BROUGHT TO YOU BY FireEye

THE VISION

EXPERTISE DELIVERED STRAIGHT FROM THE FRONTLINES OF CYBER ATTACKS

THE PROTECTIVE STATE

The evolving role of Governments in cybersecurity

POLITICAL

The role of governments as their nations' primary provider of security against all threats is as compelling as ever. Yet few still have difficulty in grasping the rapid increase in interconnectedness and interdependency to determine how best to use a Regulate, Facilitate, Collaborate (RFC) model for the benefit of the private sector in creating a robust environment in which to conduct business and, increasingly, operate critical national infrastructure.

Because the security environment around us is complex – and different organisations are more receptive to certain measures than others – there's no one-size-fits-all solution. Whilst governments cannot control every aspect of cybersecurity, they can certainly help to shape its future, with the benefit of past lessons learned from other nations and different threats. With cybersecurity vital to a properly functioning and prosperous economy, it is critical that governments take the lead, and that this is recognized by its citizens.

So far, the 21st century has seen continued wide scale deregulation and privatisation, with many nations' critical infrastructure – in sectors such as energy, transport, finance and medicine – now in the hands of the private sector. These sectors are constantly under threat, not least because of increased globalisation of societies and economies. When these threats transpire, the potentially crippling effects are felt regionally, nationally and even globally.

The difficulty in securing critical infrastructures is due in part to the differing motives of the private and public sectors. One is corporate efficiency with maximized profit, often leading to the implementation of minimum levels of security in order. The latter is social order, national security and economic prosperity. Most developed countries have an 'all hazards' approach to address a wide range of threats to their population. Yet in some cases, governments are not even the primary security provider, such as when they don't provide close supervision of, or operational control over, critical infrastructures operated by the private sector.

This changing global landscape shouldn't mean a lesser responsibility for governments as legitimate providers of security, but rather that they should work to understand the changing world and their role within this new environment of increasing interconnectedness. For governments to be successful in this new environment, their remit must transcend their historical regulatory role and, instead, they must tackle how they can best assist the private sector to invest in security (facilitation), and how the public and private sectors can work together to improve the prevailing state of security (collaboration).

We cannot overstate the importance of developing strategies through a Regulate, Facilitate, Collaborate (RFC) framework, supported by the ability to draw upon lessons learned from other types of threat such as pandemics, war and terrorism.

THE EDITORS VIEW

2017: The worst year in cybersecurity history?

The Vision recalls on a year that the industry would be happy to consign to history.

You know when a cyber attack has reached a different level when its effects are global, and the general public talk about it. Last year, we witnessed not one, but three such incidents.

When WannaCry rampaged across the globe on May 12 2017, it infected more than 300,000 computers in 150 countries. In the UK alone, more than 80 National Health Service hospitals were impacted, resulting in cancelled surgeries and diverted ambulances. President Trump's homeland security adviser Tom Bossert attributed the attack to North Korea, saying: "North Korea has acted especially badly, largely unchecked, for more than a decade... WannaCry was indiscriminately reckless. If ordinary men and women around the world hadn't known the meaning of 'ransomware', they did now.

The following month, the NotPetya virus was launched in Ukraine and rapidly spread across the world. In a way, NotPetya's 'wiper' malware was even worse than WannaCry because affected organisations' data was destroyed, rather than merely held hostage. Consumer goods manufacturers, transport and logistics companies, pharmaceutical firms and utilities suffered reported losses of over $1 billion in economic losses.

The summer of cyber woe peaked in August when Equifax reported the loss of the sensitive personal records of 145 million people. The reaction was swift and severe. Within days, the market cap loss exceeded $5 billion. In the US, the FTC and both houses of Congress launched investigations. Equifax's CIO, CISO and, later CEO all fell on their swords in the aftermath.

2017: not a year to remember with fondness, nor one that anybody would like to see repeated.

Disturbing attack trends on industrial control systems

INDUSTRY

Until recently, cyber attacks occurred mainly in digital, rather than physical environments. But the ability for organisations to control and monitor more of their physical processes online drastically increases their vulnerability.

This is being increasingly exploited by nation states who are turning their sights toward chemical facilities, energy platforms, transportation networks, manufacturing plants, pipelines and water systems. Illicit reprogramming of safety instrumented systems in this critical national infrastructure, could bring catastrophic ramifications. Not only to physical assets, revenues and reputation, but potentially, a risk to human life and political stability.

