MANDIANT
A FireEye® Company

MANDIANT CONSULTING

M-TRENDS 2016

EMEA EDITION

AUTHORS

Bill Hau
Matt Penrose
Tom Hall
Matias Bevilacqua

SPECIAL REPORT / JUNE 2016

FireEye®

INTRODUCTION

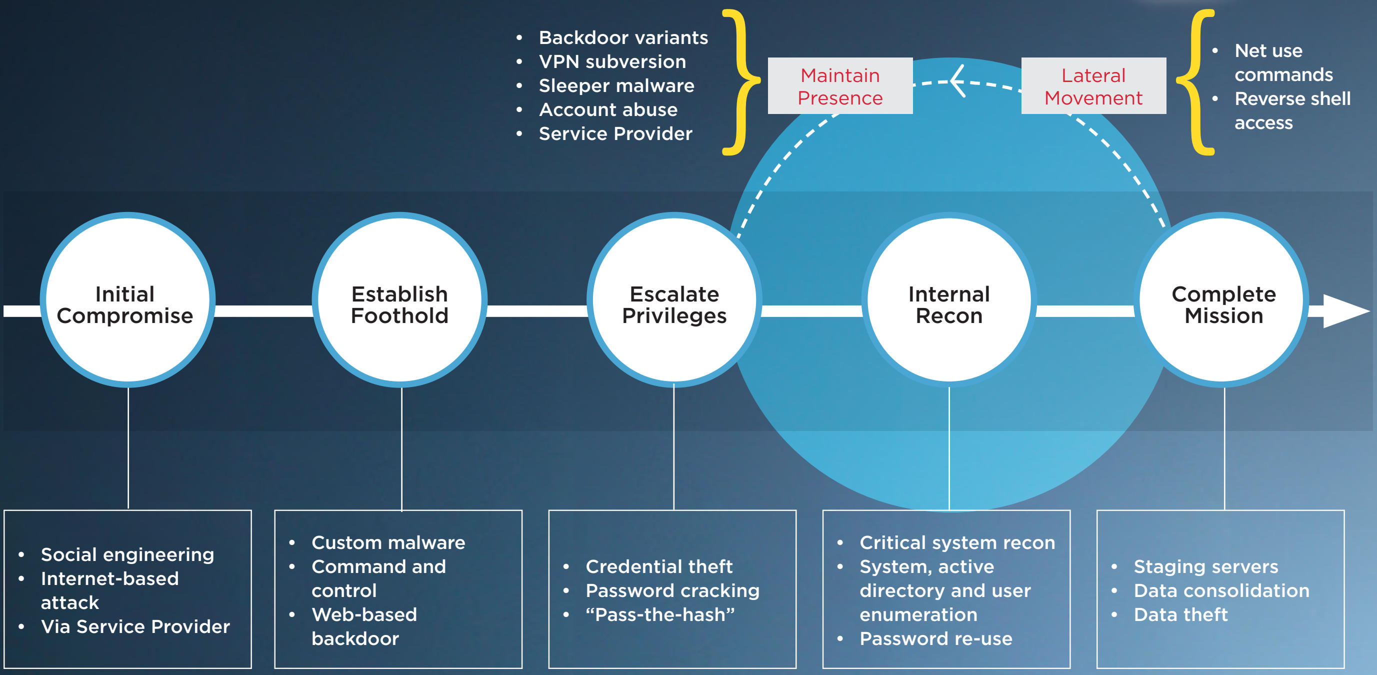
Since 2010, Mandiant, a FireEye company, has revealed trends, statistics and case studies of cyber attacks involving advanced threat actors. Mandiant Consulting responded to some of the most high profile breaches in Europe, Middle East and Africa (EMEA) in 2015. During this time we collected and analysed statistics and attacker trends from our investigations.

This is the first M-Trends reports focused on the EMEA region. It aims to empower organisations and the security community with knowledge of the unique challenges faced in the region by advanced attackers in order for you to improve your security posture.

The attack lifecycle model, depicted below, shows the typical phases of an attacker. During a breach, an attacker will usually infect a machine, move laterally within an environment and establish persistence – this eventually leads to completing the mission, usually by stealing sensitive data. This report drills down into the statistics collected during our investigations to give a perspective on the risks faced by organisations in this region.

In this report, we will review how our clients discover breaches in the first place, how attackers typically stay hidden in victim environments, how attackers move within a compromised network and how they steal data. The report will then analyse some of the key data points from the previous year and provide some guidance on improving any organisation's security posture.

