2018
ANNUAL SECURITY REPORT

Secure Link | SAFELY ENABLING BUSINESS

This report is based on over a quarter of a million security events that we have processed so far in 2018. Some were critical, a lot of them were bad. Most were just unusual, while a few were even benign.

We see a tremendous amount of security incidents. In 2018, we've seen our share of ransomware and cryptojacking, nation-state attacks, social engineering and policy breaches. Among them are some real 'gems'. For example, we've seen criminals hack into an organisation's customer relationship management database, edit the invoice template, and only change one small field: the bank account number. We've come across vast amounts of similarly strange events.

It kept us busy for a year. Some anecdotes made it to blogs and into keynotes. Some of our findings were new, while some confirmed previous research carried out by partners and others.

This report is based on over a quarter of a million security events that SecureLink has processed in 2018, as well as research from the wider IT security industry. Some were critical, some of them were bad. Most were just unusual, while a few were even benign.

We have come to know them well and got up close and personal with them, as we reverse engineered them, extracted indicators of compromises, and put them in our threat feed. They taught us a lot: how rookie criminals tend to go for ransomware and cryptojacking; how veterans deploy artisanal hacking in order to get to the loot; and how sometimes you'll only catch nation states once they start lateral movement.

This report is dedicated to them – the quarter of a million events we've researched, as mundane as they sometimes were. Without our customers, though, this report would not be possible. So ultimately, this report is for you.

Thank you!

The SecureLink team

TABLE OF CONTENTS

2018 TIMELINE

Diana Selck-Paulsson
Threat Research Analyst / TDMC
SecureLink

CYBER DEFENSE CENTER STATISTICS

THIS IS WHAT HAPPENED

As we are running managed detection and response services for many customers, a lot of data passes over our desks. As our customer base grows, so does the volume of data. Therefore, we've decided to invest effort into 'slicing and dicing' this data, and into research trends and anomalies.

We want to give you some insight into what kinds of threats we're seeing, what kinds of issues our customers are dealing with, and what differences and similarities we see across organisations.

ABOUT THE DATA

- Grand total of events analysed: 255,701
- Grand total of security incidents analysed: 21,240
- Out of the grand total of events, 8.3% are considered security incidents, based on our classification processes.
- Time period: ten months of data, starting 1 January 2018
- The period reflects the first ten months of 2018. By the end of December, we will analyse and compare the impact of the last two months of data. If we see that a trend breaks, we will interpret and append them to this report in February 2019.
- Data sources: firewalls, directory services, proxy, endpoint, EDR, IPS, DNS, DHCP, SIEM and our SecureDetect platform.

TYPES OF INCIDENTS

We classify different types of incidents, and some of these types are further subcategorised (for example, different kinds of malware). In 2018, we detected the following incident types:

Malware is malicious software such as ransomware.

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.

Social Engineering like Phishing, spoofing and other attempts to fool users.

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

TOTALS

The majority of incidents we've analysed were malware incidents, followed by network and application anomalies. It's not surprising, as they often go hand-in-hand: malware will check in to a command and control server and cause anomalous traffic within the network.

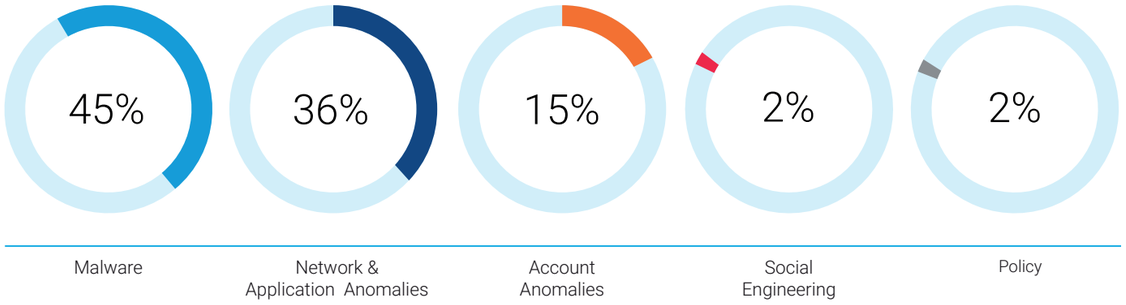
An interesting observation is that social engineering is seemingly low. An explanation can be found in the process: in social engineering, criminals trick users into clicking a link or executing a malicious file, which means it is often detected as malware and not as an initial attack vector, even though this is what has actually happened.

Pure social engineering attacks without technical components are hard to detect and sometimes under-reported, so we registered a low number.

FUNNEL: ALERT TO INCIDENT

255,701
Alerts • Use Cases • Events

21,240
Security Incidents



JANUARY 2018 – MELTDOWN & SPECTRE

'Meltdown' and 'Spectre', theoretically, allowed attackers to steal data processed by CPUs. However, they slightly differ in terms of which feature is exploited.

Meltdown breaks the most fundamental isolation between user applications and the operating system (OS), which allows a program to access the data of the OS and the secrets of other programs.

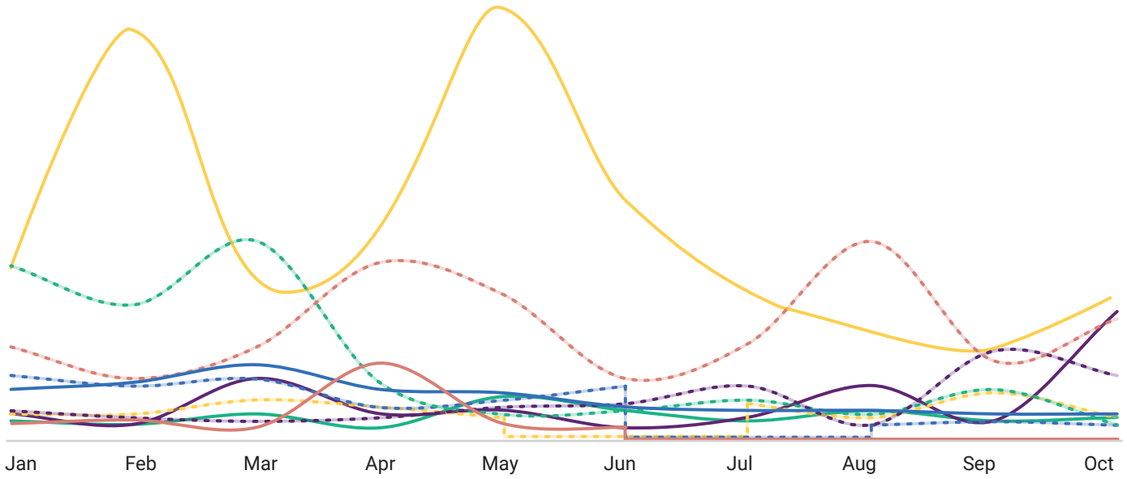
Spectre, on the other hand, breaks the isolation between different applications. As a result, error-free applications can leak data. Almost all systems are affected by Spectre, but the vulnerability is more difficult to exploit.

ZOOMING IN TO MALWARE

If we look at types of malware, we spot a few interesting trends.

Firstly, we see a very big number of PUP/PUA (potentially unwanted programs/applications). If we ignore those, we see ransomware fluctuating. We saw Remote Access Tools (RAT), often used for 'back doors', increase in the last few months. We then saw a wide range of malware types flowing through time.

Some types of malware correlate with criminal campaign activities and ransomware. For example, it shows a clear trend of how criminals gear up in Q1, peak in early Q2, go on a holiday, and get back for another go in Q3. As strange as it might sound, the more commoditised the crime market gets, the more you will see this holiday and 9-to-5 behaviour.



ORGANISATION SIZE

We are interested in learning if the size of the organisation matters. Are larger organisations a more interesting target? Or are they better protected with their bigger budgets? We divided organisations into three tiers.

When we're looking at the numbers, 8% of incidents happen in small organisations with fewer than 1,000 employees, 19% happen in the mid-range, and the vast majority, 73%, happen in large organisations.

We know from various sources confirming our own, that social engineering is the main attack vector and threat for any organisation. So let's see what happens if we take the number of personnel into account. Does a higher number of employees mean organisations suffer more attacks per head? We divided the number of incidents by the number of companies and the median company size.

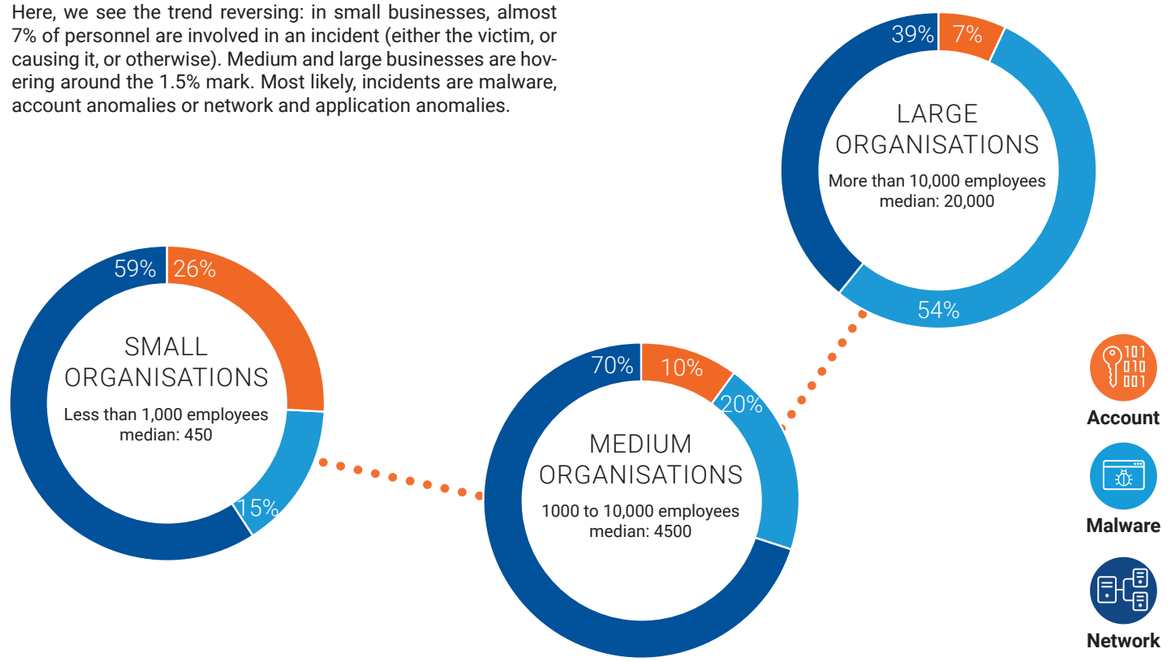
Here, we see the trend reversing: in small businesses, almost 7% of personnel are involved in an incident (either the victim, or causing it, or otherwise). Medium and large businesses are hovering around the 1.5% mark. Most likely, incidents are malware, account anomalies or network and application anomalies.

TYPES OF INCIDENTS VERSUS BUSINESS SIZE

When we look at what types of incidents we see across different sizes of organisations, the top three are quite consistent.

We can see network and application anomalies dominating small and medium enterprises. But in larger organisations malware is the dominant incident type at 54%.

A plausible explanation is that large organisations are investing time and effort in next-generation malware detection and managed detection and response. Thus, more malware incidents are stopped in the early stages. In smaller organisations, malware may get further into the network, yielding network and application anomalies, and possibly leading to incident detection.



INCIDENTS PER 100 EMPLOYEES

For companies with **under 1,000 personnel**, there's a sharp increase of incidents per head. On average, it's **five times higher** than in larger organisations.

