KPMG

cutting through complexity

Unknown threats in Sweden

Study publication

August 27, 2014

Executive summary

To many international organisations today, cyber attacks are no longer a matter of ”if” but ”when”. Recent cyber breaches at large organisations highlight more sophisticated, unnoticed and persistent cyber attacks. KPMG has conducted a study of the Swedish IT environment concerning targeted cyber attacks, a.k.a. Advanced Persistent Threats. The purpose of the study was to assess the cyber threat landscape in Sweden. KPMG partnered with FireEye and utilised its technology to conduct this research.

During recent years, we have observed an increase of severe cyber attacks targeting classified financial information, legal acts, business communication, and military or other governmental highly sensitive information. We have seen advanced targeted attacks occurring in Scandinavia, directed towards organisations such as Nordea, the Swedish Tax Authority and Telenor in Norway. In November 2013, it was discovered that the Finnish Ministry of Foreign Affairs had been exposed to cyber espionage for many years.

In order to investigate the “unknown threat” in Sweden, we have analysed the internet traffic of the participating organisations during a four week period. For the study to be representative of Sweden, we have invited organisations of different sizes, operating within a variety of verticals, in both the private and the public sector.

The study shows that all the organisations were exposed to infection attempts, where malware had successfully passed through the organisations’ perimeter defence and had reached internal hosts. The majority of the organisations were actually found to be infected as we observed communication attempts towards callback servers. The assumed purpose of those callback communications was to acquire complementary instructions, tools or malware in order to conduct further attacks from within the organisations’ networks. In most cases, we have also been able to observe attempts to exfiltrate data from the organisations.

Key findings

Highlights

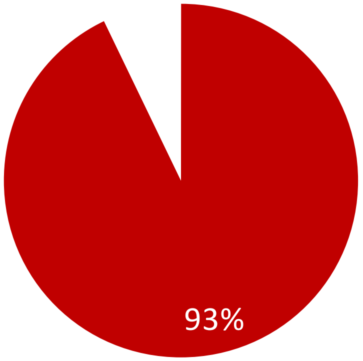
93% of the organisations were breached

79% were exfiltrating data

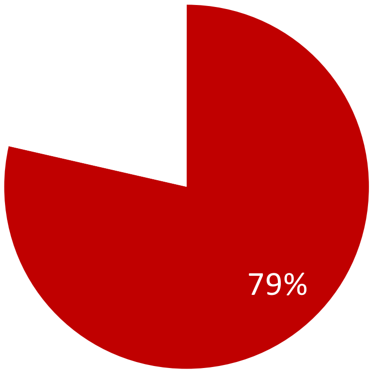
Findings revealed that a large majority of participating organisations were breached during the measurement period.
A breached organisation is defined by the existence of call-back traffic. When a malware has been executed on host level, the infection will eventually start to call a remote server and wait for a response. These servers are also known as Command and Control servers (CnC). The attacker can connect to the compromised host via the CnC server and provide further instructions in order to conduct a targeted attack on the inside of the organisation network. In this study 93% of the organisations had been breached and 79% were actually exfiltrating data.

Despite that not all organisations were breached, they all were exposed to malicious software that had penetrated the outer security perimeter. However, it is important to note that the presence of a malware on a client host does not necessarily imply that the host is infected. In order for the malware to successfully infect a host it has to exploit a vulnerability or abuse a weakness on that host. Further, the endpoint antivirus/antimalware software must have failed to block the infection.