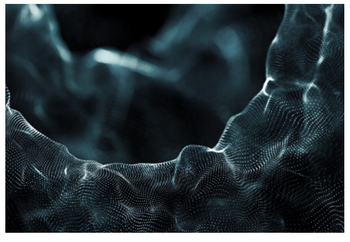
The type of systems in question monitor processes and trigger alarms if hazardous thresholds are reached. Last July, a joint US Department of Homeland Security / FBI bulletin warned that hackers had targeted such systems at the Wolf Creek nuclear power plant in Kansas. And our own investigators recently responded to an incident at a facility where an attacker deployed malware designed to manipulate safety systems. The consequences of emergency shutdown systems at a nuclear plant or chemical facility being manipulated or disabled are unthinkable.

On a similar note, please read our article describing the types of subversive concerns for industrial control systems, Page 6.

You are not an island - everybody is connected

INTERNATIONAL

Whilst today's unprecedented efficiency and speed of communication within organisations, across borders and between governments has brought untold benefits, it is causing headaches for CIOs, CISOs and others responsible for their organisations' cyber security.



Even if they are not a direct target, organisations may be affected indirectly due to connected infrastructure, as amply demonstrated in last year's widespread attacks by EternalPetya, WannaCry and BADRABBIT.

EternalPetya targeted businesses, airports and government departments in Ukraine, but also disrupted the operations of some multinational organisations with ties to the country. Any future cyber attacks on elements of Ukraine's critical infrastructure could cause substantial collateral damage to neighbouring countries and businesses operating in the region.

This serves as a warning of the potential for geopolitically motivated attacks to cause significant economic damage in the immediate and surrounding regions, wherever in the world an organisation is based or has operations. Nobody is in any doubt that, as hostile activity by nation states ramps up, these types of incident will increase, causing significant economic losses and widespread disruption.

Aside from this, organisations will continue to be caught out by more 'everyday' threats because basic precautions which should be regarded as a given are not enforced in many public and private sector organisations. Poor employee education, not updating systems and software, inadequate password control, poor supply chain due diligence and lack of governance are still making it simple for cyber criminals to operate with relative ease.

STATE OF THE NATIONS

FOUR NEW STATE-SPONSORED APTS COME TO THE FORE

INTERNATIONAL

At FireEye we label attackers as APT groups when we have solid evidence of their sponsoring nation, TTPs, target profile and attack motivations. Last year, four joined the ranks. Unlike many cyber criminals, APT attackers often pursue their targets over months or years, all the while adapting to attempts to remove them from the network and frequently targeting the same victim if their access is lost.

Russia and China still top the list of the most sophisticated adversaries, but May last year saw the first APT group attributed to a different nation and the number is increasing.

APT32 – aka the OceanLotus Group – has been targeting foreign corporations with investments in Vietnam as well as foreign governments, journalists, and dissidents since at least 2014. It's also believed that the group has targeted network security and technology infrastructure corporations with connections to foreign investors. It recently used social engineering emails with Microsoft ActiveMime file attachments to deliver malicious macros, downloaded from a remote server. We believe the group may be aligned with the Vietnamese national interest, with recent activity targeting private interests suggesting a threat to companies doing business or preparing to invest in Vietnam. Whilst being unclear about the group's specific motivation, we believe it could ultimately erode organisations' competitive advantage.

The Iranian threat group **APT33** has been conducting cyber espionage to collect information from defense, aerospace and petrochemical organisations since at least 2013. There's also evidence that suggests targeting of Saudi Arabian and western organisations that provide training, maintenance and support for the country's military and commercial fleets.

APT34, has been carrying out reconnaissance aligned with Iranian strategic interests since 2014. From monitoring the group's activity, we believe its main targets are Middle East-based financial, government, energy, chemical, telecommunications and other industries. There's strong evidence that the group is acting on behalf of the Iranian government.

APT35 – aka the Newscaster Team – is yet another threat group sponsored by the Iranian government, set up to carry out long-term, resource-heavy operations to collect strategic intelligence. Targets include the US and Middle Eastern military, diplomatic and government personnel and organisations in the media, energy, defense, engineering, business services and telecoms sectors.

Industries Investigated By Mandiant in 2017

Below shows the percentage of investigations for each industry carried out by Mandiant on targeted attack activity, conducted between October 1, 2016 and September 30, 2017.