SMALL ORGANISATIONS	MEDIUM ORGANISATIONS	LARGE ORGANISATIONS
6.8	1.5	1.3

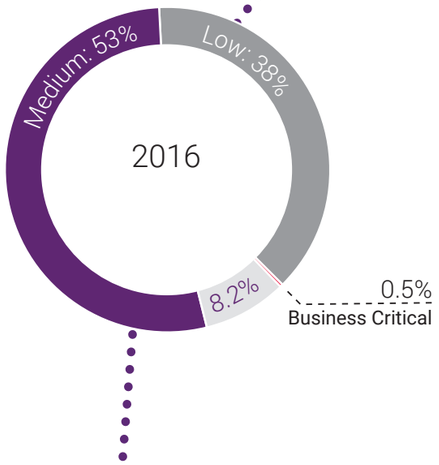
CRITICALITY

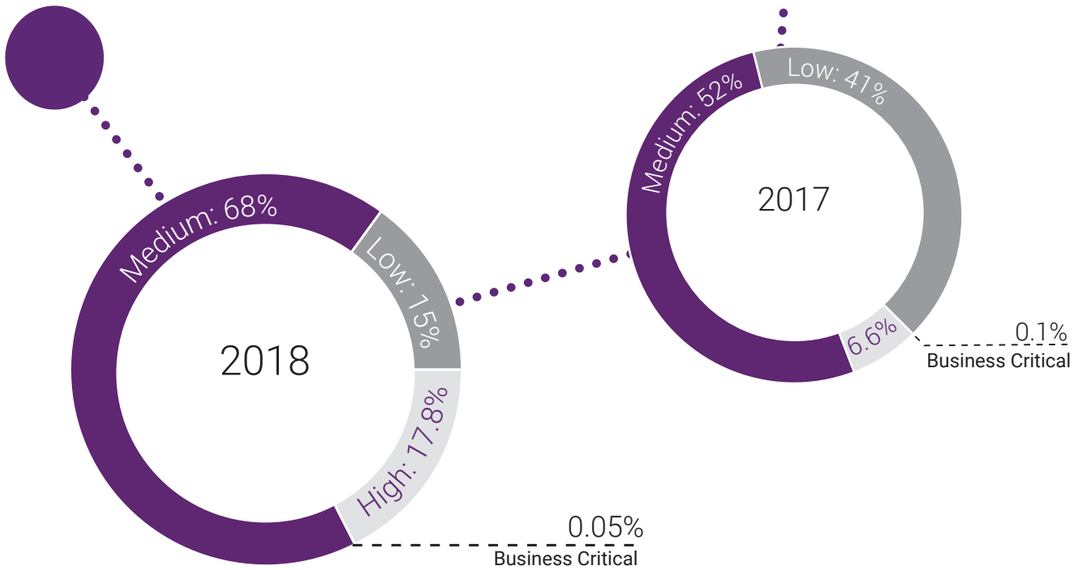
Incidents are not equal. At SecureLink, we define four levels:

- **Business critical:** Critical business impact, business processes grinding to a halt
- **High:** Significant business impact, incidents that must be taken care of immediately
- **Medium:** Limited business impact, acceptable workaround 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%

We see a shift over the years, from the outliers towards the middle. It's also notable that business critical incidents have dropped by a factor of ten. That said, these incidents are rare (we usually see several dozens of them per year) and low numbers and statistics usually don't mix well. The shift towards the middle is quite clearly visible in the charts:





FEBRUARY 2018 – OLYMPIC DESTROYER

For the first time in history, the Olympic Games were directly targeted by a malware attack. 'Olympic Destroyer' attacked the Olympic Games prior to the opening ceremony. It shut down event monitors, killed wifi on-site and disturbed the Olympic website, preventing visitors from printing tickets. Security analysts believe that the malware originates from Russia, which aligns quite well with the conflict between Russia and the International Olympic Committee regarding Russia's Olympic athletes and their doping abuse. The malware was created with 'false flags' pointing to North Korea to distract from its origin.

FEBRUARY 2018 – CRYPTOCURRENCY MINING

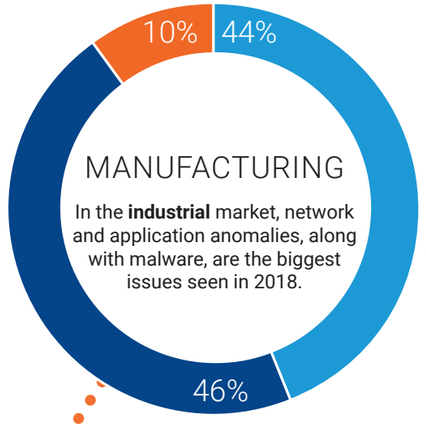
February continues to witness the evolving trend of unwanted cryptocurrency miners in organisation's environments. It was published this month that Tesla's cloud servers were hacked last year due to a failure to secure one of the application's consoles with an access password. Consequently, the servers were infected by malware, with the intention of mining cryptocurrency. SecureLink's Cyber Defense Center (CDC) sees the same trend at a variety of its customers throughout all industries.

INCIDENTS IN DIFFERENT VERTICALS

Looking at incidents, and how they're spread over different verticals, it's quite interesting to see different nuances. We've analysed seven verticals, and we were quite surprised to see many differences.

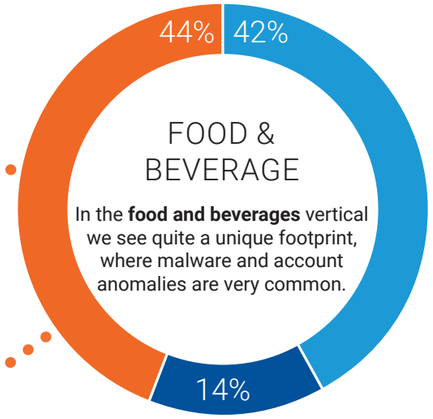
Higher numbers in these graphs do not just mean that incidents are happening more often, and the vertical is more 'vulnerable'. In fact, it can indicate quite the opposite. The ability to identify an incident may indicate a high security process maturity. For example, in Finance, there's a lot of social engineering for fraudulent purposes. Financial organisations are more mature in dealing with these incidents and are able to detect and report more of them.

	Malware	Network	Policy	Social	Account
Business Services	21.59%	51.71%	0.49%	0.12%	26.10%
Financial Services	39.00%	27.03%	1.96%	4.80%	27.21%
Manufacturing	43.83%	45.51%	0.15%	0.11%	10.39%
Food & Beverages	42.29%	13.54%	0.07%	0.07%	44.03%
Government/Public	5.52%	46.01%	4.29%	0.00%	44.17%
Healthcare	25.21%	62.98%	3.77%	0.04%	8.00%
Retail	53.43%	30.86%	2.01%	2.28%	11.41%



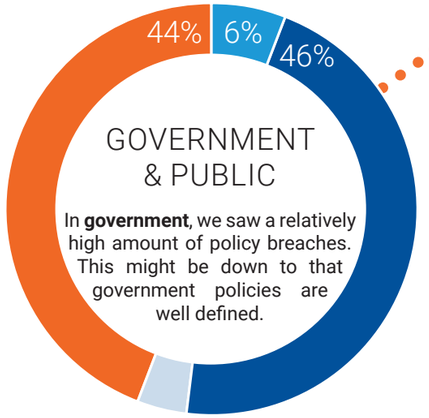
MANUFACTURING

In the **industrial** market, network and application anomalies, along with malware, are the biggest issues seen in 2018.



FOOD & BEVERAGE

In the **food and beverages** vertical we see quite a unique footprint, where malware and account anomalies are very common.

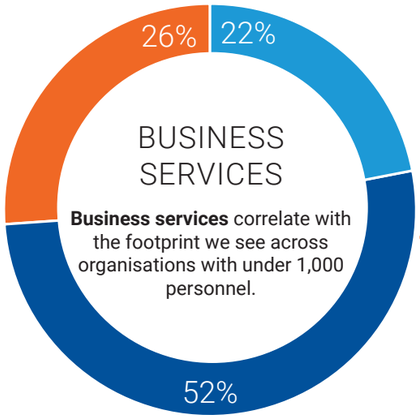


GOVERNMENT & PUBLIC

In **government**, we saw a relatively high amount of policy breaches. This might be down to that government policies are well defined.

RETAIL

The last graph shows that more than half of the incidents in **retail** are malware, in conjunction with a large percentage of network and application anomalies.



BUSINESS SERVICES

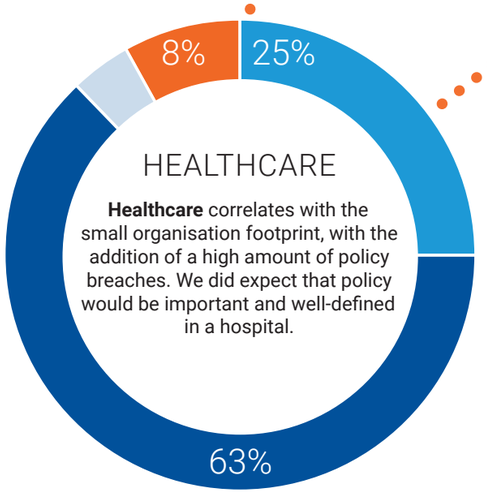
Business services correlate with the footprint we see across organisations with under 1,000 personnel.

FINANCE

Finance is the only vertical with a high level of policy breaches and social engineering. This is likely due to two reasons:

Financial organisations have a lot of experience in dealing with these attack types. They are better equipped to identify, detect and report them.

Secondly and importantly, as per quotes from famous bank robbers, 'that's where the money is'.



HEALTHCARE

Healthcare correlates with the small organisation footprint, with the addition of a high amount of policy breaches. We did expect that policy would be important and well-defined in a hospital.

CONCLUSION

The numbers show that malware and network and application anomalies are the most detected incidents. In larger organisations, we expected there would typically be a higher percentage of malware detections. And indeed, they received 73% of incidents according to our numbers. But we do not think this is because large organisations are targeted more or because they have more personnel who 'click links', and certainly not because they're more vulnerable. In fact, we see that, per head, large and mid-sized organisations actually process four times fewer incidents than smaller organisations.

In other words, smaller organisations seem to be processing a larger amount of security events. It likely requires a lot of manual effort.

In general, we see a shift from high and low impact events to medium impact events. We have certainly worked on several dozens of incidents where business continuity was at stake, but they appear to decrease over time. At the same time, high-, medium- and low-impact events are divided more evenly over time. We could say that incident impact is normalising.

MARCH 2018 – CYBER ATTACK WITH DEADLY INTENTIONS

News broke that a petrochemical company in Saudi Arabia was targeted by a deadly attack in August 2017. The unidentified adversaries' intentions were to trigger an explosion causing maximum physical damage and death. Many details remained unknown. However, these kinds of attacks are considered highly dangerous. Due to a mistake in the attacker's computer code, the explosion was prevented.

APRIL 2018 – VPNFILTER

In mid-April, a hacker group associated with the Russian APT28 group was accused by several countries of targeting internet routers. These end-of-life devices do not receive security patches any longer. They are often outdated devices using unencrypted protocols and a default password. An IoT botnet malware dubbed 'VPNFilter' infected over 500,000 devices in 54 countries. The malware uses a multi-stage approach to interfere with internet communication, gather intelligence and execute destructive operations, and even comes with a kill switch to deliberately kill itself.

APRIL 2018 - HEALTHCARE SECTOR TRAGETED BY ORANGEWORM WITH 'KWAMPIRS' MALWARE

A relatively new attack group dubbed 'Orangeworm' was uncovered in April. Orangeworm had already been seen in 2016 but re-emerged this year and is associated with a malware type called 'Kwampirs'. Researchers observed that the malware primarily targeted the healthcare sector across the United States, Europe and Asia.

Kwampirs inherits a worm-like behaviour and infects medical devices, such as high-tech imaging gear, X-rays and MRI machines. It also strikes network shares and servers, online platforms that assist patients in providing their consent for medical procedures, targeting the whole supply chain surrounding medical devices. This includes pharmaceutical companies, IT solution providers and manufacturers of medical equipment. Kwampirs propagates through unprotected network shares in old Windows networks that are rather common in healthcare environments. It is recommended to avoid using unsupported Windows systems such as Windows XP and patch devices as soon as security patches are available.

Eward Driehuis
Chief Research Officer
SecureLink

GEOPOLITICS

THE AGE OF CYBER-WARFARE

Last year we saw the weaponisation of malware go mainstream. Specifically, Wannacry and NotPetya attacks did a lot of damage. These attacks were essentially generic ransomware with one difference: apart from a few unverified claims, victims who paid the ransom did not get their files back. With word spreading among victims that these criminals' couldn't be trusted, ransom payments dwindled fast. What was left was destruction. These actors had no financial motives, and researchers frantically searched for explanations. Nation state-sponsored groups were the most plausible perpetrators, with North Korea as a prime suspect for Wannacry, and Russia for NotPetya.

Advanced Persistent Threats (APTs) were now everybody's problem. Geopolitics is an important factor in assessing the threat landscape. Infosec professionals now have to deal with new threat types, destructive attacks, with no monetary incentive, in order to support geopolitical goals.

In 2018, tensions increased and some of the greatest disruptions came from alleged nation state-related groups. This chapter outlines the most notable events.

WHO ARE THE 'BAD NATIONS'?

Who 'adversary nations' are really depends on where you live. If you're a NATO ally, it is a handful of nations attributed with hacking for geopolitical purposes, in the eastern hemisphere. There are no standards for defining or naming adversaries. One of the most widely used naming conventions is APT, a likely nation state-sponsored hacking group. If we look at a list of these APTs, we can see Russia and North Korea making the headlines. Iran has been increasing its capability for years, and Vietnam focuses on local geopolitics. China has the most APT groups, all of them focused on industrial espionage.

The list of APT nations changes depending on where you live. So, bear in mind that this report has been written with a Western bias.

RUSSIA-RELATED ACTIVITY

From the early beginnings of cybercrime, Russian nationals have been attributed with cyber-attacks. Over the last few years, the Russian government has been accused, both implicitly and explicitly, of numerous attacks and information warfare. The associated APT's are APT28 and APT29. In 2018 there were lots of related events:

January 2018

During the weekend of January 27 in the Netherlands, distributed denial of services (DDOS) attacks started targeting banks and government departments. After several days, they were still happening. This caused severe disruption to retail payments and online banking.

A week earlier, a story broke that US authorities had been bragging over 'friendly spy agencies having access to FSB networks'. This was reported in an article stating that Dutch spies were warning the US about DNC and other hacks, by hacking into the Russian spy office (APT29). Many amateur cyber sleuths found the DDOS/Russia story a bit convenient and suspected Russia coordinated a retaliation. Later it became apparent that the DDOS attacks weren't Russian retaliation, but were executed by a Dutch teenager, who thought 'it would be fun'. The story about the Dutch hacking the Russians has not been refuted.

February 2018

Robert Mueller, the special counsel investigating the 2016 Russian meddling in the US election, indicted 13 Russian nationals. Twelve of them worked for the Internet Research Agency, a notorious Kremlin-linked Russian troll farm. They were accused of meddling in the 2016 US election.

Also in February, the White House blamed Russia for the NotPetya attack. NotPetya, although smaller than Wannacry, did vastly more damage, and is considered to be the most destructive cyber-attack to date.