Breached organisations



Exfiltrating organisations



Approach

Highlights

14 organisations

5 000 employees in average

~ 70 000 client hosts

15 586 security alerts

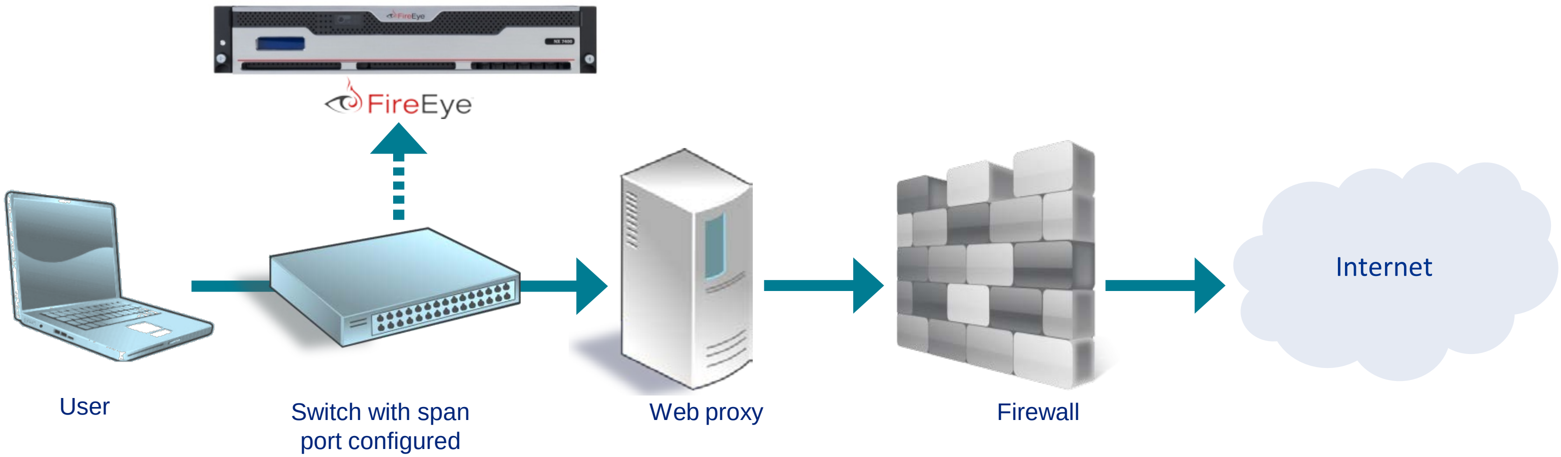
This study included 14 organisations, from which we selected a representative amount of client hosts to monitor during the month of June 2014. The incoming and outgoing internet traffic was monitored for a period of four weeks, between June 2 and June 27.

The average number of employees in these organisations is approximately 5 000. Due to the large variety of organisations participating to this study, in terms of vertical and size, we are confident to consider those organisations as a representative sample of the Swedish business landscape. For the purpose of the study, and in order to preserve the anonymity of the participating organisations, we have grouped organisations into six verticals: Finance, Government, Manufacturing, Retail, Industry and Service.

The study focused on gathering information related to malicious traffic. We only logged communications triggering security alerts. Since legitimate traffic was not logged we cannot track the exact amount of endpoints that were actually communicating through the FireEye appliances. However, we estimate the total number of unique internal hosts within participating organisations to approximately 70 000.

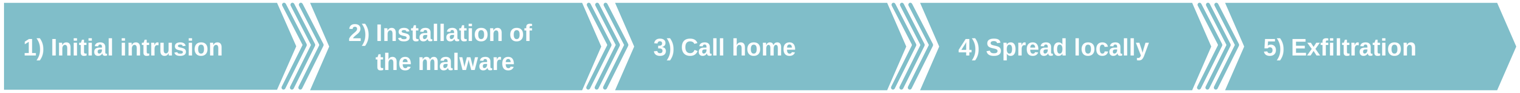
During the measurement period, we recorded a total of 15 586 security alerts.

Each organisation participating in the study were provided a FireEye NX 7400 appliance. The appliance was strategically placed on the edge of the organisation infrastructure, between the actual network security layers and the client hosts. The appliance was either positioned inline with the firewall or in mirror mode in order for the appliance to receive an integral copy of the traffic passing through the firewall and/or proxy. Both incoming and outgoing traffic were monitored.