Figure 1: Attack lifecycle model complemented with classic attacker techniques



CONTENTS

EXECUTIVE SUMMARY

IN FEBRUARY 2016, WE RELEASED OUR ANNUAL M-TRENDS REPORT, THAT TOOK A MACRO LOOK AT TRENDS AND STATISTICS FROM THE BREACHES WE RESPONDED TO IN 2015 FROM AROUND THE WORLD. THIS DOCUMENT TAKES A MICRO LOOK AT THE EUROPE, MIDDLE EAST AND AFRICA (EMEA) BREACHES.

The key observations we made for EMEA were:

- The median time to discovery of an attack was 469 days after the initial compromise, versus a global median time of 146 days.
- Organisations discovered breaches internally 88% of the time, versus a global average of only 47%.
- Breach notifications in EMEA by law enforcement agencies or government entities occurred far less than what we see elsewhere in the world.
- Mandiant Consulting was engaged by many organisations that have already conducted forensic investigations (internally, or using third parties), but failed to eradicate the attackers from their environments.

These observations make it clear that organisations in EMEA should focus on enhancing their overall security posture through improved incident detection and response capabilities.

BY THE NUMBERS

What are the challenges?

The global M-Trends 2016 report[1] revealed new developments among breaches. More breaches became public than at any other time in the past (both voluntarily and involuntarily), meaning organisations who were targeted were often put under the microscope by the media, industry regulators and shareholders to minimise the impact and handle the incident quickly. At the same time the location and motives of the attackers were more diverse, meaning some attackers were motivated by money, some claimed to be retaliating for political purposes, and others simply wanted to cause embarrassment. These trends were also echoed in EMEA.

What did Mandiant Consulting observe during our investigations?

The EMEA M-Trends statistics reveal that existing security controls in EMEA organisations are not up to the challenge of stopping or consistently detecting advanced threat actors. Figure 2 provides statistics for the breaches we responded to in the EMEA region during 2015.

Figure 2: Investigation averages

CATEGORY	AVERAGE
Number of systems analysed in an organisation	40,167
Number of systems compromised by threat actors	40
Number of compromised user accounts used by threat actors	37
Number of compromised admin accounts used by threat actors	7
Amount of stolen data	2.6 GB
Number of days compromise went undiscovered	469

[1] Mandiant, a FireEye company. "M-Trends 2016." February 2016.

Average number of days compromise went undiscovered

The median dwell time (time between compromise and detection) in the EMEA region was 469 days – or more than 15 months – versus a global median dwell time of 146 days. The reason for this gap is that the global statistic includes the U.S., where the security maturity baseline is higher and proactive threat hunting is slowly becoming a common occupation of Tier-3 security operations centres (SOCs) or the more advanced Fusion Centres.

Fifteen months provide ample time for any attacker to progress through the full attack lifecycle and achieve multiple goals within their mission objectives. To put this into perspective, Mandiant's Red Team, on average, is able to obtain access to domain administrator credentials within three days of gaining initial access to an environment. Once domain administrator credentials are stolen, it is only a matter of time before an attacker is able to locate and gain access to desired information.

Average number of machines analysed in an organisation

Our experience in EMEA indicates that that organisations typically perform some level of analysis (internally or via a third party company) prior to hiring Mandiant Consulting. Typically, these investigations only include a handful of machines, meaning they do not know the full extent of the incident (the scope). Therefore organisations and governments were often re-compromised within months after an initial forensic investigation.

Observers of the statistics will note that the average number of machines we investigated during a breach was 40,167. Mandiant Consulting advocates a comprehensive investigation using high fidelity intelligence and a rapid scalable methodology covering every system in the environment. This approach enables the organisation to fully understand the scope, paving the way for successful eradication and remediation of the threat actor from their network. It is critical to ensure that all systems on a network, not just a subset, are included in the analysis to ensure a comprehensive investigation and remediation effort.

In EMEA, many organisations use the traditional investigation methodology based on the 'follow the bread crumbs' approach that's restricted to analysing only a handful of machines, and 'spidering out' from those machines. For enterprise scale incidents, we consider this approach inadequate since it will likely not find all the machines accessed by the threat actor, thus missing the true scope of the incident. As a result, attackers either continue to remain within the environment even after the investigation concludes, or they are able to gain unauthorised access to the organisation again in subsequent weeks/months.

Average number of systems compromised by threat actors

Of the 40,167 systems investigated on average per victim environment, only 40 systems were found to be compromised on average (or roughly .001% of all systems). This reinforces the fact that investigators are truly looking for the needle in the haystack when trying to determine the timeline of a breach.

It is important to mention that while the attacker may theoretically have full access to the environment once they have escalated privileges, it is not in their best interest to operate on, or compromise, a large number of systems. Attackers normally keep their footprint to a small percentage of the environment to better avoid detection.