March 2018

Many security researchers reported on Olympic Destroyer. It targeted the South Korea Winter Olympics back-end servers with destructive attacks. What was special about it is that there were numerous false flags built in, all pointing to Lazarus, a North Korea connected group. Apparently, the attackers were trying to sow confusion about their identities by pointing to a specific and plausible adversary. Again, there was a plausible narrative: the Olympic games are relevant for Russia, as they had been humiliated on the global stage when most of their athletes were banned for doping.

June 2018

Kaspersky's 'GReAT' disclosed they were tracking attacks with 'Olympic Destroyer' and APT28 / GRU footprints. The attacks were targeting 'chemical threat prevention labs'. It is unknown if the motive was connected to the Salisbury poisonings. A plausible narrative emerged, stating that they supported the Skripal poisoning with a cyber offensive. The offensive failed, and months later they sent in operatives. This narrative is mostly based on circumstantial evidence.

July 2018

Robert Mueller indicted 12 Russian nationals. The indictment detailed a complex effort by Russia's top military intelligence service (the GRU) to sabotage the campaign of President Trump's Democratic Party rival, Hillary Clinton. Three of the 12 were present in the October 2018 WADA/OPCW indictments and were allegedly involved in both efforts.

October 2018

In October, the US indicted seven Russian nationals for espionage, connected to WADA the anti-doping agency, the 2016 Olympics and OPCW a chemical threat prevention laboratory.

Earlier that day, the Dutch Ministry of Defense (MoD) held a press conference. It mentioned that four of the seven Russian nationals had been apprehended in April. The four men travelled to the OPCW offices in the Netherlands and tried to hack into the WIFI. The OPCW investigated the Skripal poisoning, Syrian chemical warfare, and MH17. They were caught red-handed, their tools and laptops confiscated, and they were deported, since they held diplomatic passports. The MoD proceeded to disclose the tactics and procedures used by them, in detail. In a statement, which by many is seen as a response to the information warfare, the Dutch disclosed GRU methods, including WIFI tools and fake passports. Bellingcat, the open source intelligence organisation, used these details to expose hundreds of alleged Russian agents.

Other activities of APT28

In 2018, there have been further events attributed to APT28 that have no obvious connection to the ones mentioned above:

LoJax is a particularly dangerous tool. It's the first UEFI Rootkit, and it's allegedly used by APT28 to gain persistence outside of the visibility of the operating system.

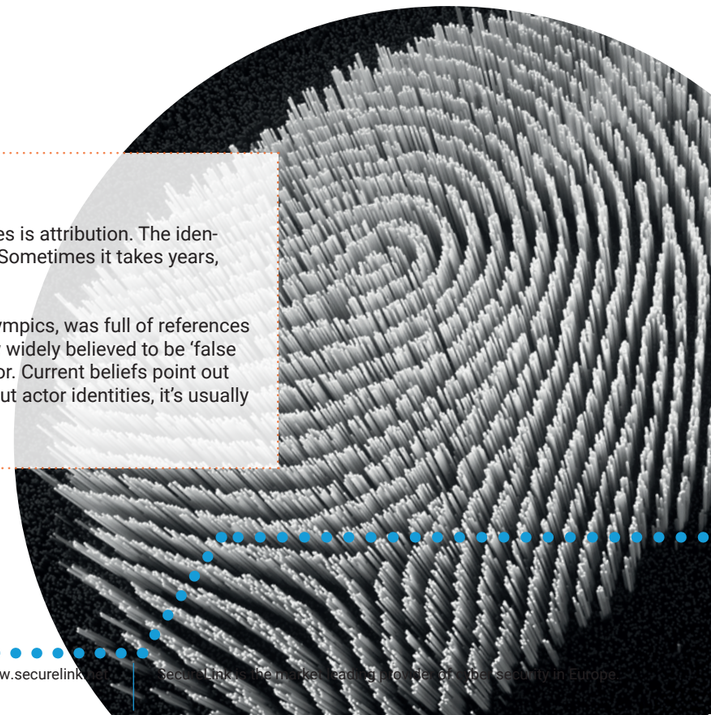
The Internet of Things botnet 'VPNFilter' is suspected to be of APT28 origin as well. The botnet infects end-of-life internet devices with default passwords and low security. The intent of the botnet is unclear, although researchers find clues in the malware having SCADA inspection capabilities. This could indicate that it's looking to disrupt critical infrastructure, in countries where cheap devices are being used in critical environments.

Sources: [1][2][3][4][5][6][7][8][9][10][11][12]: Details on page 58

ATTRIBUTION IS DIFFICULT

In threat intelligence, one of the most difficult processes is attribution. The identification of the source of a threat is a delicate matter. Sometimes it takes years, sometimes attribution is wrong.

Olympic Destroyer, when attacking the South Korea Olympics, was full of references to North Korea when it was researched. These are now widely believed to be 'false flags', deliberately pointing away from the actual creator. Current beliefs point out Russia as responsible. Whenever claims are made about actor identities, it's usually wise to keep an open mind.



NORTH KOREA-RELATED ACTIVITY

In 2018, North Korean and US leaders met in Singapore and expressed public appreciation for each other. Since this meeting, a flurry of friendly diplomatic meetings have taken place. Sworn enemies North and South Korea have met and shaken hands. This diplomatic progress correlates with North Korea taking the world stage on a cyber level.

2016

North Korea entered the stage with a bang in 2016. Back then, the Lazarus group was tied (loosely) to the regime. Lazarus became notorious in February of that year, for stealing $80 million from the Bank of Bangladesh, using stolen SWIFT network credentials. The narrative became that the Lazarus group focused on stealing money for the North Korean regime. In those days, this attribution was not very strong, and the narrative was doubted. Before 2016, North Korea was suspected of the Sony attack (due to the movie The Interview, poking fun at Kim Jong-Un) and numerous attacks on South Korean banks.

2017

In 2017, the Wannacry attack tools had similarities with some earlier Lazarus tools, and so it was again vaguely attributed to Lazarus.

Also in 2017, numerous cryptocurrency exchange attacks happened, which some attribute to North Korea. With the rise of cryptojacking, North Korea was again suspected of many of them. The narrative became that the regime was trying to get its hands on as much foreign money as it could. North Korea being a very poor dictatorship, the narrative makes sense.

2018

In October 2018, North Korea got its second APT designation. Next to APT37, FireEye released a report implying that a separate group (APT38) is responsible for stealing money for the North Korean regime. Targeting the SWIFT inter-banking network is one of their favourite modus operandi. This implied that the group should be experts in money laundering too. APT38 had links with Lazarus, but they are not one and the same. The Lazarus group remained elusive.

In October 2018, a report came out describing how North Korea, through APT38, Lazarus, or a combination, has stolen over half a billion dollars from bitcoin exchanges. The funds were likely used for government financing.

Sources: [13][14][15][16][17][18]: Details on page 58

CHINA-RELATED ACTIVITY

As we can see in the APT list, China is the country with the most numbered APT groups. It also has the world's second largest economy, it has nuclear weapons and the world's second largest defense budget. In all these things, China is second to the USA, but catching up.

In 2018, the USA started a trade war with China and many other economic zones, including the European Union, Mexico and Canada. In numerous statements, the US president has pointed to China as the biggest aggressor. Some cyber security agencies support this statement, and we at SecureLink have observed increased activity in our Cyber Defense Center.

China, allegedly, has a long history of industrial espionage. In the cyber domain, half of the named APTs are attributed to it. APT1, 2, 3, 10, 12, 16, 17, 18, 19, 27 and 30 are all believed to be tied to China. Focusing on numerous different verticals or geographical regions, these groups are specialised in different espionage types.

Apart from trade wars, China is involved in other conflicts. In 2018, attacks on Taiwan have increased.

In unprecedented events in October, China has abducted and arrested Meng Hongwei, the Chinese president of Europol, which is a politically neutral institution. The charges are bribery, and the Chinese consider the matter to be between them and France, where Meng lives.

Sources: [19][20][21][22]: Details on page 58

APRIL 2018 – DRUPALGEDDON2

The Drupal vulnerability 'Drupalgeddon2' enables attackers to take over websites to deliver cryptocurrency miners and other malware. Drupal released a patch without disclosing many technical details, but after roughly two weeks a Drupalgeddon2 PoC exploit code was released on GitHub. This sparked large-scale exploitation and scanning attempts, including attacks to deliver cryptocurrency miners, a PHP backdoor and an IRC bot written in Perl. During the last week of April, researchers detect-ed a botnet (Muhstik) taking advantage of this.

APT LIST – CURRENTLY ACTIVE [23][24]

	#	Alias	Associated country	Intended purpose	Target
APT	**1**	Unit 61398, Comment Crew	China	Espionage	Information Technology, Aerospace, Public Administration, Satellites and Telecommunications, Scientific ReseaTAVrch and Consulting, Energy, Transportation, Construction and Manufacturing, Engineering Services, High-tech Electronics, International Organisations, Legal Services Media, Advertising and Entertainment, Navigation, Chemicals, Financial Services, Food and Agriculture, Healthcare, Metals and Mining, Education
APT	**2**	Putter Panda	China	Espionage	Government, Defense, Research, and Technology sectors in the United States, with specific targeting of the US Defense and European satellite and aerospace industries
APT	**3**	UPS Team	China	Espionage	Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications, Transportation
APT	**4**				
APT	**5**				Regional Telecommunication Providers, Asia-Based Employees of Global Telecommunications, and Tech Firms, High-Tech Manufacturing, Military Application Technology
APT	**6**				
APT	**7**				
APT	**8**				
APT	**9**				
APT	**10**	MenupasmenuPass, Stone Panda, Red Apollo, CVNXs team	China	Espionage	Construction and engineering, aerospace, and telecom firms, and governments in the United States, Europe, and Japan
APT	**11**				
APT	**12**	IXESHE, DynCalc, and DNSCALC	China	Espionage	Journalists, government, defense industrial base
APT	**13**				
APT	**14**				
APT	**15**				
APT	**16**		China	Espionage	Japanese and Taiwanese organisations in the high-tech, government services, media and financial services industries
APT	**17**	Tailgator Team, Deputy Dog	China	Espionage	U.S. government, and international law firms and information technology companies
APT	**18**	Wekby	China		
APT	**19**	Codoso Team	China		Legal and investment
APT	**20**				
APT	**21**				
APT	**22**				
APT	**23**				
APT	**24**				
APT	**25**				

[23][24]: Details on page 58

	#	Alias	Associated country	Intended purpose	Target
APT	**26**				
APT	**27**	LuckyMouse, Iron Tiger, EmissaryPanda, Threat Group-3390	China		National data center of an unnamed central Asian country
APT	**28**	Fancy bear, Tsar Team	Russia		The Caucasus, particularly Georgia, eastern European countries and militaries, North Atlantic Treaty Organisation (NATO) and other European security organisations and defense firms
APT	**29**	Cozy bear, The Dukes	Russia		Western European governments, foreign policy groups and other similar organisations
APT	**30**	-	China		Members of the Association of Southeast Asian Nations (ASEAN)
APT	**31**				
APT	**32**	OceanLotus Group	Vietnam		Foreign companies investing in Vietnam's manufacturing, consumer products, consulting and hospitality sectors
APT	**33**	-	Iran		Aerospace, energy in U.S., Saudi Arabia and South Korea
APT	**34**	-	Iran		Financial, government, energy, chemical, and telecommunications, within the Middle East
APT	**35**				
APT	**36**				
APT	**37**	Reaper	North Korea		South Korea, Japan, Vietnam and the Middle East – various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare
APT	**38**		North Korea	Financial	Tageting finance / Swift networks

MAY 2018 – EFAIL

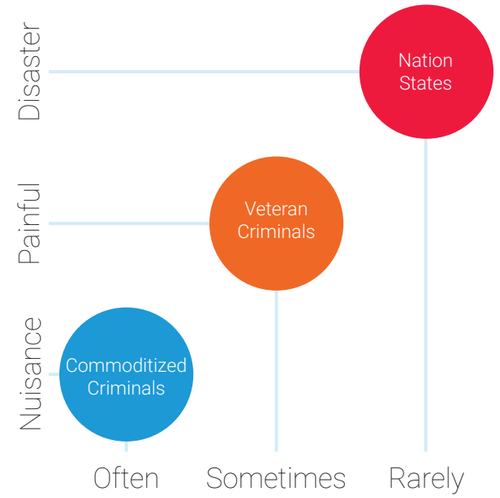
On May 14th, security researchers discovered 'Efail', a flaw that abuses a critical vulnerability in OpenPGP and S/MIME, standards which are both used for end-to-end email encryption. In order to mitigate the risk of being eavesdropped, the automatic loading of remote content should be disabled.

If enabled, an attacker who captures an encrypted email could resend the email to the victim in a reformatted way, which enables the attacker to decrypt both the current and previously sent emails.