Attack anatomy – five stages

Advanced Persistent Threat (APT) are composed of several penetration stages with the main ambition to gather sensitive information from a targeted organisation and exfiltrate it. A typical scenario combines sophisticated exploits to circumvent network security perimeters, execute malicious code and establish communication with remote servers, known as command and control (CnC) servers. An APT typically begins with an exploit against commonly used software, such as a web browser, email, office software, or media players. The target of an APT might not necessarily be the infected host itself but more likely another internal system, in the range of the compromised host. The last stage of an APT will be to exfiltrtate gathered information to a CnC. APT are often perpetrated by well organised and financed actors with long terms objectives to acquire specific information. An attack can be executed over a long period of time using a wide variety of malware to infiltrate the targeted organisation. An APT attack life cycle can be decomposed into five distinct stages.



1) Initial intrusion

2) Installation of the malware

3) Call home

4) Spread locally

5) Exfiltration

Stage 1 – Initial Intrusion

The first stage of a cyber attack is the exploitation of a targeted system. In this first step malware are delivered to the endpoint but can potentially be prevented by the organisation's perimeter security, e.g., firewall, proxy or antivirus/antimalware gateway. On the last resort, if undetected on the network level, the endpoint security measures might still stop the intrusion. System exploits are typically delivered through the Web (remote exploit) or through email (local exploit) as an attachment. The exploit code is embedded within a Web object (e.g. JavaScript, JPG) or file (e.g., XLS, PDF) to compromise the vulnerable OS or application enabling an attacker to run code, such as connect-back shellcode to call back to CnC servers and download more malware.

Stage 2 – Installation of the malware – user executes the vulnerable code

Once a victim system is exploited, arbitrary code is executed enabling malware to be installed on the compromised system. Visiting a web page or a simple double click of the mouse is all it takes for the user's system to become compromised and infected with the malware payload.

Stage 3 – Call home - Establish connection with a remote server

The malware installed during the prior stage often contains a Remote Administration Tool, or RAT. Once up and running, the RAT "calls home" by initiating an outbound connection, often an SSL-encrypted channel, between the infected computer and a CnC server operated by the APT actor. Sessions initiated from within the trusted network will most likely be undetected by traditional security measures.

Stage 4 – Spread locally and find other hosts to infect

It's highly unlikely that the initially breached end-user computing device contains strategic data. So the APT attacker must spread laterally through the network to search for high-value servers and databases containing sensitive data — the ultimate target of the APT. Lateral movement does not necessarily involve the use of malware or tools other than those already supplied by the compromised host operating system, such as command shells, NetBIOS commands, VNC, Windows Terminal Services, or other similar tools used by network administrators to service remote hosts. Once the ultimate target has been identified and adequate logon credentials are possessed, the attacker's hard work and determination begin to pay off.

Stage 5 – Exfiltration stage - sensitive information is stolen from the organisation

In this last stage, the attacker will exfiltrate data from the infected system. The attacker can take large amounts of data and compress it into small archive files in order to facilitate its transportation and remain undetected.

Source: FireEye

Malware types

Highlights

49% of the detected malwares were unknown

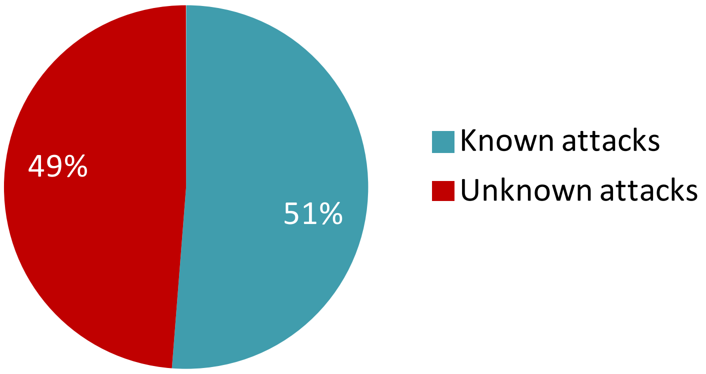
Out of15 586 security alerts, 49% were unknown threats. An unknown malware is a malicious code that has not yet been reported and classified by the internet security community, at the time of the attack. They can still be categorised through the analysis of their behaviour or content.