Average number of compromised user and admin accounts used by threat actor

Once an attacker has gained initial access to an environment they will often start escalating privileges. Attackers often try to get domain or local administrator (or root) privileges as quickly as possible. These accounts are used for lateral movement, access to applications and databases, for remote access, or just to ensure continued access in the case where a set of credentials gets changed. From a forensic investigation point of view, investigators must hunt for threat actors posing as 'an insider'; using legitimate credentials to blend in with normal user activity. Mandiant Consulting observed that attackers used an average of 37 user accounts and seven administrator-level accounts during a compromise. Determining which compromised credentials were utilised during any one attack is crucial to understanding the full extent of the incident.

Typically, threat actors require access to different systems to fulfill their objectives, potentially requiring multiple sets of credentials. Examples of sets of credentials sought after by attackers include:

Local administrator credentials to achieve persistence for malware and to spread laterally on other desktops and laptops.

Domain administrator credentials to achieve persistence at the domain level, including on servers.

Database credentials to access customer records stored in applications.

Domain credentials for VPN and other remote access tools to leverage legitimate ingress vectors into the organisation and blend in with regular users.

Application credentials with access to financial systems to manipulate money transfers.

During sustained breaches, advanced threat actors tend to migrate from malware for remote access (backdoors and web shells) to corporate remote access solutions such as VPNs or virtual desktop solutions in an effort to persist within the environment undetected. After successful migration to remote access, attackers may no longer have need of the malware and may remove it from the environment in an effort to hide their tracks.

Average amount of stolen data

The volume of data stolen is likely not the full picture. Forensic evidence is typically volatile in nature, and full fidelity network traffic monitoring may not be available throughout the full timeframe of the breach. We found forensic evidence identifying an average of 2.6 GB of data stolen per victim environment in EMEA. The particularly high dwell time (469 days) in EMEA mixed with logs rolling over time reduces the amount of evidence available to investigators to understand the full scope of data loss. This means that the 2.6 GB of data stolen, on average, per victim is likely a low number.

The statistics in the ‘By the numbers’ section, show threat actors continue to circumvent existing security defences of EMEA organisations. Threat actor activity largely remains undetected, which is demonstrated by the high dwell time. Security postures of EMEA organisations have room for improvement. The global dwell time statistic show that better security posture is achievable, and effective, for organisations that choose to adopt new detection methods and technology.

BREACH NOTIFICATION

What is a breach notification?

Breach notifications are events or activity that alert an organisation to security incidents. In order to show the challenges faced, Mandiant Consulting differentiates these between internal and external notifications.

Internal notifications are typically identified by security devices or technology:

Antivirus systems will typically alert when a known malicious file is identified using signature definitions.

Proxy servers can alert when a user visits a website known to be associated with malware.

Detection technologies can alert when particular content crosses an estate boundary, such as when suspicious content leaves the network in a ZIP file.

There are many other internal devices and technology often used for internal breach notifications, and many are introduced into a network with a lack of integration with other systems and without the ability to aggregate and reduce alert volumes.

External notifications typically originate from regional law enforcement agencies that use threat intelligence to monitor critical national infrastructure organisations for evidence of advanced persistent threat (APT) activity. The mandate for these organisations have changed in recent years, with their scope widening to cover more organisations that are not classified as critical national infrastructure.

What is the challenge?

Internal detections have their own challenges. Few organisations have their own threat intelligence and therefore are dependent on technology for detection, which can be difficult for organisations to manage for a number of reasons:

- Detection technologies are often misconfigured or misplaced in the network, and networks changes from time to time, reducing the likelihood of detecting threat activity. This is especially relevant when more communication channels used by attackers are now using encryption such as HTTPs.
- Organisations do not have their own threat intelligence capability, and therefore outsource this to another third party and have to rely on the fidelity of that intelligence.

External notifications by nature have a delayed response. Discovery of an incident often requires physically visiting an organisation and briefing them on the situation, a process that often takes days or weeks to initiate. This does not provide an immediate response to the incident and is difficult to rapidly scale. By the time relevant individuals meet, the threat actor could be far along into the attack lifecycle and close to completing their mission objective.

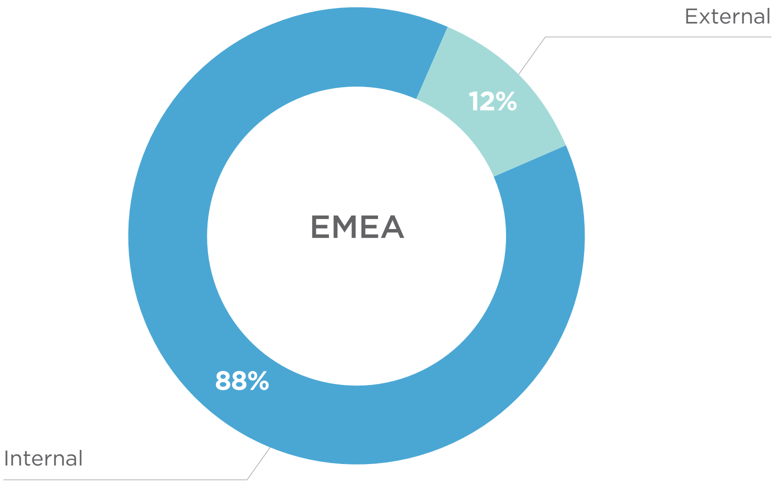
What did Mandiant Consulting observe during investigations?

