services from security providers that they trust.

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





It all starts with visibility

Cyber security budgets are usually restricted, so investments need to be spent wisely. To make good investment decisions, you need data and visibility to understand where to make the best investments.

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, and demand a lot of tuning and maintenance. In the end, they are only as good as the data used, which is often poor due to lack of resources. We still believe that SIEM is an important component in your SOC toolbox, but you would reach much quicker time-to-value and in many cases also better, threat detection abilities by deploying endpoint-based detection (EDR) or network-based detection (NDR).
We see a trend in investing in both of these technologies, but also as a managed service (MDR), for customers that do not have their own 24x7 CSIRT team.

SIEM -> 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 (which are not security, by the way) are creating new environments 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 that can connect to cloud API's and extract inventory and security data, will be very helpful for your security team. This will provide some control of your cloud infrastructure and make compliance work easier.

Ransomware causes power outages in Johannesburg

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

OT / ICS Visibility

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

The benefits are immense, but the challenges are also significant. A good start is to get visibility of what is connected to these networks so they can be secured. This requires specific technology that understands and decodes the protocols used in these environments.

Privileged Account Visibility

The majority of data breaches use privileged accounts to do lateral movements and data exfiltration. Why? Because it’s easy. Many companies do not have good control of their highly sensitive accounts. It is often estimated that the number of privileged accounts is about three times the amount of normal user accounts. Do you have control of who has access to these accounts, how passwords are shared and rotated and what people actually do when they are logged in as an administrator?

Having visibility of your current privileged accounts is a great first step of your privileged account management strategy.

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 criticial data, should have the appropriate protection needed.

Detection will shift from “standard” to customer specific detections.

Generic rules in a SIEM is 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 customers aren't able to, or don't have the time to, set up a functioning detect & respond team on their own, so we expect that the market for Managed Detection & Response service will continue to grow significantly.

AUG

POC: Ransomware can spread to DSLR cameras

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

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 bank to shut down the site[t39].

French Police remotely remove RETADUP malware from 850,000 infected PCs

National Gendarmerie takes out a RETADUP botnet using a flaw in the malware's CNC-communication. The cybercrime division (C3N) ceases control of the CNC-server and triggers 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 U.S. (to safeguard medical records from cyberattacks) is hit by Sodinokibi ransomware[t41].

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].

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[t43].

Personal details of nearly every Ecuadorian citizen leaked

General manager of IT consulting firm Novaestrat is arrested after personal records of pretty much the entire population (including prominent embassy resident Julian Assange) were left exposed on an unprotected Elasticsearch server[t45].

Cryptomining botnet Smominru keeps spreading

According to research from Gaurdicore the malware infects up to 90,000 clients each month and makes use of the EternalBlue vulnerability (known from the infamous WannaCry campaign)[t46].

Profile of Twitter CEO Jack Dorsey hacked

Hackers social engineered an AT&T employee into giving them Dorsey's cell phone number, which they SIM swapped and used Twitter's "Tweeting via SMS" feature to tweet as the CEO. The feature has since been disabled.[t44].

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[t47].

Report summary:

WHAT HAVE WE LEARNED?

Richard Jones
CISO
SecureLink

2019, a multifarious and successful year where cyber criminals have profited from rich pickings. Our desire to give everything an IP address: simplifying our lives, changing the way we interact with commodity household and business appliances – has brought new opportunities for cyber criminals to exploit, making large scale data heists possible.

"You can't hack something that doesn't have an IP address" comments Col. Jason Rossi of the US Airforce. A year when the Pentagon finally scraps the floppy disk system controlling its nuclear weapons, citing its tech-savvy youngsters couldn't understand how to maintain the antique devices. Built in the 1970s, using software created in the 1950s, it has endured without an IP address, nor has it been breached and has also remained glitch-free since it was first implemented. The new generation simply cannot understand it, and so the decision to retire the archaic contraptions was an easy one. No IP address: it's not cool working on something so old, expertise has been lost, and the queue for the soldering iron course has died out.

Our desire for IP connected lives has accelerated, and it doesn't show any signs of stopping soon. Connectivity is everywhere: it keeps our lights on, our transportation systems running, and it has now become vital for life support systems. However, with digital connectivity comes threats, more specifically cyber threats, followed swiftly by cyber harm. Throughout this report we focus on information, and the very cyber threats targeting our information.