Depending on their type, malware can have many different purposes. It may aim to take control of a client, open a backdoor, utilise processor power, collect data, spread an attack or exfiltrate sensitive information. Considering that attacks might have started prior to or ended after the measurement period, it was not always possible to determine in which stage of the APT attack some of the detected malware was operating.

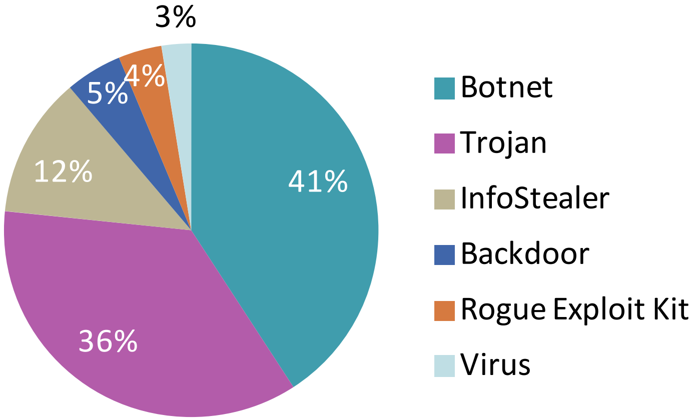
In the study, we did not correlate the FireEye alerts with other organisational security logs, such as firewall, proxy, antivirus/antimalware or system logs.
We are therefore not able to confirm, at the infection stage of an attack, if a malware was successfully penetrating the targeted host or propagating inside the organisation's network.

- **Trojan**: Malware taking control of the client
- **BackDoor**: Malware having full access to the client and can have lateral movement
- **Botnet**: Small, hidden programs that are often controlled by a malicious actor. Bots on a large number of client hosts can be connected to form a botnet.
- **InfoStealer**: Malware typically targeting financial information or users credentials/data
- **Rogue Exploit Kit**: "water holing" websites delivering malware via an exploit
- **Virus**: Known Virus/Worm

Known vs. unkown threats



Malware types



Malware objects and web exploits

Highlights

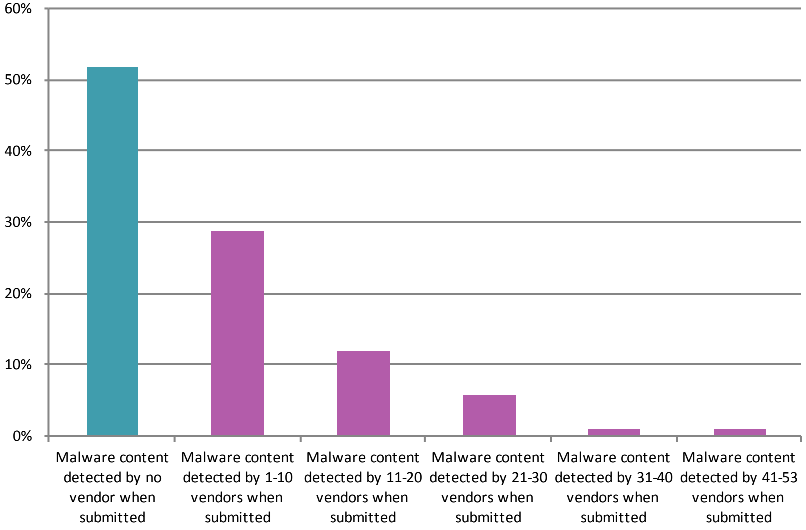
52% of the identified malware were unknown to antivirus vendors

We have identified a total of 195 unique malware objects also called binaries, that had penetrated the organisations' security perimeter. Each malware object , or binary, is identified with a signature (hash-code). The individual signatures of those binaries were tested against virustotal.com in order to identify whether the malware was known by the time of the attack. 52% of the malware were not yet registered by any of the main 53 antivirus vendors. It is important to note that the binary file might have been previously observed, but for different reasons not yet shared with the public.