Last year we found that organisations mostly focused their security protection mechanisms on inbound network traffic at the estate boundary (such as firewall devices, denial of service protection services and intrusion detection system devices). This approach misses out on the opportunity to identify malicious outbound network traffic originating from desktops and servers, oftentimes from malware command and control. Proxy servers and external DNS services provide protection from 'common threats' and low risk malware; however, the detection capability is similar to antivirus technology, where a set of signatures is used to block only known malicious activity.

The problem occurs when threat actors create a new command and control infrastructure, with new malware files, written just days before an attack is initiated. Most advanced threat actors use customised malware, which may be unknown to antivirus solutions and proxy server black lists, and therefore may be unable to detect it as malicious. Detection of advanced attacks can be challenging, as attackers create new malware, new infrastructure and new techniques to evade detection. Most organisations use only antivirus for host based protection, and often lack security monitoring for internal network communications to sensitive areas such as customer databases, repositories for intellectual property documentation and critical infrastructure due to associated costs.

Mandiant investigations in EMEA revealed that organisations predominantly rely on internal detection capabilities and rarely receive breach notifications from third parties. If the days to discovery was significantly lower and internal notifications were maintained, this would indicate a mature security posture.

Figure 3: Incident notification



The statistics for EMEA show a large gap from the global detection methods of 47% internal detection vs. 53% external detection; EMEA has a clear bias towards internal detection. Different factors have likely played a role in the disparity observed between global vs. EMEA effectiveness of external breach notifications. The most significant reason for this is that governments in EMEA do not have either the visibility to detect such attacks, or if they do their mission is not to protect commercial organisations. This is changing in some countries where critical national infrastructure has come into the purview of government protection.

Once an organisation identifies or is notified of a breach, it is important to understand how the breach originated to identify potential weaknesses in the network security posture and ensure successful remediation and eradication of the threat actor from the network.

ATTACK VECTORS

Mandiant Consulting has seen a number of different methodologies for threat actors to bypass security controls to gain access to environments. The M-Trends 2016 report highlighted a global trend in third party or outsourced organisations being an initial entry vector. As organisations become reliant on these relationships and the services they provide, threat actors will continue to exploit the often limited security controls put into place when allowing third parties to access an environment.

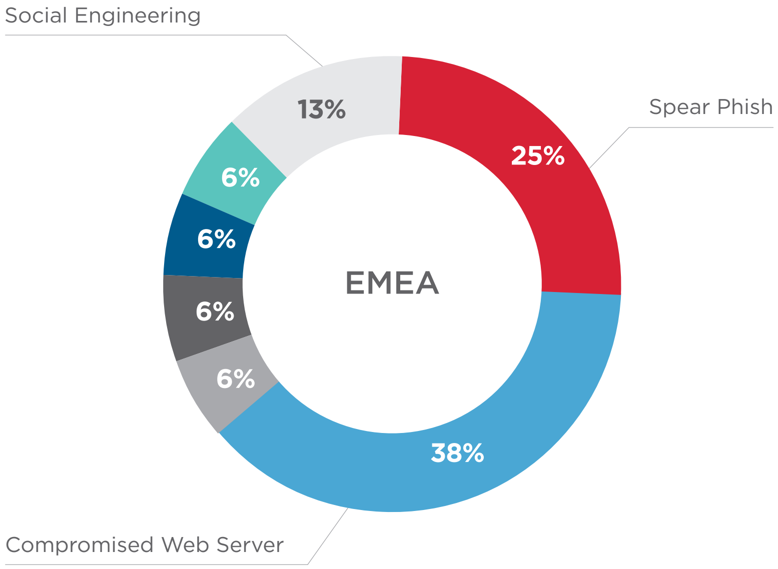
Our investigations into victim EMEA companies revealed threat actors continue to rely on traditional methods to establish an initial foothold within their targets, including:

- Sending crafted emails (spear phishing) with weaponised attachments or embedded links to malicious websites.
- Compromising a web server using a remote exploit.
- Using default credentials on external interfaces.