CONCLUSION

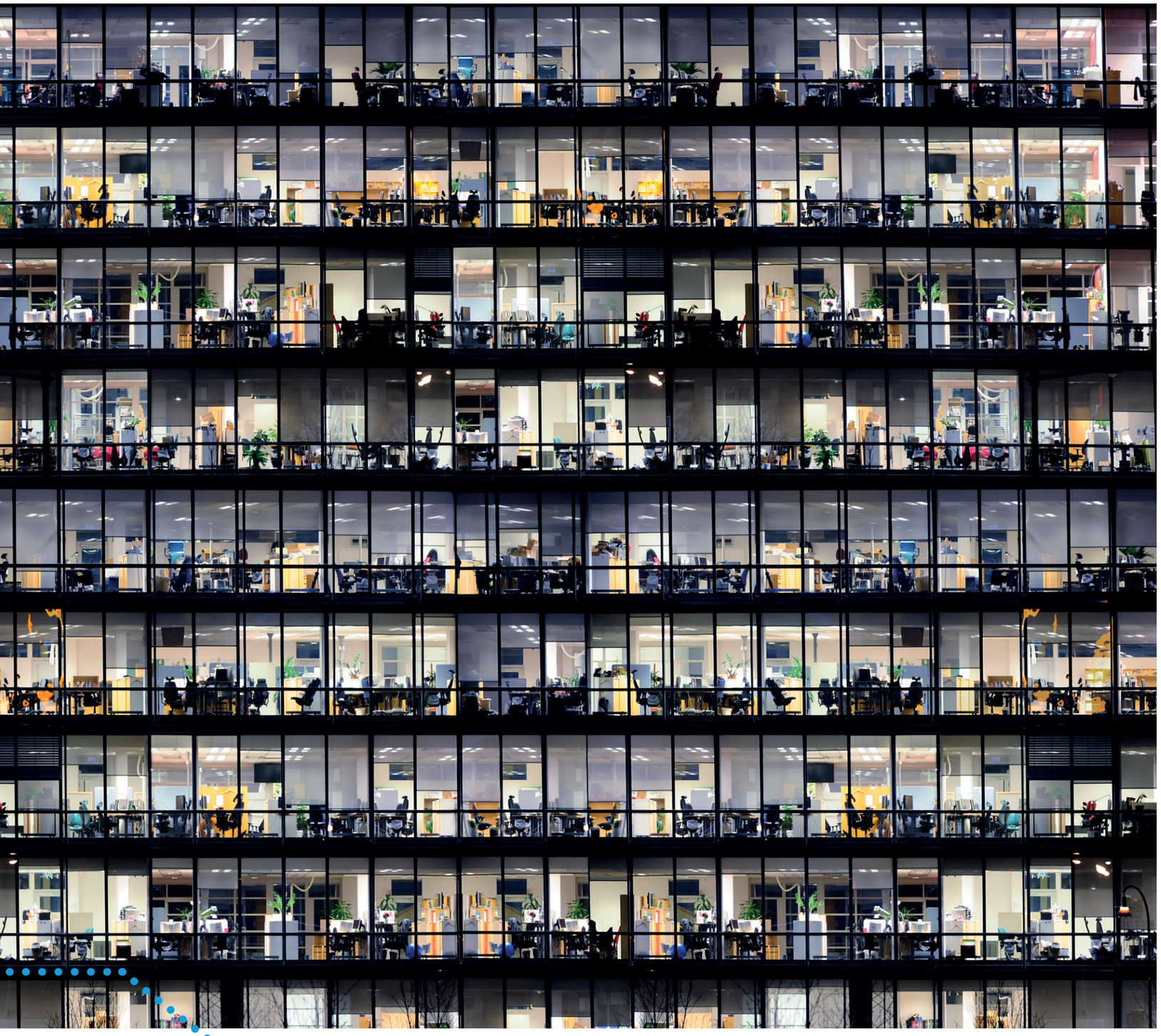
As nation states have invigorated their presence in cyberspace, incidents are increasing: espionage, sabotage and large-scale theft. Many organisations feel a false sense of security in their 'low profile'. They reckon that as they're not an interesting target, their risk is low. While this instinctively feels true, more organisations are discovering that being in a supply chain of a target increases your risk too. Finally, many get caught in the crossfires, and suffer collateral damage.

We're not saying that everyone will be a victim. We're saying there are new risks. A few years ago, commoditised cybercrime was all there was. Today, it is certain to target you, but the impact is low. Veteran criminals just might attack you, and if they're successful, your organisation will suffer.



Nation states probably won't target you, but they will attack someone in your network, and the impact is high.

We need to take this new paradigm into account.



Danut Niculae
Security Consultant
Operations Center
SecureLink

PENTESTING-STORIES

HOW MAY WE HACK YOU TODAY?

Breaches and hacks occur so often that we sometimes forget there are stories behind them. There is a chain of events leading up to a hack, and it's difficult to predict how and where criminals will strike.

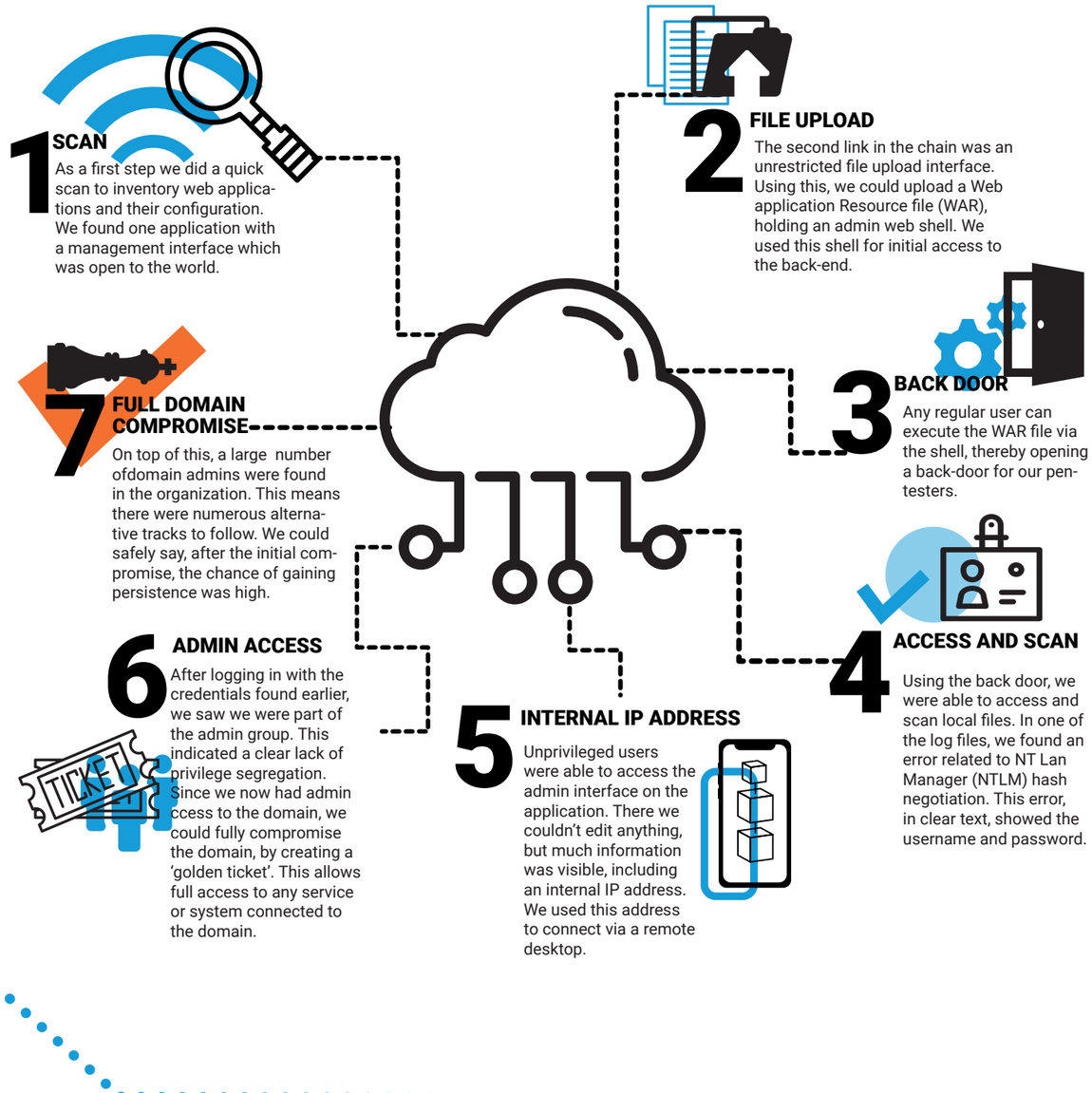
We always love reading pen-test stories. That's why we are sharing some stories ourselves. Our aim is to offer some detail on several attack methods and, at the same time, offering lessons learned.

STORY 1: ERRORS AND LIMITED HYGIENE LEAD TO FULL DOMAIN COMPROMISE

Our first story starts with a large commercial business service organisation, moving some of their customer-facing operations to a private cloud. We were asked to focus on this cloud infrastructure in our tests.

Ultimately, we found a chain of vulnerabilities and misconfigurations, allowing a full domain takeover.

The Golden Ticket attack is used by threat actors to obtain domain persistence. The technique leverages the lack of validation on the Kerberos authentication protocol in order to impersonate a particular user, valid or invalid. This is due to the fact that users who have a Ticket-Granting Ticket (TGT) in their current session are considered trusted by Kerberos and therefore can access any resource in the network.



MAY 2018 – PROCESS DOPPELGÄNGING

'Process Doppelgänging' sounds ominous in the best of situations. At the beginning of May, a ransomware was discovered using this technique. Fileless code injection takes advantage of a built-in Windows function and an undocumented implementation of the Windows process loader. It can replace a legitimate program with a malicious one in the memory. The upshot is that this malware could defeat most modern antivirus solutions and forensic tools. The malware is a 'SynAck' variant and the first, as far as we know, to leverage process Doppelgänging. It seems to target specific countries by crudely matching a list of users' installed keyboard layouts. If you use United States, Kuwait, Germany or Iran layouts, beware.

LESSONS LEARNED

The organization had actually spent a lot of effort to protect the external facing web application. However, what could be considered a combination of "details" lead to this fairly easy compromise. Outbound communication was unrestricted, which is an ideal situation for any attacker wishing to exfiltrate data.

1. Assure that web applications restrict file uploads. And, if they need them, to a certain type.
2. Always limit access. A first step is to limit access to internal IP addresses.
3. Avoid giving privileges to people that don't need it. Keep good security hygiene.
4. The root cause was a mis-configuration in one single application. A combination of other things made this breach huge.
5. Had the attack been real, the damage would be significant. As in reality it's very difficult (and takes a lot of time) to recover from a full compromise. One likely scenario is that the victim needs to rebuild the domain from scratch.

STORY 2: HARD SHELL, SOFT CENTER

Sometimes you're pressed for budget, pressed for time, or both. We understand that. So, when we get a request, along the lines of: "Could you just quickly invest a few days to check into something…" we take it seriously. A quick check is usually better than no check at all. In this case, we got the request to see what we could achieve, if we invested a few days in this project. The goal was to assess what would happen, if an attacker would walk into the office and connect to the network.

1 SCAN

Once we were connected, the first thing we saw is that we were in a Microsoft Windows Domain environment.
It was up-to-date and patched. Now, one thing we know about Windows is it has a default trust model. This model represents: once you're in, you're trusted.

2 PHISHING

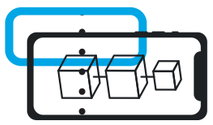
There are multiple ways to approach this model. One of our favorite ways is tricking a user with phishing into opening an email with a hidden malicious SCF file. This will include a link to an icon from our attacker's computer. As the machine will retrieve the icon from an Service Message Block (SMB) connection, it first needs to identify and authenticate itself before we can retrieve the icon. Hence the NTLMv2 hashes will be broadcasted with the authentication phase, which then is ours. But we didn't have this kind of time, and criminals trying to get to your things, won't either. So, we used a different method.

3 LINK-LOCAL MULTICAST NAME RESOLUTION

The process to target was 'Link-Local Multicast Name Resolution' (LLMNR). This process allowed us to resolve names without being connected to DNS servers. It was built upon the default trust model and was enabled by default, so it could be exploited. While there are good arguments against LLMNR, and you can disable it, doing so will likely cause difficulties, especially with legacy applications. So, for all practical purposes, the process is always there.

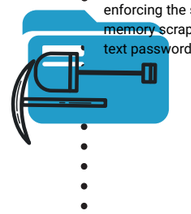
4 HIJACK LLMNR

If only we had a way to hijack LLMNR queries. The trick is to shout louder than your neighbor. "Hey, I know who this is!". There is a nifty tool available for this, from SpiderLabs, an American company. Listening to queries and responding to the potential victim's machine broadcast, that this machine is, in fact, the machine the queries are listening for. Because the victim's machine and user belong to a domain, and so is the machine they are trying to query, the victim will send encrypted authentication credentials and identity validation.



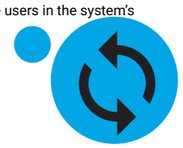
5 OBTAIN HIGHEST ACCESS LEVEL

We collected hundreds of password hashes this way. Using those hashes, we could relay them to another machine, accessible by a domain admin. As soon as the hashes are broadcasted by the administrator, we relay those hashes onto a machine and obtain the highest access level on a Windows machine; System.



7 GOLDEN TICKET

With this clear text domain admin password, we again generated a 'golden ticket', which means complete domain compromise and persistence for many years.



8 DOMAIN CONTROLLER SYNC

Once we had a domain admin, we used a secondary technique called Domain Controller Sync (DCSync) which tells the Domain Controller (DC) that there is a secondary domain controller and that we like to synchronize users. The DC then sends us all the users in the system's hashes.