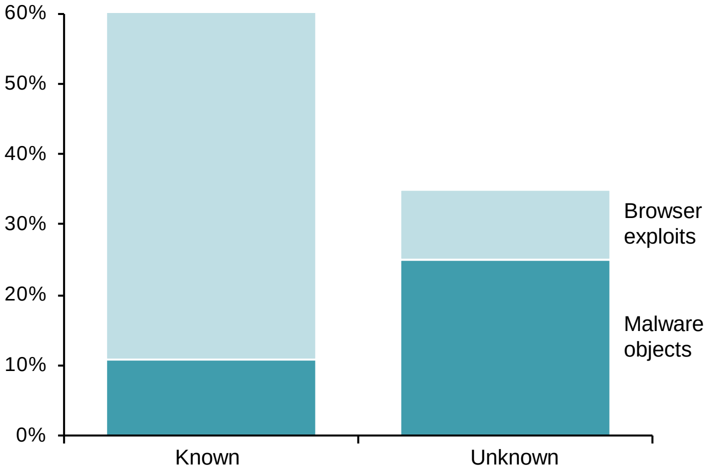
In addition to malware objects, we have also observed alerts that can be directly associated to Internet usage, i.e., internet related exploits. An exploit is a malicious code that aims to exploit a vulnerability in e.g., a web browser, plug-ins, etc.

Known browser exploits refers to URLs that are known to contain malicious content such as exploits.

Binary analysis



Distribution



Callbacks

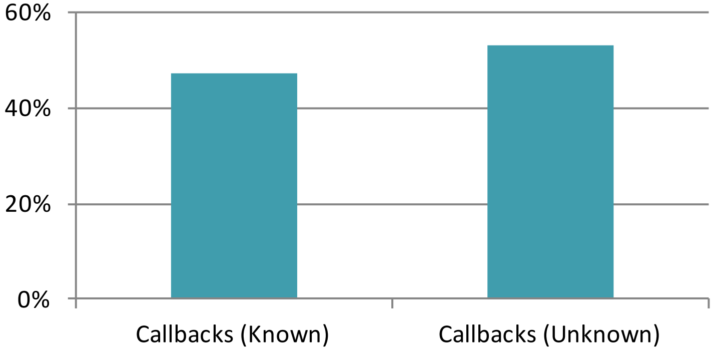
Highlights

83% of the detected callbacks were related to exfiltration

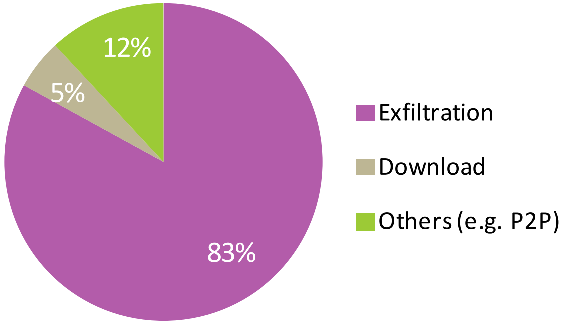
Out of 14 organisations, 13 were subjects to callback traffic indicating that they were actually breached. Moreover, in 11 organisations, we observed callbacks from the same IP addresses for which we had previously noted a malware object or web infection (browser exploit) activity within a few minutes. We can therefore safely assume that those malware attacks were successful and that the targeted hosts actually got infected. We observed a total of 535 such events.