Note that spear phishing is a type of social engineering attack. We have called out this attack vector as a separate category to show the prevalence and success of this attack in the breaches investigated.

The variety of attack vectors emphasises the need for multi-vector monitoring capabilities within organisations.

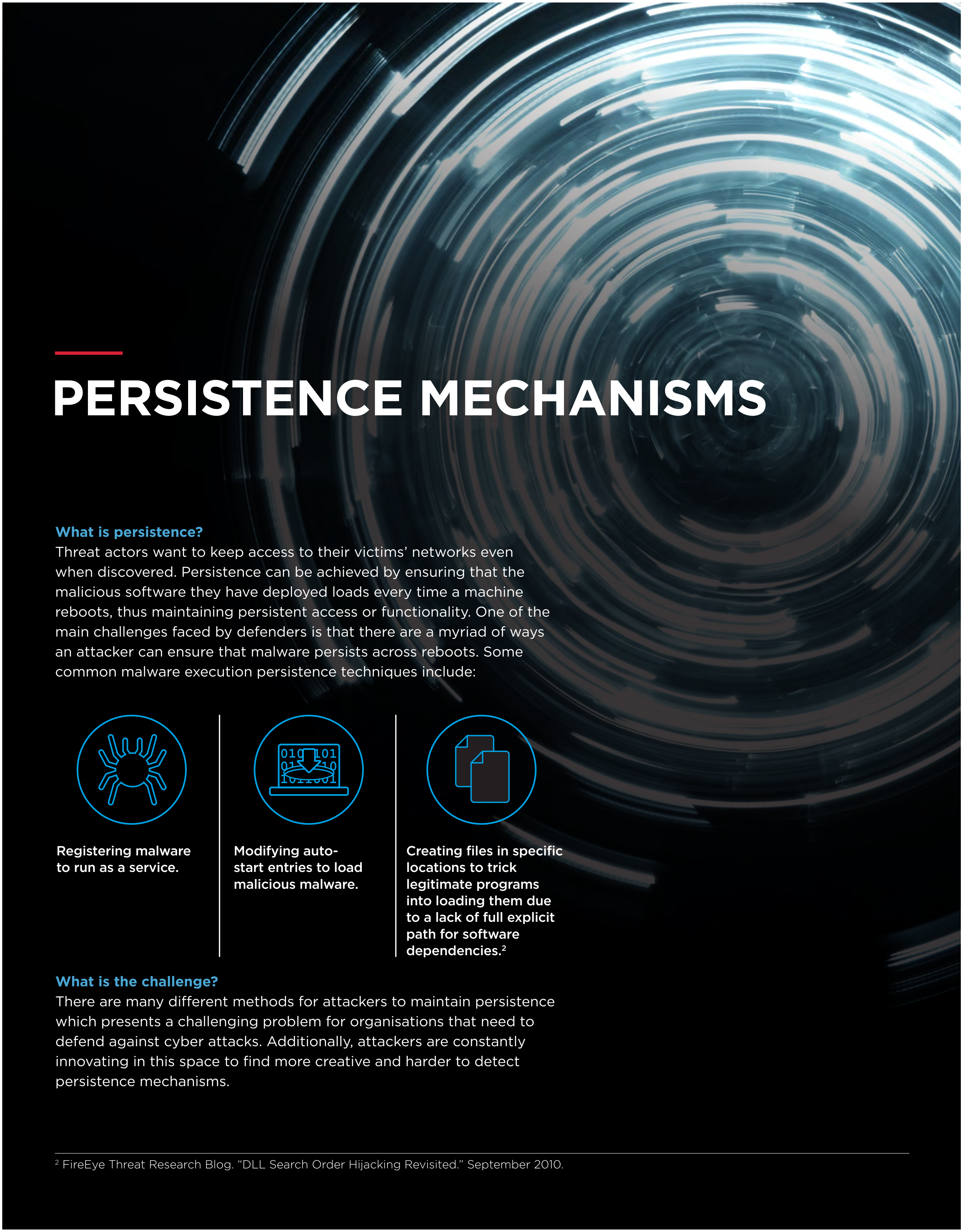
Figure 4: Attack vectors



KEY		⬛	Default Credentials
🟥	Spear Phish	🟦	SQL Injection
🟦	Compromised Web Server	🟩	Compromised Mail Server
◼	Citrix Vulnerability	⬜	Social Engineering

Spear phishing typically involves sending a tailored email to a specific individual that is designed to make the recipient think it is legitimate. This highlights the requirement for continued email security and email log analysis. Real time analytics are favoured, but are only usually observed in organisations with mature security teams that aggregate log data, enrich with threat intelligence and prioritise alerts to detect evidence of threat actors.

While threat actors will often be determined to get a foothold in an environment, the effort is wasted unless they can maintain persistent access.