Industry	Americas	APAC	EMEA	Global
Financial	17%	39%	24%	20%
Business & Professional Services	18%	10%	12%	16%
Other	12%	20%	22%	15%
Entertainment and Media	11%	7%	5%	10%
Healthcare	12%	2%	2%	9%
Government	6%	7%	18%	8%
High Tech	9%	10%	7%	8%
Retail and Hospitality	10%	2%	4%	8%
Energy	5%	2%	7%	5%

Source: M-Trends 2018 report

A FINANCIAL STRONGHOLD

HOW ONE BANK IS WINNING THE CYBER WAR WITH FIREEYE

"It was the Mandiant Incident Response services from FireEye that enabled us to understand the extent of the breach, reverse engineer all of the malware, and block further attempts."

— Spokesperson for Financial Services Provider

CASE STUDY

FireEye's expertise recently helped one of Asia's oldest and most profitable financial services providers to block a sustained cyber attack and prevent further breaches.

The attack first became apparent when bank staff were unable to access a domain controller — a server that responds to security authentication requests within a Windows Server domain. An internal investigation discovered a suspicious login account with domain administrator privileges, enabling unrestricted access to thousands of Windows servers and clients across the organisation. The potential for many host systems to have been compromised became quickly apparent.

The bank immediately retained our Mandiant Incident Response services to assist with an enterprise-wide investigation. Initial findings revealed that the breach followed a very familiar pattern: initial compromise, establishment of a foothold, escalation of privileges, internal reconnaissance and completion of mission.

The drawn-out campaign was uncovered before the attackers managed to accomplish their final goal. However, our team found that 96 systems had been breached, including 30 which had active malware running at the time of investigation. These included many advanced malware samples that were named to blend in with commonly-installed utilities on the bank's systems.

The attackers had planted backdoor and data loading programs before using screen grabbing and key logging to capture passwords from authenticated users. They had established their presence in the Microsoft Windows environment during the first month of the attack, but evaded detection by the bank's security infrastructure by using encryption, anti-forensics and other sophisticated techniques.

On the Mandiant team's advice, the bank put in measures that successfully blocked the attackers' infrastructure access. It also blocked comms between the bank and an infected subsidiary to halt any further lateral movement attempts, as well as removing compromised access control lists which had been fraudulently set up between the bank and the subsidiary.

26 servers & 70 workstations compromised

20 IP addresses & 5 fully qualified domain names associated with attackers' infrastructure

30 hosts identified with screen grabber malware artefacts

50+ user profiles infiltrated with key logging software

The attackers withdrew on realizing that the bank was committed to tracking their activity. An aggressive remediation plan was drawn up covering short, medium and long-term time frames, as guidance and supervision for several external vendors involved in executing the plan.

As is always the case, the profiles and characteristics used in the attack were uploaded to Mandiant Advanced Threat Response Centers around the world to further enhance our industry-leading global threat intelligence.

THE VOICE OF THE CLIENT

Jed Lumain, Chief Technology Officer, Rizal Commercial Banking Corporation, summarizes the benefits of partnering with FireEye.

"RCBC is one of the top universal banks in the Philippines. We are forth to eighth, depending on the metric that you want to use. We pride ourselves in being very innovative. We have the courage to go and try out new things.

"We are entrusted with the very precious personal information of our clients and we have to be very careful about that ... our business is trusted. In the last two or three years, crime suddenly took notice of the fact that you don't have to go to the bank to steal anything ... you can do it from wherever, and so that became a problem.

"We now have to worry about third party connections as well. We sort of prioritize what we call ingress points where these are potential areas where you could be breached. We knew that email is the easiest source, so we started with FireEye ES PX, which would actually mimic the person from clicking on that link or that attachment but safely, because they do it in a sandbox and they observe what happens to that payload. We also have the NX which actually guards our internet traffic or our HTTP traffic. It guards the browsing capabilities of all our employees and it guards our applications to where it connects to one of my favourite applications, the HX. We have several thousand endpoints and it's really impossible to monitor each one of them. HX gave me a way to protect all these endpoints even when they are travelling or outside the bank.

"You get to learn about the problems that others – probably across the globe – have encountered so you don't get to suffer the consequences. You cannot have a solution that works for a problem in the past; you have to have a solution that works for a problem for today. So far, we have had that kind of solution with FireEye.

"One of our basic strategies is to work with very few and select partners. We have viewed FireEye as one of those strategic partners ... both the people and the technology in FireEye are very reliable to us. FireEye is one of the main security companies out there, but it's probably the only one that comes up with innovations that are really relevant."

CURRENT CYBER THREATS TO INSURANCE AND FSI

ANALYSIS

The volume of sensitive data, high worth of client bases and prominent profiles of organisations in the financial services and insurance sectors make them continued key targets for attackers.

Here, we look at the three most likely types of attackers, and their motives.

Cybercriminals

Consumer services and mobile apps for personal financial management are key targets for credential theft. Existing infections such as bots can provide a way to gain access to large networks of high value victims.