Callbacks are outbound connections to CnC servers. CnC servers can serve diverse purposes during different stages of an attack and can therefore be divided into several categories. They are either used to retrieve further attack instructions, RAT software (remote administration tool) or more malware into the compromised host, or to exfiltrate gathered data at the latest stage of the attack. The majority of the CnC servers identified during the study were unknown, which means that they were probably staged for the purpose of a specific targeted attack. The staging area might be a cloud based virtual host that can instantly be wiped away after the data has been extracted.

Known vs. unknown destinations



Callback type



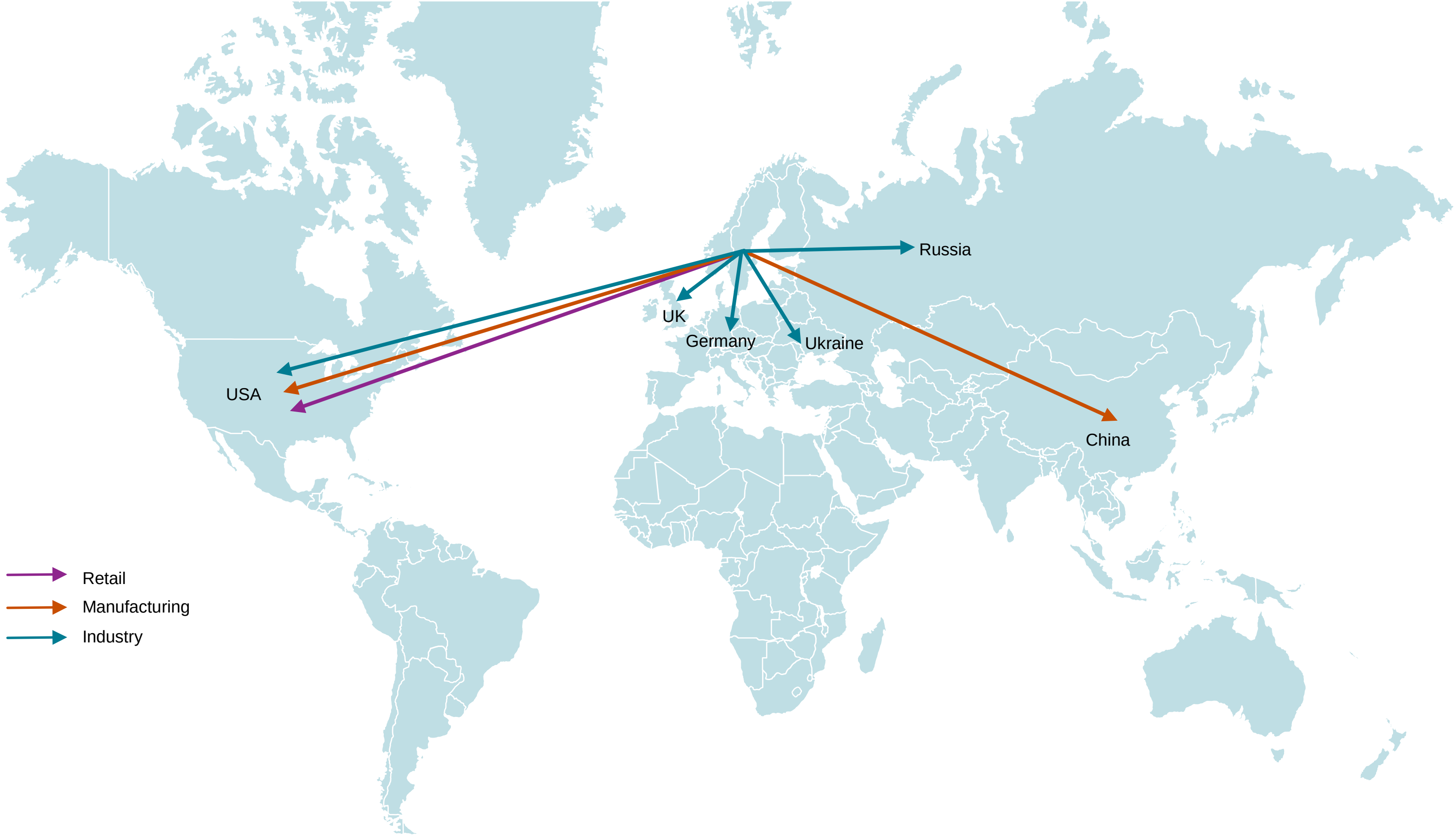
Callback destinations

Highlights

Manufacturing and Retail mainly exfiltrates towards USA

Industry mainly exfiltrates towards Ukraine, Russia and UK

CnC servers used to receive exfiltrated data are unlikely to be the final storage destination for the leaked information. CnC servers toward which data is posted are most likely used as bridges before the data is forwarded further on. Ninety percent of those CnC servers receiving exfiltrated data were located in the USA. That considered, we have observed that organisations that were subject to exfiltration were initiating callback connections to different destinations, depending on which vertical they belong too. For instance, industry organisations were mainly leaking towards Ukraine, UK and Russia. Some verticals did not have enough volume to determine a significant trend with regards to callback destinations.



Conclusion

Highlights

An average organisation generates 43 security incidents per day

Two infected hosts per organisation each day

According to this study, client hosts in an average organisation’s network are generating an aggregate average of 43 security incidents per day, with the most active organisation generating around 226 security events per day. We have also discovered that organisations were averaging two new infected devices each day and 30 exfiltrations of data per day.

Such figures illustrate how discouraging it is for security departments to manually manage alerts in order to discover which constitute a real and present threat. It also sheds light on why recent high profile attacks at organizations, like the Finnish Ministry of Foreign Affairs in Helsinki, were undetected for so long, since alerts don’t equal infections. The only way to determine if a device is infected is to correlate logged activities, which takes way too much time and man hours.