PERSISTENCE MECHANISMS

What is persistence?

Threat actors want to keep access to their victims' networks even when discovered. Persistence can be achieved by ensuring that the malicious software they have deployed loads every time a machine reboots, thus maintaining persistent access or functionality. One of the main challenges faced by defenders is that there are a myriad of ways an attacker can ensure that malware persists across reboots. Some common malware execution persistence techniques include:

Registering malware to run as a service.

Modifying auto-start entries to load malicious malware.

Creating files in specific locations to trick legitimate programs into loading them due to a lack of full explicit path for software dependencies.[2]

What is the challenge?

There are many different methods for attackers to maintain persistence which presents a challenging problem for organisations that need to defend against cyber attacks. Additionally, attackers are constantly innovating in this space to find more creative and harder to detect persistence mechanisms.

[2] FireEye Threat Research Blog. "DLL Search Order Hijacking Revisited." September 2010.

What did Mandiant Consulting observe during investigations?

During investigations we observed that most organisations depended only on antivirus to detect malicious persistence mechanisms. Antivirus is a signature-based technology that is not capable of detecting every malicious event across an entire estate. A number of commercially available tools are capable of monitoring persistence mechanisms; however, we often found EMEA organisations have not reached the security maturity to introduce this kind of technology, and are often struggling with other security issues. As a result, they have not prioritised this in their roadmap.

In EMEA breaches, Mandiant investigators observed a range of persistence mechanisms, most of which included backdoors, web shells and VPN access.

Backdoors

Backdoors are typically programs designed to secretly communicate with attackers across the internet. Backdoors need to make network connections to command and control servers to be able to receive instructions from the threat actor on what to do next. They can be categorised into malware 'families' that describe collections of malicious files sharing similar attributes or characteristics to associate one another. These characteristics can be one of many values, including filenames and malware command and control infrastructure. Backdoors are typically executable files (.EXE or .DLL extension), which are loaded by the operating system that attempts to connect to an attacker's infrastructure. The executable file would normally use a persistence mechanism to be loaded every time the machine reboots – such as installing as a service or persisting in the Windows registry – and would typically beacon periodically to ask for instructions from the threat actor.

Web shells

Web shells are a form of backdoor, though we track these separately. A significant portion of breaches we investigated leveraged web shells as an alternative method for maintaining persistence into a compromised environment. Web shells typically involve a simple ASP, JSP, or PHP page uploaded to a compromised web server made possible by the attacker exploiting a vulnerability, such as a missing patch. The code is loaded by the web server, which the attacker then accesses to obtain remote connectivity. Both web shells and backdoors will allow a threat actor to communicate with infrastructure outside of the network – one major difference is that most backdoors beacon out to the attacker's command and control (C2) server, whereas the attacker has to initiate an inbound connection to a web shell for remote access. In some cases web shells are easier to hide than traditional executable malware.

VPN

VPN credentials are highly desired by threat actors because no malware is required to remotely access the target's network. This allows a threat actor to blend in with legitimate user traffic and logon events, making it difficult to detect anomalies especially when there are a large number of users working remotely or when the attacker leverages regional jump points or proxies.

VPN credentials, web shells and backdoors will allow a threat actor to communicate with infrastructure outside of the network. Persistence mechanisms used for maintaining a foothold in a target's network will always leave evidence of malicious activity that monitoring or hunting activities can detect. Communications from malware backdoors, web shells and external VPN connections will cross the network boundary, which will likely go through proxy servers, firewalls and IDS systems, all of which contain log data that can be analysed for threats. The challenge for businesses is to implement technology to capture these events and alert on specific behaviour. However, the complexity of modern networks and the vast quantities of data to analyse often introduces hurdles.

LATERAL MOVEMENT

What is lateral movement?

Threat actors will often move laterally from the initial infected machine to other neighbouring hosts within the network to perform reconnaissance activities and to also increase the number of machines infected in order to maintain persistence. Lateral movement often occurs without the use of malware making detection of newly compromised systems, where malware was not implanted, more difficult.

What is the challenge?

Digital footprints left behind by attackers are often found in host based event logs and in the internal network traffic between machines. Identifying lateral movement is a difficult task for organisations, because it requires analysing the logs of multiple internal hosts and sometimes large quantities of internal network traffic. This in turn requires log data centralisation and expensive technology, which is often not within the means of an organisation's budget to implement.

What did Mandiant Consulting observe during investigations?

Threat actors move from machine to machine using a variety of methods. Most targeted organisations we responded to were not familiar with these attacker techniques, such as:

A combination of using Windows default network administration shares[3] and the legitimate Windows task scheduler[4] to remotely install malicious files.