9 FULL DOMAIN COMPROMISE

In the end, using the LLMNR hijacking tool, we came into possession of almost everyone's encrypted passwords, in this case thousands. Just to be sure, we tried to crack them in our offices, to check for alternate processes to
gain persistence. We were surprised to discover, that only within a few days, we had managed to crack half of them, on humble hardware. This meant, even if the initial compromised accounts were blocked, or disabled, we would have several ways back into the domain.

LESSONS LEARNED

This is a typical case of 'hard shell, soft center'. As soon as the organization gave us network access and a room to sit in, we were already in the soft center, and within a day the domain was fully compromised. This is due to many problems with the 'soft center' architecture: there was limited segmentation, an open trust model and an open network.

On top of this, the easy cracking of thousands of passwords, meant many passwords could be 'guessed'. Using several libraries of known passwords, we got half of them. There's always a balance between usability and password complexity, and here the balance was off.

A few days is usually too little for a thorough, valuable assessment of an app or architecture. In this case we could leverage the little time to justify a budget for more time. It really helped that the community is sharing great tools but bear in mind the bad guys use these tools too.

Finally, for a hacker, 'hard shell, soft center', is a dream situation. How to limit the consequences?

- Limit the hacker's access on the network as much as you can.
- Use segmentation, so that hackers bump into obstacles when they try to advance.
- Detect strange network behavior, such as the hijacking tool, and build a process so you can follow up on alerts.

Eward Driehuis
Chief Research Officer
SecureLink

PARADIGM-SHIFT

IS RANSOMWARE DEAD?

In early 2018, we observed cryptocurrency mining incidents taking over from ransomware incidents. In this chapter, we're going to dive into the numbers, interpret them, and add some historical context.

Cybercrime has historically had the widest and deepest impact on average technology users. Many people know someone who has been defrauded, or have been victims themselves. Although the scales are tipping as nation state threats and espionage are on the rise, for many, cybercrime is the biggest risk.

When investigating cybercrime, most of the research is into the technical side: malware, DNS names, indicators of compromise and Tactics, Techniques and Procedures (TTPs). Paradoxically, for criminals, the most difficult process in their work has always been laundering the money.

MONEY LAUNDRY IN RELATION TO ATTACK TYPES

There are roughly three phases in money laundry evolution:

- The money mule phase: criminal transactions are passed on from money mules (inbetweeners passing the money on to the next account). Typically used for lower amounts, it requires a lot of effort to manage mules.
- For larger amounts, criminals build networks of shell companies and financial insiders. They're able to move greater amounts of money at once.
- With electronic currencies like Bitcoin and Monero, laundry and transactions are taken care of in one step.

The last phase opened new doors for criminals and they started to actively look for new ways of making money through stealing electronic currency.

RANSOMWARE

Crypto ransomware, although in existence since 1989 (ominously called the AIDS virus), has been commoditised by a gang of banking fraudsters running GameOver ZeuS. In 2013, their technical lead created CryptoLocker. It was run from their existing fraud infrastructure and they infected around half a million victims. Out of those victims only a fraction paid, earning them an estimated $2 million on top of their fraud revenue (which was much, much larger). Dozens of copycat attacks followed but targeting random devices through botnets never led to large earnings for criminals. It's easy and cheap to deploy, though. In the last two years we've seen ransomware used in more bespoke scenarios: criminals hack corporate networks, destroy backups, and then ransom files for larger amounts.

COIN MINING

There's another way to earn bitcoins: mining them. Mining is the process of investing computing power in the network, for which random (lottery) rewards are extended. Criminals have dabbled in this process for some time now. They quickly understood that bitcoin is literally 'too difficult' to mine, so they looked for other coins. A few years ago, they occasionally mined for Litecoin, and today's coin of choice is Monero. Monero, incidentally, is less traceable than the others, so it also serves money laundry purposes better.

In our Cyber Defense Centers (CDC), we roughly identify three kinds of mining, in increasing shades of darker grey:

WHAT IS MINING?

Bitcoin and other coins are created on blockchain. It relies on a peer to peer network to maintain integrity and it gives (random) awards to those investing their computation power in the network.

The power is needed to make the integrity calculations, the random reward is a (part of a) coin. To increase chances of finding a coin, mining pools exist. The reward is split over the nodes participating in the pool.

Bitcoin was the first and the most widely adopted electronic currency. There is a maximum number of bitcoins that can be mined, and it gets increasingly hard to find one.

Power need increases exponentially. That's why criminals, in the mid 2010's looked at other coins to mine. Litecoin was easier on the CPU but was never a big money maker. Monero is today's coin of criminal choice. Partly because is easier to mine, partly because it's less traceable. This makes it more suitable for money laundry.

Browser mining: Visit a website and a JavaScript starts mining coins. Apart from a slow web browser, you won't be harmed. The strength of the attack is in the volume.

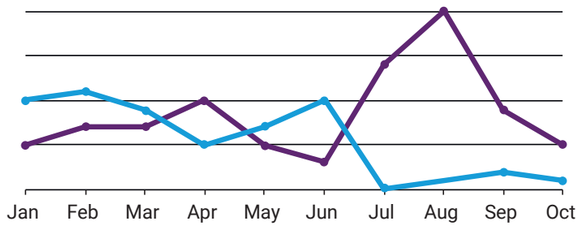
Insider mining: The sysadmin managing a network of several hundred PCs in your office deployed miners on them. If he/she makes sure they only run at night, this won't disrupt the important work you do during the day.

Mining botnets: Criminals repurpose their botnets to leverage your CPU power and send the results to a mining pool.

In our CDC, we've observed an absolute increase of both ransomware and coin mining. All three types of mining (browser, insider and botnets) are increasing, where of course the malware variant is the most purposely criminal. Mining grew harder in the first half of the year. In June, suddenly, coin mining activity halted and ransomware became the largest attack type in July. From there on we've seen a ransomware increase, correlating to the release of a new version of Gandcrab.

STATS FROM THE CDC

• **Ransomware** versus • **Cryptocurrency miner** attacks in 2018:



EXPLAINING THE TRENDLINES

It makes sense that coin mining became popular. It was a different and far easier way to steal electronic currency than with ransomware. If you look at it from an ROI perspective, ransomware has never quite been the money-maker the criminals hoped. A number of process flaws lie at the heart of the failure:

- Many will not pay and accept the damage in lost data.
- Many can recover through back-up and restore, and will not pay.
- Initially, the process was paying the same amount for every infected machine. This did not work in enterprises. PCs (the vulnerable machines) were just reinstalled. There was no good enterprise model in the beginning.
- You need to interact, or automate interaction, with your victim. Criminals can only return the keys if they get a unique identifier from their victim, match it to the appropriate key, and return it. It's a lot of work.
- Many want to pay but find it hard to buy and transfer electronic currency. Especially vulnerable targets, like elderly people, might want to pay, but they just can't.

For these reasons, only one in a hundred paid in early ransomware attacks. This led to the next issue: the rest of the victims needed to deal with data loss or recovery costs. There was a lot of collateral damage for a very modest return for the criminals. This in turn made the attacks riskier, because law enforcement and researchers are actively tracking you.

Coin mining doesn't require interaction with the victims and doesn't require payment. The coins are added automatedly to the pool where criminals can just get them. As far as a process goes, this is much easier for the criminals. The process is not destructive. Which means your victims see it as a lower risk, and so does law enforcement, researchers, and the board of directors.

So why, then, the sudden decline starting in June and the increase of ransomware?

The answer is prone to interpretation. First of all, there might have been events outside of our visibility. But if we disregard that, there might be more reasons:

- There's been quite a devaluation of electronic currency. End of December 2017 a bitcoin cost $20,000, while in June it was around $8,000, and in October a little bit above $6,000. With the value, the hype is decreasing, and the ROI of mining cryptocurrency is declining equally. This might have discouraged people to go after it.
- Browser mining is relatively easily blocked. After an introduction period, enterprises are getting their prevention in place. The number of attempts might be much higher than the number of successful attempts, but the result is less browser mining.
- Ransomware got in the news quite a bit in 2018. This might have motivated criminals to give it another go.

ATTACK EVOLUTION

At SecureLinks Cyber Defense Centers, we've seen a new type of ransomware attack on the rise, satisfying a more 'veteran' business model. Criminals penetrate networks in traditional ways (phishing, spam runs, watering holes). They then disrupt the target's recovery processes, for example, by destroying online back-ups meticulously. Only after they're assured that recovery is very difficult and/or expensive will they release the ransomware on the network. Then, they ask a 'Goldilocks' ransom: an amount that is not too high, not too low, but just right.

These attacks do not impact the graphs a lot, since they are happening less often than the commoditised ones. But their impact is a lot higher and often an emergency response team on-site supports the efforts of the victims.

We've seen similar trends in crypto mining. Criminals quietly enter a network and stay hidden, and go after server parks where a lot of CPU power is concentrated, like database clusters. We've also seen attacks where the criminals manage to infect a high number of endpoints, sometimes as many as one third of an enterprise network.

When these machines have been infected, they need to send the outcome of their calculations to a central hub. We've seen, in many cases, that prevention technology blocks this 'checkout process', and the mining networks, although present in the network, don't actually yield a profit for the criminals. At least these infections aren't destroying files, as ransomware does.

Sources: [31][32]: Details on page 59

CONCLUSION

Electronic currency, and certainly Monero, is a fantastic tool for criminals. Going after it is only natural for them. As it's always criminals (rookie or veteran) going after it, they're looking for the easiest way to do it. Automated mass ransomware automates a lot of the steps, but the process is too cumbersome and flawed. We see the future for ransomware in bespoke efforts: penetrating corporate networks, destroying back-ups, and then ransoming for a large amount.

Is coin mining the silver bullet for bad guys who want Monero? The process is automated and easy, the tools are automated and easy, there's no interaction needed and every infection yields results. But the pickings are still slim. In order to make any real money, criminals need tremendous volumes, thousands of tens of thousands of infections. That ups the ante but also the criminal's risk.

We reckon that for rookie criminals, mining might be interesting. For the high rollers, bespoke ransomware attacks and other extortion schemes are more interesting. The increase in bespoke ransomware attacks, destroying back-ups, is a worrying development.

With these attack types on the rise, we see that traditional ransomware and crypto mining will remain a nuisance, and an enticing entry-level attack type for criminals.

JUNE 2018 – WANNACRY WANNABE

We have seen lazy attacks before. It is also a known fact that criminals leverage each other's 'brand and reputation'. In this case, scammers borrowed Wannacry's bad reputation. By sending emails saying 'Hello! Wannacry is back!' they threatened victims, saying they would encrypt everything and demanding a ransom of 0.1 Bitcoin ($650 USD) to prevent it. The attack was not actually backed by anything. Anyone tech-savvy understands there is no technology available today that is able to encrypt across Mac, Windows, Android and iPhone. This is a lazy attack for sure, but alas, statistics dictate that, with a large enough number of emails, some will provide a payday for this type of criminal.

JUNE 2018 – VPNFILTER CONTINUES

The 'VPNFilter' malware, reported in our CDC security update, has expanded its list of affected home router devices. So far, 500,000 routers in over 50 countries have been affected by it. The list of known routers includes devices made by Linksys, Mikro Tik, Netgear, TP-Link, QNAP, Asus, D-Link, Huawei, Ubiquiti, UPVEL and ZTE. For more information on what the malware does, you can consult the CDC security update of May 2018. We recommend, if not done already, rebooting your router and running a firmware update if available. If your router or any other network device has an auto-update function, make sure to enable it.

JULY 2018 – NETSPECTRE

In July, researchers published the discovery of 'NetSpectre', a major evolution of the Spectre attack that allows an attacker to steal data remotely over a network. It originates from the original v1 vulnerability. Consequently, all CPUs affected by Spectre v1 are likely affected by NetSpectre. The attack is carried out remotely and does not require the initial steps of a victim downloading and running malicious code; it exploits a flaw in the speculative executive mechanism. Besides its innovative nature, NetSpectre is, as of now, still regarded as very slow, with an exfiltration speed of barely 15 bits/hour. It remains a theoretical threat for the time being.

JULY 2018 - MAJOR HEALTHCARE DATA BREACHES

Two major breaches within the healthcare sector were reported in July. In the first, a Canadian company which provides healthcare services experienced a data breach in which the attackers gained access to employee and patient health records, demanding a ransom to avoid them leaking the data online. Stolen data included personally identifiable information (PII) such as dates of birth, health numbers, phone numbers and details of past surgical procedures and medications. Interestingly, the hackers were the ones reporting the incident instead of the company itself. While the company stated afterwards that they registered 1,513 stolen records, the hackers sent a sample of 80,000 records that they were in possession of.

The second breach came to light on the 17th of July, as SingHealth, the largest healthcare group in Singapore, noted a massive data breach of 1.5 million records for patients who visited SingHealth clinics between May 2015 and July 2018. A particular health record of interest seemed to be that of Singapore's Prime Minister Lee Hsien Loong, which contained information about his medication. It was later concluded that the attack seemed well planned, sophisticated and targeted, even potentially nation state-sponsored.

Diana Selck-Paulsson
Threat Research Analyst / TDMC
SecureLink

SOCIAL ENGINEERING

WHY ARE WE ALWAYS FALLING FOR THIS?

A BEHAVIORAL PERSPECTIVE

Social engineering attacks have a great impact on organisations. After all, they are the first point of entry that might enable an attacker access, physically or virtually. In our Cyber Defense Centers (CDCs), we see a wide variety of adversaries using it, from junior cyber criminals to hardened APT actors. If we look at FBI and Europol statistics, we see social engineering is present in most of the top ten attacks.