Hacktivists

Hacktivists focusing on economic, social or political issues will seize the chance to disrupt and/or embarrass organisations they view as responsible, or at the very least have any involvement. Alternatively, they may draw attention to an unrelated issue using this highly visible platform.

APT groups

APT groups sponsored or otherwise associated with a country may conduct disruptive or destructive attacks to give their government leverage over an adversary.

We investigated a situation at a bank that had discovered criminals using fraudulent debit cards to make unauthorized ATM withdrawals in Eastern Europe. They had breached the bank's card management system and software, and then stolen, or attempted to steal, $150,000 from customer accounts. The breach had been made possible by an employee inadvertently visiting a website hosting a browser-based exploit that installed a backdoor on his or her system. This enabled the attackers to use the employee's legitimate credentials to gain access to the card management system and increase recorded balances and withdrawal limits for several customer accounts. They then changed the accounts' PINs, which allowed them to take the maximum amount from these accounts using seemingly legitimate credentials.

UNAUTHENTICATED PROTOCOLS

Many industrial control systems (ICS) protocols operate without authentication and therefore lack the ability to ensure that data comes from a trusted source. This enables any computer on the network to send commands that alter the physical process, such as changing the set point or sending an inaccurate measurement value to the Human Machine Interface (HMI).

This may in turn lead to incorrect process operation, with a number of potentially catastrophic results including damaged goods, damage or destruction of plant equipment, risk to personnel and environmental damage. Source authentication is normally achieved by verification and use of cryptographic keys.

OUTDATED HARDWARE

Because ICS hardware can be quietly running away in the background for decades, it may operate too simplistically or lack the processing power and memory to handle the threat environment present in modern network technology. We're referring to PLCs, RTUs, VFDs, protective relays, flow computers and gateway communicators.

Both these and software assets may also not be viable for monitoring or testing, and the older systems become, the fewer people possess detailed technical knowledge of their operation, and how to resolve problems. Not only that, but the effect of system changes could also be difficult to predict, bringing its own risks.

WEAK USER AUTHENTICATION

User authentication is the ability to ensure that only intended individuals can access a computer or use its programs. With ICS, this is commonly done by means of passwords, and here lies a problem. User authentication weaknesses in legacy systems often include passwords that are hard-coded, easily cracked or guessed, stored in easily recoverable formats or sent in clear text.

Any attacker who obtains these passwords may be able to interact with the controlled process at will. It's also not uncommon for users to not be included within corporate IT governance strategies, nor made aware of the implications of poor practice.

WHAT ABOUT THE PLANT FLOOR?

6 SUBVERSIVE CONCERNS FOR INDUSTRIAL ENVIRONMENTS

MANUFACTURING FEATURE

Industrial enterprises including electric utilities, petroleum companies, and manufacturing organisations invest heavily in industrial control systems (ICS). Without the technology operating the plant floor, their business doesn't exist.

Board members, executives, and security officers are often unaware that the technology operating the economic engine of their enterprise invites undetected subversion.

Here are the six key weaknesses that an adversary can use to undermine a plant's operation.

WEAK FILE INTEGRITY CHECKS

Integrity checking means being able to verify the integrity and origin of data or code, normally achieved by cryptographic verification. Unfortunately, this is deficient in ICS under the following circumstances:

Weak software signing: allows attackers to either mislead users into installing software that didn't originate from the vendor, or maybe replace legitimate files with malicious ones.

Weak firmware integrity checks: An attacker who can upload firmware – which is normally more difficult to change or update than software – can control the entire operation of the device.

Weak control logic integrity checks: inadequate checks mean that a PLC will accept the logic without verifying it, enabling unauthorized users to alter set points and take control of the equipment.

VULNERABLE WINDOWS OS

Engineering workstations and HMIs often run outdated and unpatched Microsoft Windows operating systems, leaving them exposed to known vulnerabilities when connected to the internet. In some cases, this means that attackers can access systems without needing specific knowledge, purely by using kits that incorporate exploits for older and non-updated systems.

This can happen even if patches are available (it's not difficult for attackers to obtain exploit code for vulnerabilities affecting supported Windows operating systems, let alone Microsoft Windows XP for which support ceased in 2014, and Windows Server 2003 and Small Business Server 2003, support for which ended in 2015).

UNDOCUMENTED THIRD-PARTY RELATIONSHIPS

In our experience, organisations running ICS seldom document and track third-party dependencies in the ICS software that they operate. Indeed, many vendors themselves may not immediately be able to lay their hands on what third-party components they use, making it difficult for them to share information about vulnerabilities with their customers.