The ability to reduce the time spent to find infected devices is primordial. It takes months for organisations to discover a malicious breach and as much or longer to resolve it, according to the Verizon 2014 Data Breach Investigations Report. The ability to reduce the time-to-discovery to one day, would help organisations to block and contain ongoing attacks, stop further proliferation and prevent potential exfiltration of data. Not only is this a tremendous saving in time, but it significantly shrinks the window of when an organisation is vulnerable to a particular attack.

Are you ready to respond to cyber attacks?

Infection by malware or suspected intrusion into the organization's systems are serious incidents that could have a huge impact on business.

Despite best efforts to maintain a tight security posture across networks and systems; cyber attacks do, and more importantly will occur. Security is a process and not a solution, and as such safeguarding IT networks and sensitive data from electronic attack and exposure, both from the internet and internally at an organisation is a constant effort.

The slightest lapse in security processes could prove detrimental to an organisation, resulting in critical system down-time or exposure of sensitive corporate and customer information with severe consequences of financial and reputational loss, and potential legal implications.

Advanced Persistent Threats (APTs) to organisations are ever increasing with nefarious individuals or organisations devoting significant time and effort in gaining unauthorised and persistent access to networks and systems. APT actors will most likely not be discouraged if an occurrence of their targeted attacks was once successfully contained.

The inevitability of cyber attacks whether small isolated events or large-scale network compromise, outage or data exfiltration therefore presents a strong business case for developing an effective response capability.

A comprehensive cyber response capacity should cover all facets of proactive and reactive cyber response, consisting of Prepare & Train, Detect & Initiate, Contain & Investigate, Recover and Report & Improve.

Source: KPMG UK

Credits

Quentin Authelet

Head of Information Security &
IT Governance Services

KPMG AB

T: +46 8 723 91 00

E: quentin.authelet@kpmg.se

This study was conducted by KPMG Sweden and FireEye.

KPMG cutting through complexity™

FireEye™