Social engineering is a technique to deceive and manipulate victims for a certain goal, such as unauthorised access to a computer system for financial gain, causing harm or disruption. Social engineering can, in some cases, be considered as the 'art' of manipulation; it is very well planned, researched and executed in order to lure victims into revealing sensitive information or granting unauthorised access. Social engineering is an external information security threat.

The damage of a social engineering attack can be devastating. Social engineering is a way in. It can use several techniques, and, thus, reported social engineering attacks can be represented in several classifications of registered attacks. Among others, this could be Business Email Compromise (BEC) and phishing in all its variations, such as vhishing (by voice), smishing (by SMS) and pharming (via malicious code).

According to the Internet Crime Report [30], which is published every year by the FBI's Internet Crime Complaint Center (IC3), BEC was one of the most reported crimes in 2017, with an estimated financial loss of $676,151,185. Phishing/vhishing is number three, when you consider the number of victims. This means the IC3 has received 25,433 complaints that were actually reported by victims. The number of unreported attacks is assumed to be much higher, which means the financial loss of these attacks is expected to be much higher as well.

While social engineering is nothing new and has been around for many years, the process of social engineering attacks has been researched increasingly; thus, knowledge can be gained on why victims still fall for social engineering attacks. Simply put: who is to blame? The issue is twofold. Previous research has identified human factors as a cause. Secondly, the organisations' digital footprints expose information about their employees.

SOCIAL ENGINEERING ATTACKS - WHAT YOU SHOULD KNOW ABOUT THEM

As with any form of crime, social engineering attacks have patterns or a certain modus operandi with which they can be associated. Mitnick and Simon (2002) have developed a social engineering attack cycle that provides a sufficient framework for characterising it and analyses each phase[28]. A social engineering attack is usually initiated by some sort of communication, such as a phone call, an email, a face-to-face conversation, a letter or through storage media such as a USB key.

Before any means of communication is initiated, a social engineer will spend a certain amount of time on gathering information on their target(s). Consequently, a goal needs to be formed, and a target needs to be defined as either an individual person, a group of individuals or a whole organisation prior to a malicious request being sent.

POPULAR INITIAL ATTACK VECTORS

Phishing/ Spear phishing:

An attempt to obtain sensitive information through use of emails crafted to appear as legitimate business communication.

Spear phishing is more carefully crafted phishing with a narrower selection of targets. Probability of success is higher for spear phishing than regular mass phising campaigns.

Vishing:

Also known as voice phishing. Vhishing occurs when an employee receives a phone call in which the attacker will try to trick the employee into revealing sensitive information.

Baiting:

The attacker deliberately left a storage medium, such as a disk or USB device, to be found by the target or someone who is close to the target. This technique relies on human curiosity that will lead to unauthorised access to the organisation's internal network, sensitive information or financial information, depending on the attacker's end goal. Let's say an employee finds a USB device in the building of the organisation. The device is marked with the organisation's logo and the title 'Staff Planning 2018'. Would you not be curious? Or at least try to return it to its rightful owner due to sensitive information that seems to be stored on the device?

Pretexting:

The attacker is using a pre-defined scenario based on a prepared script. The goal is to create a situation in which the victim has to reveal sensitive information to solve this scenario, even though under normal circumstances the victim wouldn't disclose this information.

Once the target(s) and the goal are identified, the first contact will be initiated through a chosen communication medium. As the target varies in its form, so does the attacker; the social engineer can either be an individual or a group of people.

The length of a social engineering attack can vary greatly, from only a few minutes to months, depending on the goal and the target's resilience.

THE PSYCHOLOGY BEHIND IT – WHY DO PEOPLE STILL FALL FOR IT?

What makes us want to comply with malicious requests on a human level? Are there human traits that might be especially deceptive for the art of social engineering? Research has found a few characteristics that make some of us more prone to fall for social engineering. Some of our behavioral patterns might be more 'hard-coded' than others. For example, finding a USB flash drive laying on the floor near the entrance of one's organisation might trigger either the victim's curiosity, or the urge to return it to its owner, to do what's right.

Another example of this is tailgating. Tailgating means that the social engineer follows someone while the door is still open and thus overcomes the first obstacle of physical access control, be it through a door badge, a PIN code or other means of access control. Most individuals were raised with the value that holding a door open for someone else is just common manners and thus it is being polite in its most basic form. For a social engineer, this means that he or she only needs to exploit this human vulnerability to achieve physical access to their target or at least overcome the first physical hurdle.

Other behavioral patterns that make someone comply with a malicious request are, for example, building relationships. This is a social engineer attack that takes more time and makes someone (the victim) more likely to trust someone else (the attacker) when interacting in a positive way. Other human vulnerabilities can be exploited by availability: when it's a limited amount and/or only available during a short period of time. The availability trigger makes the victim want to react fast on something without considering possible risks.[26]

Similar to the tailgating example, there are other behavioral traits that might convince an individual to agree on certain requests if he or she thinks that this is something that is expected of him or her, and thus the right thing to do (social validity). Such as returning the media storage to its rightful owner, holding a door open for someone else, or helping someone out by providing sensitive information in order to solve a problem.

And finally, if an individual hesitates to comply to a certain situation, an authoritative figure might erase the last doubts. If such a figure requests a certain action of us, we are less likely to question this request. A social engineer leverages this vulnerability and will disguise him or herself behind a person with authority, such as a manager, or even a CEO.

Another human trait that correlates with victimisation is the initial level of trust. Individuals who show greater trust are more likely to be manipulated and exhibit a lower social engineering resilience. Resilience can be understood as the ability to cope with a certain situation, such as an attack, by using one's own social resources to resist or return to a state that is considered 'normal'. With a low social engineering resilience, a victim has no sufficient resources or skills to withdraw from the situation.

Another reason for risky behavior is that, besides manipulation techniques, victims might not be as aware of the value and sensitivity of the information. How could information about a supplier, like a cleaning company, be harmful? [27]

THE ORGANISATION ITSELF AS RISK FACILITATOR

Organisations today have a digital footprint. These have evolved over time and they're now an essential factor for competing with others on the market. While organisational websites aim for a good web presence and other commercial goals, they also enable attackers to find and select employees as potential targets. From there, an attacker can passively collect information about a targeted employee or group of employees. Recent research shows that due to available tools online, data collection of chosen targets, and thus potential ways in, is achievable by anyone through those tools (Edwards et al., 2016)[25]. One of the suggested tools is an OSINT platform, which is an open source intelligence platform that can be used by basically anyone who has access to an internet connection, no prior technical knowledge needed. Once the attacker has collected the full name or email address of their target, OSINT can be used to find vulnerabilities relevant for the social engineering attack and collect more information about them. This could be other email addresses that the victim is using privately, social media accounts (profile pairing based on username), and correlation of other web presences of the victim.

LINKEDIN AND TWITTER ARE VALUABLE TOOLS FOR SOCIAL ENGINEERS!

[25][26][27][28][30]: Details on page 59

Depending on the private digital footprint and personal attitude towards data privacy, possibilities to gather information about the victim's whereabouts, hobbies, posted content, writing style, etc. can be used in favour or against the victim, depending on the chosen method of the social engineering attack.

Besides collecting the full name and email address of a potential target, other information willingly provided by the organisation could lead to the selection of an employee as a target. Social media plays an important part in an organisation's online marketing strategy. If we look at LinkedIn and Twitter, both platforms offer an opportunity to the attacker. LinkedIn can be used for mapping an organisation and retrieving a list of employees based on self-reported roles on the employees' profiles (Edwards et al., 2016)[25]. If there is a mismatch between employees presented on the website and employees found on the LinkedIn profile due to the fact that not every employee might have a LinkedIn profile, the attacker can impersonate that 'missing' employee to connect to potential targets.

In the example of Twitter, an attacker can match the list of employees retrieved from the website with the profiles of the people that the organisation is following back.

According to a study, an organisation is most likely to follow its employees back than non-employees because it will be more selective in whom it follows in comparison to the number of 'Followed By'[25]. This means that employees can be found and linked with yet another profile in addition to their full name, email address, LinkedIn profile and other possible gathered information.

Additionally, mentioning a colleague or employee in social media provides information on business relationships and on links between targets. Based on job titles and business relationships, an attacker can even be selective, trying to exclude targets who seem to have knowledge in IT or show signs of having knowledge on security topics and thus be security aware (ibid.).

Needless to say, all of this is handed out willingly by the organisation and collected passively by an attacker without any active engagement and therefore the organisation itself can be considered as a risk facilitator.

Social engineering attacks distribution during 2018 (source: SecureLink CDCs)

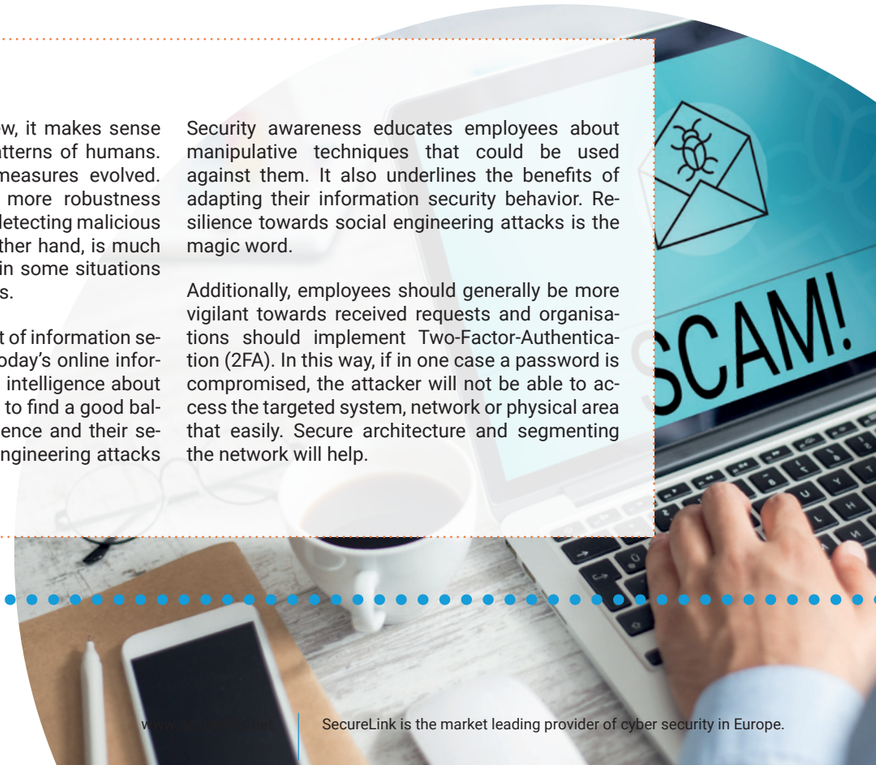
CONCLUSION

From an attacker's point of view, it makes sense to focus on the behavioural patterns of humans. Historically, technical countermeasures evolved. Nowadays, this shows much more robustness against phishing attempts and detecting malicious activities. The human, on the other hand, is much more complex, hard to predict in some situations and easy to manipulate in others.

Social engineering in the context of information security management leverages today's online information to help an attacker gain intelligence about their target. Organisations need to find a good balance between their online presence and their security posture, to make social engineering attacks more difficult.

Security awareness educates employees about manipulative techniques that could be used against them. It also underlines the benefits of adapting their information security behavior. Resilience towards social engineering attacks is the magic word.

Additionally, employees should generally be more vigilant towards received requests and organisations should implement Two-Factor-Authentication (2FA). In this way, if in one case a password is compromised, the attacker will not be able to access the targeted system, network or physical area that easily. Secure architecture and segmenting the network will help.



[25]: Details on page 59

Eward Driehuis
Chief Research Officer
SecureLink

SURVEY

THE FUTURE OF THREATS

As we're nearing the end of this report, we can't escape the inevitable: some predictions must be made. We are by no means downplaying the importance of predictions. Extrapolating data offers us some short-term relief. Usually, we want more certainty.

As we use a data-driven approach, extrapolating graphs typically means a little bit more of one thing and a little bit less of something else . We'll offer what we see.

GENERAL PREDICTIONS

Criminal-to-consumer attacks

Ransomware and cryptojacking will alternate. The lower the bitcoin price (there's been a 67% year-to-date price drop), the more ransomware we will see. Criminals will want to evolve from here to the next level.

Criminal-to-business attacks

Website skimming and credit card theft is on the increase, as criminals are gaining experience. Some veteran groups will perform more semi-targeted attacks and find new and creative ways to extort businesses, for example by destroying back-ups and then ransoming the network.

Nation state attacks

As geopolitical tensions are increasing, countries like North Korea and Russia will flex their muscles. Espionage is on the rise (from an already high level) due to trade wars adding to these tensions. There will probably be new nation state players in the game soon.

IN 2019, WHO DO YOU THINK WILL FORM THE BIGGEST THREAT FROM THE OUTSIDE?

PLEASE RATE THEIR THREAT LEVEL.

ABOUT THIS SURVEY

This said, what's going to be the next big new threat? Are adversaries turning the power of artificial intelligence on us? Will the internet of things (IoT) be our downfall? Will energy grids be consumed by malware?

We decided to release a little questionnaire among SecureLink personnel. Granted, there might be little science in here, but as we're tea-leaf reading, it's as good as any approach. The wisdom of hindsight will offer clarity in the future.