Using a program from the legitimate Windows SysInternals toolset to push malicious binaries onto remote machines.

Utilising the remote desktop application to log into remote machines and copy across malicious files to install.

Although many other lateral movement techniques exist, the aforementioned techniques are by far the most common because they are required for system administration purposes, organisations often do not impose security controls around this activity, and because most organisations are not monitoring or alerting on lateral movement.

In addition, we found that organisations typically did not vary the local administrator account password across systems in the environment. Therefore, when credentials were compromised, attackers could remotely log into most hosts across the estate unimpeded. There were few obstacles for the attacker to install their malicious software across the network.

[3] Microsoft. "How to remove administrative shares in Windows Server 2008." October 2012.
[4] Windows Incident Response. "How To: Track Lateral Movement." July 2013

INFORMATION STOLEN

What is information stealing?

Stealing information is often a primary objectives for a threat actor. If the attacker is not attempting data destruction or extortion, they are likely after information, such as intellectual property designs, merger and acquisition documentation or information relating to a competitive bid.

What is the challenge?

Organisations struggle to securely store company data because it is a complicated task that requires constant management and involves many systems. We often observed our customers using the following data stores, which may be targeted by attackers:

File shares (mapped drives) are often used for collaborating and sharing documents.

SharePoint sites are an emerging trend for sharing document sharing and collaboration.

Databases can be used for storing customer information, financial transactions and health care records.

Laptops often store large volumes of documents because users are often mobile and may copy parts of team shares onto their desktop to save time when working remotely. Local email data stores (such as Outlook PST/OST files) also allow users to access their entire mailbox while offline.

There are many challenges associated with securing data and managing access controls for a large user base is a constant battle.

What did Mandiant Consulting observe during investigations?

Mandiant found that compromised organisations were surprised to learn how easy it was for attackers to access many of the company data stores. For example, the Windows operating system comes preinstalled with numerous system administration command line tools that can often be abused by threat actors to access file shares. The executable net.exe is one favoured tool.

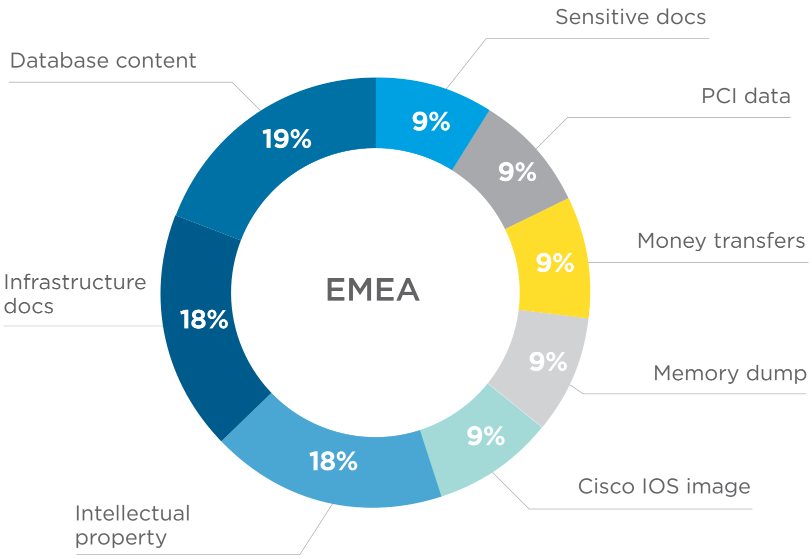
The three simple commands in Table 1 are often observed used by attackers performing internal reconnaissance tasks, finding a list of the servers, identifying the shares and mounting them to gain access to company information.

Table 1: Example of net commands often observed during investigations

COMMAND	DESCRIPTION OF COMMAND
C:\> net view	Returns a list of hostnames which are in a domain
C:\> net view \\server	Returns a list of network shares which are available
C:\> net use s: \\server\projects	Maps the network share 'projects' to the drive letter S:

Last year, an average of 2.6GB of data was exfiltrated from breached organisations in EMEA, based on our investigations. Attackers routinely attempt to cover their tracks, evidence erodes over time and the lack of appropriate visibility in most organisations hinders the ability of investigators to accurately assess the actual volume of data stolen. Therefore, it is likely that the total average volume of data stolen per compromise is significantly more.

Figure 5: Information stolen classifications



Data theft is predominantly linked to one or more of the following goals during a breach:

- **Environment reconnaissance information:** To a threat actor this information is high-value as it often reveals where valuable assets are within the corporate network, how networks are segmented and highlights the key jump points that attackers need to leverage to reach their goals.
- **Economic gain information:** This includes sensitive documentation such as intellectual property designs and customer data records that can be sold or used to gain industry advantage over international rival organisations (sometimes observed in the biotechnology, pharmaceuticals, aerospace and defence sectors).
- **Strategic intelligence information:** This may include obtaining copies of email conversations between senior executives to reveal company purchasing strategies, long-term road maps and financial decisions often of interest to nation states.