An attacker who understands these dependencies can target ICS software that an organisation may not even know it has. Numerous vulnerabilities in ICS systems produced by global vendors have gone undetected – sometimes for years – for this very reason.

FOLLOW THE MONEY

DISSECTING THE OPERATIONSOF THE CYBER CRIME GROUP FIN6

0 9 8 5 7 9 2

FINANCIAL

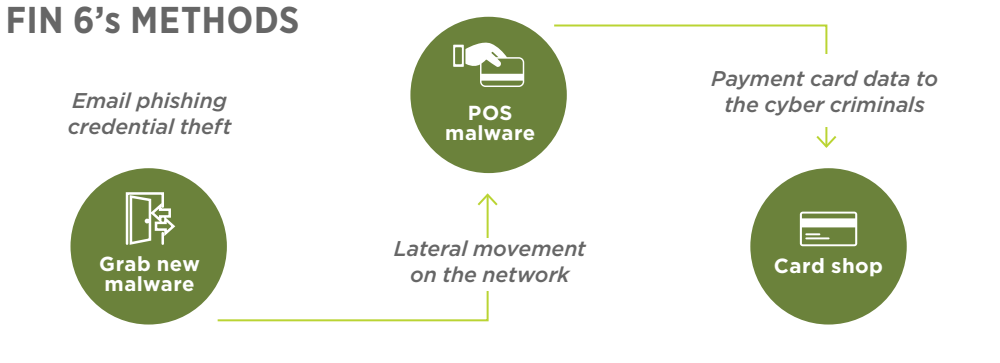
FireEye Threat Intelligence and our subsidiary iSIGHT Partners recently got together to illuminate the activities of a financial threat group known as FIN6. This unique combined insight provided extensive visibility into its operations, from initial intrusion to navigating victims' networks, and the sale of the stolen card data.

Frustratingly, reports on payment card intrusions and theft are often fragmentary, concerning individual elements of the attack rather than capturing the end-to-end cycle of compromise, data theft, illicit sale and use. This is due to the full scope of attacker activity traditionally occurring beyond the view of any one investigation team.

FireEye Threat Intelligence and iSIGHT Partners (part of FireEye) recently combined our research to illuminate the activities of one particular financial threat group. This combined insight has provided unique and extensive visibility into its operations – from initial intrusion to the methods used to navigate victims' networks to the sale of the stolen payment card data.

From tracking sophisticated FIN groups, we know that they employ a high level of planning, organisation and task management to accomplish their goals. They generally target a particular demographic or type of organisation, and their unwavering goal is financial gain from the data they steal. They profit from the direct sale of stolen data (as is the case with FIN6), unauthorized transfer of funds or, sometimes, insider trading.

FIN 6's METHODS



Three years ago, FireEye Threat Intelligence supported several Mandiant Consulting investigations in the hospitality and retail sectors where criminals had aggressively targeted point-of-sale (POS) systems, stealing millions of payment card numbers.

Benefiting from iSIGHT Partners' collected intelligence, we ascertained that the stolen payment card data was sold in an underground card 'shop' which is advertised on multiple underground cyber crime forums and offers millions of stolen payment card records. This closes the loop on the 'lifecycle' of cyber criminal activity and personifies one of the final stages of cyber criminals: monetizing their stolen data.

Having identified that data stolen from several of FIN6's victims was being sold by this shop as far back as 2014, we can safely conclude that it has almost certainly ended up in the hands of fraud operators across the world. In each case, the data began appearing in the shop within six months of the FIN6 breach and, in turn, was invariably purchased very soon afterwards. The volume of data through the shop varies according to the breach, but in some cases more than 10 million cards associated with a specific FIN6-linked breach have been identified. The same shop has sold data from millions of other cards, potentially linked to breaches perpetrated by other attackers.

Good threat intelligence comes from a combination of factors, requiring visibility into the threat landscape including both a broad view (the ability to identify activity across a range of countries, industries and organisations) and a deep view (the ability to gather detailed information about how cyber criminals operate). And, of course, it requires skilled analysts who are able to review, fuse and understand the available data.

In this case, the combined intelligence from our teams was able to not only identify malicious activity aimed at stealing payment card data, but provide a detailed of the operational lifecycle from compromise through monetization of that stolen data.

The account of FIN6 has shed valuable light on how real-world threat actors operate, not only in technical terms but compromise also into the human factor. It has identified interactions between different criminals or groups, and how it is not just data being bartered or sold in the underground, but also tools, credentials and access.