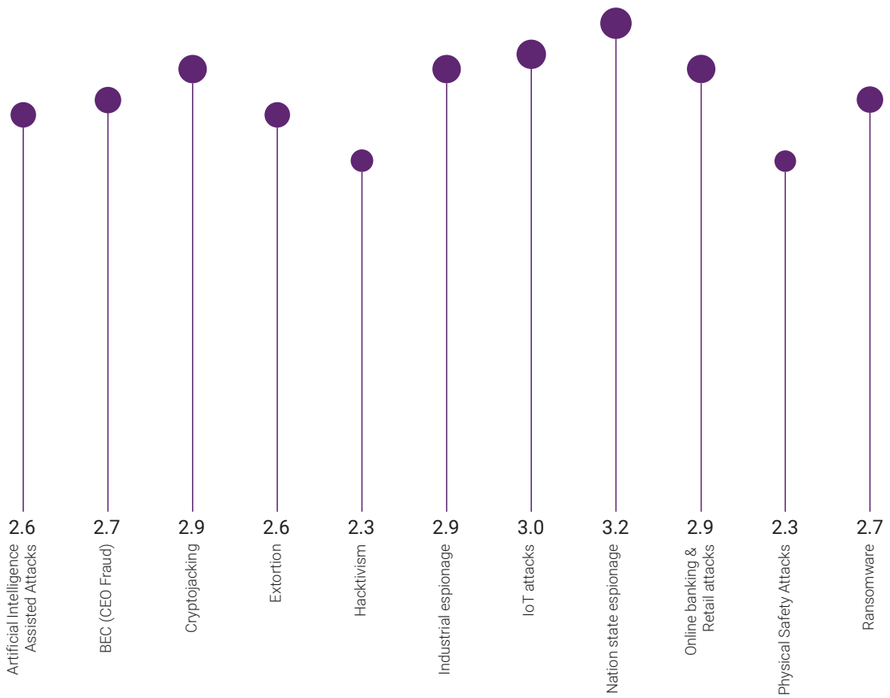
These predictions are provided by engineers (29%), management (20%), marketing and sales (18%), analysts (17%), and those in other roles (16%).

Nation states and organised criminals are perceived to be a higher future threat than lone wolves. This might be due to advances in endpoint security and the relative ease of detecting cryptomining, as we're seeing.

JULY 2018 - PYLOCKY

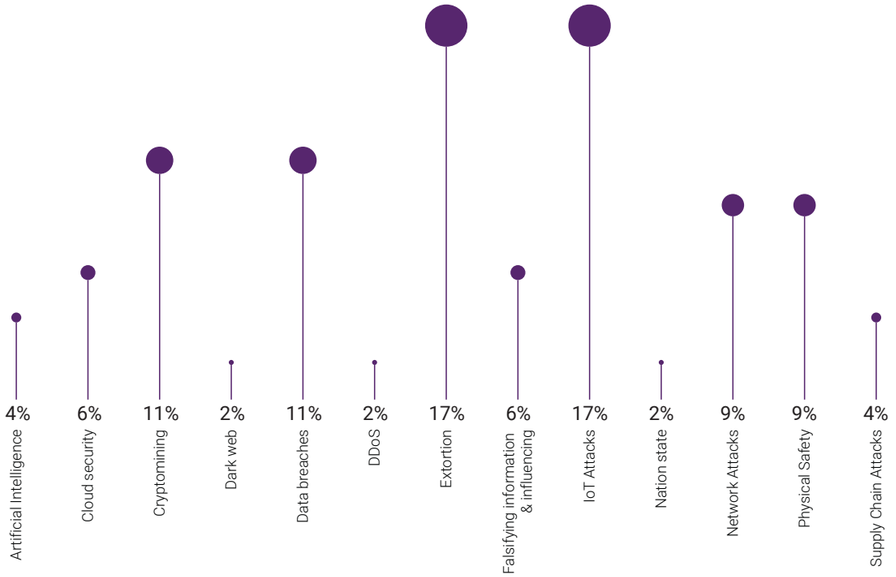
One of the notorious ransomwares, 'Locky', was honoured by a bad actor. Or, at least, they tried. Our CDC was among the first to detect this and did some research. The malware used many Locky references and was (surprisingly) written in Python. The signing certificate was issued to a small UK company, showing signs of compromise. It was issued on July 24th 2018, three days before the SecureLink CDC came across the malware sample in the wild. 'PyLocky' is mainly targeting France.

PLEASE RATE HOW BIG OF AN IMPACT THESE ATTACKS ARE GOING TO HAVE IN 2019



Again, nation state attacks will have an impact. IoT attacks come second. This might be because at SecureLink we feel IoT security is in its infancy.

GIVEN THE EVOLUTION IN TECH, RULES, REGULATIONS, AND GEO POLITICS, WHAT ARE THE NEW ATTACK VECTORS YOU SEE FOR 2019?



Looking at potential new attacks, we're fearing some net IoT attacks, but also expect creative extortion attacks (bear in mind, good old ransomware is also a form of extortion). Finally, we expect more data breach innovations, like 'Magecart'.

CONCLUSION

Our predictions, and please take them with a grain of salt, are that attacks on consumers will remain constant. Attacks on business will increase, as perpetrators find new ways to extort them.

We are already observing an increase in nation state attacks; our prediction is that this will continue in 2019. Adversaries might discover how to leverage the internet of things for profit or espionage. New and creative extortion methods will pop up. Finally, data breaches will increase as adversaries find more methods, such as website skimming.

Stefan Lager
Director Group Portfolio Management
SecureLink

SECURITY PREDICTIONS:

WHAT 2019 HAS IN STORE FOR US

A LOOK INTO THE FUTURE

Just a few years ago, threat modelling in cyberspace was easy. Cyber criminals were going after our money and malware outbreaks were recoverable. Over the years, threats have become more diverse, as espionage and geopolitics are now driving low-frequency, high-impact attacks.

Organisations are aiming to become more mature in security, with detection and response processes built on top of their prevention strategies.

PREVENTION

Although focus is shifting, let's not forget that every organisation needs prevention. Let's have a look at the vast amount of data impacting the defenses:

- 400,000+ new malware types are detected on VirusTotal every day
- 4,000+ new vulnerabilities are reported in the National Vulnerability Database every month
- 1,000,000+ threat intelligence indicators of compromise are updated every hour

The traditional security approach of reacting after an incident is detected and some type of signature or pattern to block it is written is not a futureproof strategy. On top of that, someone needs to get hit first. In many targeted attacks, this wait-and-see method is no longer valid.

INTELLIGENT SOLUTIONS. LITERALLY.

The best way to combat unknown threats in an efficient way is to be able to predict them. The most promising prediction technology is machine learning.

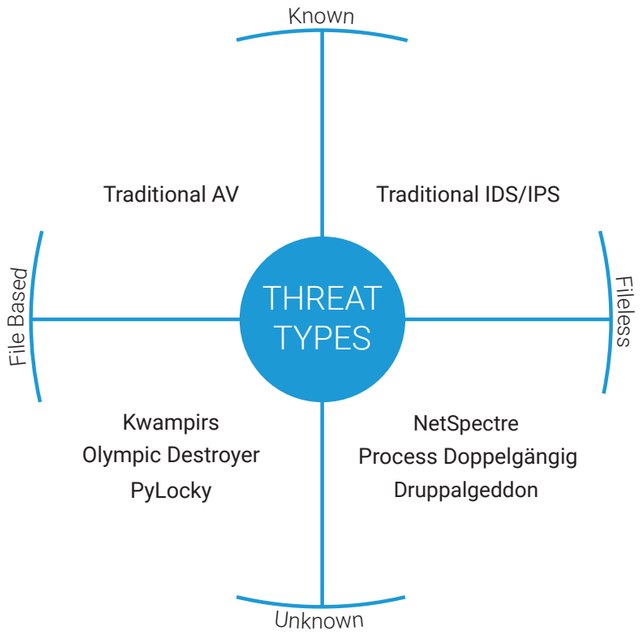
We spot this technology in next-generation antivirus platforms, which successfully leverage machine learning to predict the likelihood that an unknown file or behaviour is bad. We also see it in other platforms, like next-generation intrusion detection systems.

We must not forget that machine learning is just maths. Machine learning by itself will not solve any problems. It's how you implement it, train the details of the data and the amount of data, that will determine if it's useable or not. As machine learning has become a 'buzzword', many vendors claim to have machine learning technologies. We are in the business of verifying these claims and have tested them. And we experienced huge differences in how well they work.

We see organisations increasingly struggling with determining the best process and technology combinations to fit their risk appetites. Our advice is to ask for help and guidance on this journey.

HUMAN CAPITAL IS SCARCE IN CYBER

According to studies[32] 1.8 to 2 million cyber security professionals will be missing by 2022.



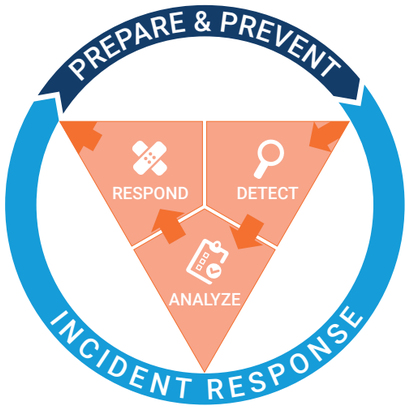
LIMIT THE IMPACT OF A BREACH

We recommend adopting the mindset of: 'My defences are going to get breached, so I need to control the harm when it happens'. Speedbumps around every corner make the hacker's life difficult.

- Segment your network to avoid adversaries having full access after an initial breach
- Avoid local admins on your endpoint, control your privileged accounts altogether
- Deploy multi-factor authentication
- Continuously scan for and remediate your vulnerabilities
- Make sure configurations are according to best practices

DETECTION & RESPONSE

Once you've accepted that your defences will be breached, you can start working on your detection and response strategy.



DETECTION AREAS

We listed the most adequate detection categories, while keeping the threat landscape in mind:

Endpoint

Endpoint Detection and Response (EDR) will detect traffic even if it's encrypted. That said, many devices (like Internet of Things devices) cannot receive an agent. On top of this, a breached endpoint can't be trusted. So, if your risk appetite is low, you need more than endpoint security.

Network

Solutions based on machine learning can detect all infected endpoints in the network, including those that cannot have an agent. This is very non-intrusive to deploy. Traffic encryption reduces detection abilities, and local escalations on endpoints are hard to detect. Detection of behaviour is difficult, and you need to map your network coverage really well, especially in complex environments.

Logs

Collecting logs and analysing them are basic requirements for threat detection and compliance reasons. Most companies start here. However, not everything is logged and not all data that is required for an investigation may be present. Many organisations reduce the number of logs collected for financial reasons. This will decrease your threat detection ability.

As you can see, balancing detection is important. The three approaches have different benefits and limitations. For many of our customers with a low risk appetite, a combination of two or even all of these satisfy their needs.

HUMAN CAPITAL
IS SCARCE IN
CYBER SECURITY

According to studies **1.8 to 2 million** cyber security professionals will be missing by 2022. [32]

[32]: Details on page 59

ANALYSIS

Finding good security analysts is a challenge these days. Human capital is scarce in cyber. As the threats are becoming more and more advanced and complex, the detection tools follow suit.

In the past, everything was black or white. Signature matched, or not. Today, machine learning is used by the most advanced security tools. Machine learning predicts, it does not know. Analysts need to understand all of the indicators and decide if it's good or bad. To do this right, you need context. The best tools in the markets are the ones that can combine good machine learning functionality with enriched context to help the analysts decide if a response is required or not.

RESPONSE

When an incident is escalated to a response team, they normally follow two steps. First, enrich the incident to better determine the appropriate response. Secondly, perform the response on either a user, endpoint or network level.

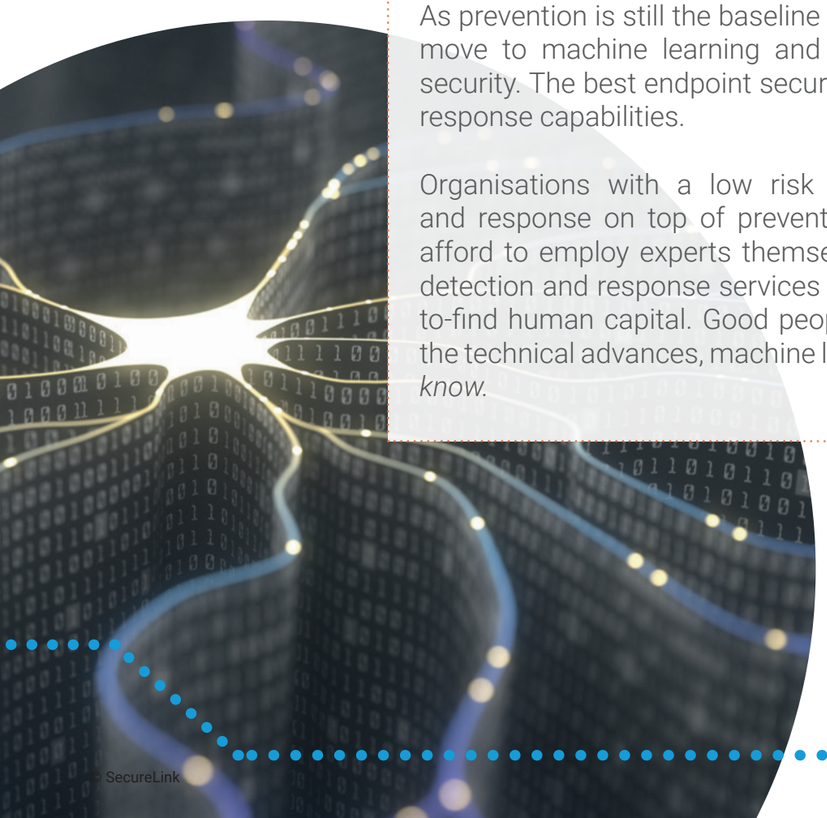
The quicker you respond, the less (financial) impact the breach will have. The challenge is that these tasks are as time-consuming as they are advanced.