The data sources targeted in EMEA are not unique to this region, attackers will typically go after these due to their tactical and strategic value.

STEPS TO IMPROVE YOUR SECURITY POSTURE

Checking for evidence of compromise

Depending on the maturity of an organisation's security posture, the ability to actively monitor and hunt for threats in the environment can be limited. At a minimum, organisations should:

1. Review network ingress/egress points and use appropriate monitoring on each application service (web browsing, email, remote virtualised desktop solutions, etc.) that crosses the estate boundary.
2. Review each security logging device and ascertain how security risks will be identified and alerted when they occur.
3. Adopt a behavioural analysis detection approach of log data to identify high-risk security threats (such as APTs) as signature detection will only find 'known threats'.

Responding to a security breach

The following key points should be considered as part of the initial reaction plan when faced with a cyber security incident:

Assemble a Crisis Management Team: It is advisable to create a Crisis Management Team with representatives from security, IT, communications, legal, risk/compliance and any directly affected business lines. This helps to synchronise each part of the business to make a cohesive response to the incident.

Fully scope the incident: Successful remediation (removing the threat actor from your environment) can only take place once the incident has been fully scoped and the extent of the threat actor activity in the environment has been detected. Organisations with an effective Incident Response team, appropriate set of methodologies and supporting technologies should scope the incident as quickly as possible to keep pace with the information requirements from the Crisis Management team.

Avoid premature remediation: Without any doubt, this is the most frequent error from first responders. Attempting to remediate the breach before fully scoping the incident (understanding the full extent of the breach) often leads to a false sense of security and enables threat actors to continue the on-going intrusion undetected.

Reach out for professional incident response support when required: While most organisations have in-house skills to handle commodity malware or minor security breaches, an intrusion from a targeted threat actor tends to require a completely different methodology and supporting technology. The old-school IR methodologies and technologies that rely on 'following-the-breadcrumbs' to map the threat actor's actions in the environment will fail on large security breaches or when facing skilled threat actors. The only way to reliably respond to these scenarios is by deploying specialised technology to provide the Incident Response team with real-time enterprise-wide forensic visibility into endpoints and network traffic. At a minimum, organisations should have an incident response retainer signed with a trusted provider.

GLOSSARY OF TERMS

- **Spear phishing:** A targeted email weaponised with malware or containing links or redirects to malicious websites designed to infect machines.
- **Compromised web servers:** Web servers that have been hacked or compromised in some way for malicious purposes.
- **Social engineering:** Attempts by threat actors to trick or fool someone into divulging sensitive information or passwords, or performing some action that results in a compromise of system(s) or the release of sensitive information.
- **Remote vulnerabilities:** Weaknesses in the 'third party supplier access' isolation environment that allows threat actors to gain access to an asset, providing them visibility into a large part of a corporate infrastructure.
- **Default credentials:** Gaining access to hardware and software systems where the owners did not change the default passwords (most default passwords for hardware and software packages can be found on the Internet).
- **SQL injection:** Attacking a web server by sending malformed SQL queries in an attempt to gain access to the database engine or underlying operating system.
- **Compromised mail servers:** Specifically targeting public or internal mail servers to gain access to email communications or hijack the mail server for a spam hub.
- **Backdoor:** Malware running on a host that listens or communicates out to the Internet or another remote location for attacker commands. Threat actors use backdoors to gain access to compromised computing resources.
- **Web shell:** A backdoor running on a web server. Usually this is a simple HTML, JavaScript, PHP, etc. page added to a compromised web server that provides remote connectivity.
- **Malicious service:** Persistent process (survives reboots) running on a computer that performs one or more malicious actions, such as connecting to a C2 server, logging keystrokes, stealing password, etc.
- **Metasploit:** A popular open source framework used for developing and executing exploit code against a remote host. Used by both penetration testers (white hats) and cyber-criminals (black hats).
- **Ingress:** Inbound data flow for a network
- **Egress:** Outbound data flow for a network
- **Endpoint:** A hardware system, that could be a computer or a server that is capable of communicating on a network
- **SOC:** Security Operations Centre, a facility for monitoring and analysing a network environment
- **IR:** Incident Response

For more information on Mandiant,
visit: **www.fireeye.com/services.html**

FireEye, Inc.
Reading International Business Park
Basingstoke Road
Reading, Berkshire, RG2 6DA
+44(0) 203 747 5600 / europe@fireeye.com

fireeye.com

© 2016 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. SP.MTRENDSEMEA.EN-UK.062016