The very fabric we rely on for our connected thirst has never been so fractured and insecure. With millions of vulnerabilities, some decades old, still present in our applications and networks, Edward Snowed bemoans of governments resisting the only viable solution we can rely on - encryption.

Six years ago, a very small percentage of all our internet traffic was encrypted. Today however, and in a large part due to the tech giants (Apple, Google, Facebook and Twitter) who adopted TLS only communications, nearly 80% of all our communications is now secured; something governments even consider as being too secure, something our research into public key infrastructures has shown.

So far, the tech giants have resisted pressure from governments to weaken security protocols in their services and have refused to bake backdoors into their apps, but governments are finding alternative ways to control and intercept communications.

We are now facing a significant digital dilemma: on the one hand we hold fast the rights and freedoms of individuals, while on the other hand, the need to protect the vital interests of nations and our very lives. Information then, is vital but mass surveillance surely casts a continent-sized shadow across the internet, driving the demand for off-grid communications, in turn creating a new darker-net so deep we simply refer to it as the Mariana net.

2020 will bring new threats, ones we did not, and in fact could not predict. We must channel our efforts to focus on the threats and opportunities we do know about with adaptable security architectures.

OCT

Password cracked after 39 years

The password belonged to Ken Thompson, one of the fathers of the initial UNIX. Even in the year of 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/q2-q4!a" [t48].

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 SecureLink's 6 Cyber Defense Centers unless otherwise indicated.

CDC statistics

[2.1] https://coinmarketcap.com/currencies/monero/
[2.2] https://coinmarketcap.com/currencies/ethereum/
[2.3] https://coinmarketcap.com/currencies/litecoin/
[2.4] https://coinmarketcap.com/currencies/bitcoin/
[2.5] https://www.biznesstransform.com/transforming-the-food-and-beverage-industry-with-digital-technologies/

What really disrupted Europe

[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-e-mail-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

Databreaches in healthcare

[5.1] https://enterprise.verizon.com/resources/reports/dbir/
[5.2] https://techcrunch.com/2018/08/09/the-healthcare-industry-is-in-a-world-of-cybersecurity-hurt/
[5.3] https://www.hcinnovationgroup.com/cybersecurity/article/13030570/what-can-the-industry-learn-from-recent-highprofilehealthcare-cyber-attacks
[5.4] https://www.zdnet.com/article/top-dark-web-marketplace-will-shut-down-next-month/
[5.5] https://www.theverge.com/2019/5/3/18528211/wall-street-market-silkkitie-valhalla-dark-web-takedown-police-germany
[5.6] https://bitcoinmagazine.com/articles/major-darknet-marketplace-wall-street-market-shuttered-law-enforcement
[5.7] https://techcrunch.com/2019/05/07/deep-dot-web-arrests

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.bloomberg.com/news/articles/2019-01-24/china-is-said-to-block-microsoft-s-bing-due-to-technical-error
[t6] https://www.carbonblack.com/2019/01/24/carbon-black-tau-threatsight-analysis-gandcrab-and-ursnif-campaign/
[t7] https://www.europol.europa.eu/newsroom/news/xdedic-marketplace-shut-down-in-international-operation
[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/vfe-mail-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://thehackernews.com/2019/04/e-mail-signature-spoofing.html

[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://software.intel.com/security-software-guidance/insights/deep-dive-intel-analysis-microarchitectural-data-sampling#MDS-buffer-overwrite

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

[t44] https://thehackernews.com/2019/09/tweet-via-sms-text-message-hacking.html

[t45] https://www.vpnmentor.com/blog/report-ecuador-leak/

[t46] https://www.guardicore.com/2019/09/smominru-botnet-attack-breaches-windows-machines-using-eternalblue-exploit

[t47] https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet

[t48] https://thehackernews.com/2019/10/unix-bsd-password-cracked.html

Disclaimer

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

Very special thanks
to all Cyber Hunters, Analysts and engineers in our CDCs.

Secure Link
Part of Orange Cyberdefense

About SecureLink, part of Orange Cyberdefense

Building trust. Enabling business.

We're specialists in cyber security. It's our focus every hour of the day, every day of the year. That's why we're among the best – if not the best – in the world at what we do. But true cyber security isn't just about protection. It's about enabling, too. It's about empowering businesses by allowing them to safely embrace innovation, efficiency and collaboration. True cyber security is about adding value by building trust and making life easier for our customers.