To help with this challenge, there is a new type of solution in the marketplace called Security Orchestration, Automation and Response (SOAR). With the help of this solution and a subject matter expert, you can now deploy predefined playbooks that help with enrichment and response actions much faster and without requiring a high level of expertise from the operator.

CONCLUSION

As prevention is still the baseline for defenses, organisations move to machine learning and behaviour-based endpoint security. The best endpoint security feeds into detection and response capabilities.

Organisations with a low risk appetite deploy detection and response on top of prevention. Large enterprises can afford to employ experts themselves. For others, managed detection and response services can help alleviate the hard-to-find human capital. Good people are key: because for all the technical advances, machine learning predicts, it does not *know*.



AUGUST 2018 - DARK TEQUILA

'Dark Tequila', a malware campaign which has been ongoing for an astonishing five years, has been targeting Mexican users with a very sophisticated and complex malware. It contains modules, one of which is designed to steal banking information and login credentials for a big set of popular websites, including Amazon, Dropbox and Microsoft Office 365. Victims reported to have been infected either via spear phishing or contaminated USB devices, but only those who meet certain geolocation criteria are targeted.

SEPTEMBER 2018 - UEFI ROOTKIT

In late September, security researchers found the first-ever Unified Extensible Firmware Interface (UEFI) rootkit in the wild. Rootkits are malware designed to access areas of the OS otherwise forbidden, and this specific variant, 'LoJax', targets the UEFI, which is the successor or replacement for Basic Input/Output System (BIOS) and provides an interface between the OS and the firmware. Since UEFI resides below OS level, it is invisible to endpoint security. This makes these things very persistent and dangerous.

OCTOBER 2018 - KRAKEN

A new version of the 'Kraken' ransomware is on the market, which now uses Ransomware-as-a-Service (RaaS). For $50, you get a new build every 15 days. If the ransom gets paid, affiliates receive 80 percent, while 20 percent is given to the supplier. Then, the supplier provides the affiliate with the decryption key, which in turn is given to the victim. This is a new, appstore-like business model, which will likely see the individual criminals not get rich, but the suppliers might be striking gold with these models.

OCTOBER 2018 - LIBSSH 'JEDI MIND TRICK'

On the 16th of October, a critical vulnerability in libssh was disclosed. The vulnerability affects all versions of libssh 0.6 and later and enables an attacker to completely bypass the SSH authentication process. It's achieved by presenting the SSH server with a SSH2_MSG_USERAUTH_SUCCESS message instead of the expected message, SSH2_MSG_USERAUTH_REQUEST, which is given to initiate the authentication; a 'Jedi mind trick' which would be much more dangerous if libssh adoption were higher. Openssh, for example, doesn't use it.

REPORT SUMMARY:

WHAT HAVE WE LEARNED?

Within the first ten months of 2018, we've received over a quarter of a million alerts and investigated over twenty-thousand of them. Malware attacks account for the majority of these at 45%, with network and application anomalies coming in second at 36%. The rest is divided amongst policy breaches, social engineering and account anomalies.

Ransomware and cryptomining have overtaken each other several times throughout this year as criminals attempt to earn quick money through attacks on consumers. Social engineering is often the point of entry, for both criminals and nation states. We keep falling for it, because of how our brains are wired.

We have noticed a correlation between the number of alerts and the company size: in companies with upwards of 1,000 personnel, there is an average of 1.5 incidents per 100 personnel. The biggest companies have less at 1.3 incidents per 100 personnel. Organisations with under 1,000 personnel have significantly more incidents at 6.8 per 100 personnel. As these are relative numbers, in terms of the total number of alerts, the larger the company is, the more incidents it will encounter.

Considering different verticals, retail experiences mostly malware attacks. Other industries such as manufacturing, food, beverages and finance experience a high percentage malware attacks too, over 40%. Unsurprisingly, we see most social engineering in finance and retail. All verticals experience network and application anomalies, which often indicates something worse.

The healthcare industry has the highest percentage of these anomalies, with business services coming second and government and manufacturing tied for third place at 46%.

Nation state attacks have altered the threat landscape. With geographical conflict and trade wars fuelling these threats, the three incentives most observed are espionage, destruction, and government financing. The nations that are most discussed are Russia and North Korea, but China's activity is also on the rise.

While not everyone is a target for nation states, most victims are collateral damage or just happen to be in the supply chain of the actual target. This widens the risk to consumers, rather than just to an elite few.

Security solutions are continuously evolving. Prevention solutions are leveraging machine learning and artificial intelligence heavily, as are managed detection and response solutions. There is no single solution to detect all known threats today. A combination of looking at the endpoint, the network and/or logs is required. Furthermore, as machine learning predicts rather than knows, threat analysts are in high demand. Human capital is getting scarce.

2019 TIMELINE ▸

CONTRIBUTORS, SOURCES & LINKS

SOURCES

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

Statistics and numbers

All statistics originate from SecureLink's 6 Cyber Defense Centers

Geo politics

Concerning Russia

- [1] U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations | OPA |...
- [2] Dutch government says it disrupted Russian attempt to hack chemical weapons watchdog | Reuters
- [3] 12 Russian Agents Indicted in Mueller Investigation - The New York Times
- [4] Hackers Who Hit Winter Olympics 2018 Are Still Alive and Kicking
- [5] Olympic Destroyer: A False Flag Confusion Bomb | The first stop for security news | Threatpost
- [6] What to know about the Russian troll factory listed in Mueller's indictment - Vox
- [7] https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/
- [8] https://www.wired.com/story/white-house-russia-notpetya-attribution/
- [9] https://www.reuters.com/article/us-netherlands-cyber/dutch-tax-office-banks-hit-by-ddos-cyber-attacks
- [10] https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections/
- [11] APT28 Uses LoJax, First UEFI Rootkit Seen in the Wild
- [12] https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware

Concerning North Korea

- [13] https://www.cnbc.com/2018/06/11/donald-trump-and-kim-jong-un-meet-at-historic-summit-in-singapore.html
- [14] https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/
- [15] https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/
- [16] https://www.bbc.com/news/entertainment-arts-30512032
- [17] https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html
- [18] https://thenextweb.com/hardfork/2018/10/19/cryptocurrency-attack-report/

Concerning China

- [19] https://www.bbc.com/news/business-44529600
- [20] https://www.telegraph.co.uk/technology/2018/10/09/china-ahead-russia-biggest-state-sponsor-cyber-attacks-west/
- [21] https://www.bloomberg.com/news/articles/2018-09-19/chinese-cyber-spies-target-taiwan-s-leader-before-elections
- [22] https://www.theatlantic.com/international/archive/2018/10/meng-hongwei-china-interpol/572728/

Attack group information

- [23] https://attack.mitre.org/
- [24] https://www.fireeye.com/current-threats/apt-groups.html

Social engineering

- [25] Edwards M, Larson R, Green B, Rashid A, Baron A (2016) Panning for gold: Automatically analysing online social engineering attack surfaces. Computer & Security 69: 18-34.
- [26] Flores WR, Ekstedt M (2016) Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computer & Security 59: 26-44.
- [27] Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A (2017) Correlating human traits and cyber security behavior intentions. Computer & Security 73: 345-358.
- [28] Mitnick KD, Simon WL: The art of deception: controlling the human element of security. Indianapolis: Wiley Publishing, 2002.
- [29] Mouton F, Leenen L, Venter HS (2016) Social engineering attack examples, templates and scenarios. Computers & Security 59: 186-209.
- [30] FBI IC3 report, Internet Complaint Center, https://www.ic3.gov/default.aspx

Ransomware versus cryptojacking

- [31] North Korean hacker crew steals $571M in cryptocurrency across 5 attacks
- [32] Cryptocurrency theft hits nearly $1 billion in first nine months: report | Reuters

Predictions

- [33] Frost & Sullivan: 2017 Global Information Security Workforce Study (Europe) https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

Timelines

- https://www.reuters.com/article/us-netherlands-cyber/dutch-tax-office-banks-hit-by-ddos-cyber-attacks
- https://thehackernews.com/2018/01/healthcare-data-breach.html
- https://ds9a.nl/articles/posts/spectre-meltdown/
- https://securelink.net/resources/trending/flaws-in-almost-all-cpus-what-now/
- https://medium.com/@sekuryti/meltdown-more-like-letdown
- https://securelink.net/resources/trending/false-sense-security-parasite-infection/
- Mashable – Someone hacked a Tesla cloud account to mine cryptocurrency
- ZDNet – A giant botnet is forcing Windows servers to mine cryptocurrency
- Wikipedia – Bredolab botnet
- DigiCert – DigiCert Statement on Trustico Certificate Revocation
- Twitter – Geoffrey Thomas
- The Register – Suprise: Norks not actually behind Olympic Destoyer malware outbreak
- Business Insider – Winter Olympics organizers say the 'Olympic Destoyer' cyberattack took down their computer servers during opening ceremonies
- Forbes – How Similar Are WannaCry and Petya Ransomware?
- ZDNet – Mett coldroot, a nasty Mac trojan that went undetected for years
- The Hacker News – Hackers Exploit 'Telegram Messenger' Zero-Day Flaw to Spread Malware
- Chromium – utorrent: various JSON-RPC issues resulting in remote code execution, information disclosure, etc.
- TripWire – Poisoned BitTorrent client kickstarted malware outbreak that tried to infect 400,00 PCs
- https://securelink.net/resources/trending/january-2018/
- https://twitter.com/GUCCIFER_2
- https://www.forbes.com/sites/samarmarwan/2017/07/11/crowdstrike-helped-trace-the-dnc-hack-to-russia-now-business-is-booming/#7465613b4434
- https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer

- https://www.express.co.uk/news/world/935815/dnc-hacker-guccifer-2-mueller-investigation-donald-trump-election-russia-spy
- https://securelink.net/resources/trending/physical-safety-cyber-security-inching-closer/
- https://securelink.net/resources/trending/false-sense-security-parasite-infection/
- https://securelink.net/resources/trending/1-4-billion-passwords-discovered-should-you-care/
- GRIZZLY STEPPE – Russian Malicious Cyber Activity | US-CERT
- Medic! Orangeworm malware targets hospitals worldwide • The Register
- PyRoMine uses NSA exploits to mine Monero and disable security features
- https://twitter.com/SeamusHughes/status/988487142363025 40
- https://twitter.com/mikko/status/992379231479967745
- Proccess Doppelgänging: New Malware Evasion Technique Works on All Windows Versions
- EFAIL
- VPNFilter Update – VPNFilter exploits endpoints, targets new devices
- BackSwap Banking trojan Uses Never-Before-Seen Techniques
- Criminal movers and shakers, according to the FBI's IC3
- How to use login verification
- Olympic Destroyer is still alive – Securelist
- Olympic Destroyer: A False Flag Confusion Bomb | The first stop for security news | Threatpost
- WannaCry ransomware scam tries to extort money without actually infecting your computer
- https://blog.talosintelligence.com/2018/06/vpnfilter-update.html
- VPNFilter: New Router Malware with Destructive Capabilities | Symantec Blogs
- MyHeritage breach leaks millions of account details – The Verge
- MyHeritage Statement About a Cybersecurity Incident « MyHeritage Blog
- Thousands of patient records held for ransom in Ontario home care data breach, attackers claim | CBC News
- Singapore banks told to tighten data verification following SingHealth breach | ZDNet
- NetSpectre — New Remote Spectre Attack Steals Data Over the Network
- Vulnerability Note VU#304725 – Bluetooth implementations may not sufficiently validate elliptic curve parameters during …
- This new cryptomining malware targets business PCs and servers | ZDNet
- DNC warns candidates: Don't use ZTE or Huawei phones
- Democratic National Committee cyber attacks – Wikipedia
- Forbes: Why Fortnite won't be in the Play Store
- Faxploit: Breaking the Unthinkable | Check Point Software Blog
- A distilled threat with a Mexican flavor – Securelist
- https://tech.newstatesman.com/security/magecart-ba-ticketmaster
- https://www.forbes.com/sites/geoffwhite/2018/09/26/how-the-dridex-gang-makes-millions-from-bespoke-ransomware/#7fde8488440d
- https://securityintelligence.com/news/sednit-apt-group-uses-first-uefi-rootkit-detected-in-the-wild-to-execute-lojax-malware/
- https://www.bleepingcomputer.com/news/security/gandcrab-v5-released-with-random-extensions-and-new-html-ransom-note/
- https://arstechnica.com/information-technology/2018/10/bug-in-libssh-makes-it-amazingly-easy-for-hackers-to-gain-root-access/
- https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2

VERY SPECIAL THANKS
TO ALL CYBER HUNTERS, ANALYSTS AND ENGINEERS IN OUR CDCS.

ABOUT SECURELINK

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.