MANDIANT
A FireEye® Company

MANDIANT CONSULTING

M-TRENDS 2016

ASIA PACIFIC EDITION

SPECIAL REPORT / AUGUST 2016

FireEye®

CONTENTS

EXECUTIVE SUMMARY

MANDIANT, A FIREEYE COMPANY, RESPONDED TO A LARGE NUMBER OF HIGH PROFILE BREACHES IN 2015. WE MADE SEVERAL OBSERVATIONS BASED ON OUR INCIDENT RESPONSE ENGAGEMENTS IN THE ASIA PACIFIC (APAC) REGION:

- The majority of breaches in APAC never make the news headlines
- APAC organizations are frequently unprepared to identify and respond to breaches
- The median time of compromise to discovery of an attack was 520 days — three times the global median time of 146 days
- Regionally focused threat activity and attacker tools exist
- Prior to engaging Mandiant Consulting, many client organizations had already conducted forensic investigations (internally or using third parties), but failed to eradicate the attackers from their environments

INTRODUCTION

Since 2010, Mandiant, a FireEye company, has revealed trends, statistics and case studies of some of the largest and most sophisticated cyber attacks in modern history. In February 2016, we released our global annual M-Trends report based on data from the breaches we responded to in 2015. This M-Trends report is the first to focus on the Asia Pacific (APAC) region.

In this report, we share key trends and review how our clients discover breaches. We also discuss how attackers typically stay hidden in victim environments, how they move within a compromised network and how they steal data. The report then analyzes some of the key data points from the previous year and gives you knowledge of unique, region-specific challenges so you can improve your security posture and better defend your networks against sophisticated, well-funded and relentless advanced attackers.

In 2015, we continued to see heightened levels of cyber threat activity across APAC. We surmise that this is likely fuelled by regional geopolitical tensions, relatively immature network defenses and response capabilities and a rich source of financial data, intellectual property and military and state secrets. Based on available data, we observed the following five trends:

1. **MOST BREACHES IN APAC NEVER BECAME PUBLIC.** They didn't land on the front page of the local newspaper or the news ticker of a regional news channel. Unlike in markets with greater security maturity such as the United States, most governments and industry-governing bodies lack effective breach disclosure laws. This is changing slowly.

2. **APAC ORGANIZATIONS ARE OFTEN UNPREPARED TO IDENTIFY AND RESPOND TO BREACHES.** They cannot defend their networks from attackers because they frequently lack basic response processes and plans, threat intelligence, technology and expertise.

3. **ORGANIZATIONS ACROSS APAC ALLOWED ATTACKERS TO DWELL IN THEIR ENVIRONMENTS FOR A MEDIAN PERIOD OF 520 DAYS BEFORE DISCOVERING THEM.** This is 374 days higher than the global median of 146 days.

4. **SOME ATTACKER TOOLS WERE USED TO ALMOST EXCLUSIVELY TARGET ORGANIZATIONS WITHIN APAC.** In April 2015, we uncovered the malicious efforts of APT30, a suspected China-based threat group that has exploited the networks of governments and organizations across the region, targeting highly sensitive political, economic and military information. This group appeared to have operated uninterrupted for at least a decade. Why? They likely had little reason to change their operating methods because they were not detected.

5. **PRIOR TO ENGAGING MANDIANT, MANY CLIENT ORGANIZATIONS HAD ALREADY CONDUCTED FORENSIC INVESTIGATIONS INTERNALLY, OR USING THIRD PARTIES, BUT FAILED TO ERADICATE THE ATTACKERS FROM THEIR ENVIRONMENTS.** These efforts sometimes made matters worse by destroying or damaging the forensic evidence needed to understand the full extent of a breach or to attribute activity to a specific threat actor.

Taken together with our global trends and findings, these regional APAC observations reveal a dangerous threat landscape. Organizations must understand that cyber threats are not a U.S. problem, but a global one. APAC organizations should focus on enhancing their overall security posture — people, processes and technology — through improved incident detection and response capabilities. The information presented in this report should help provide justification for the renewed focus.

The Mandiant attack lifecycle model (Fig. 1) shows the typical phases of an attack and serves as a standard framework for this report. During a breach, an attacker may initially compromise a system through a spearphishing attack or strategic web compromise, and then move laterally within the environment to establish persistence by deploying backdoors on multiple computers. Once persistence mechanisms are in place, the attacker may steal privileged credentials, perform internal reconnaissance to identify their target data, and eventually exfiltrate and steal sensitive data.

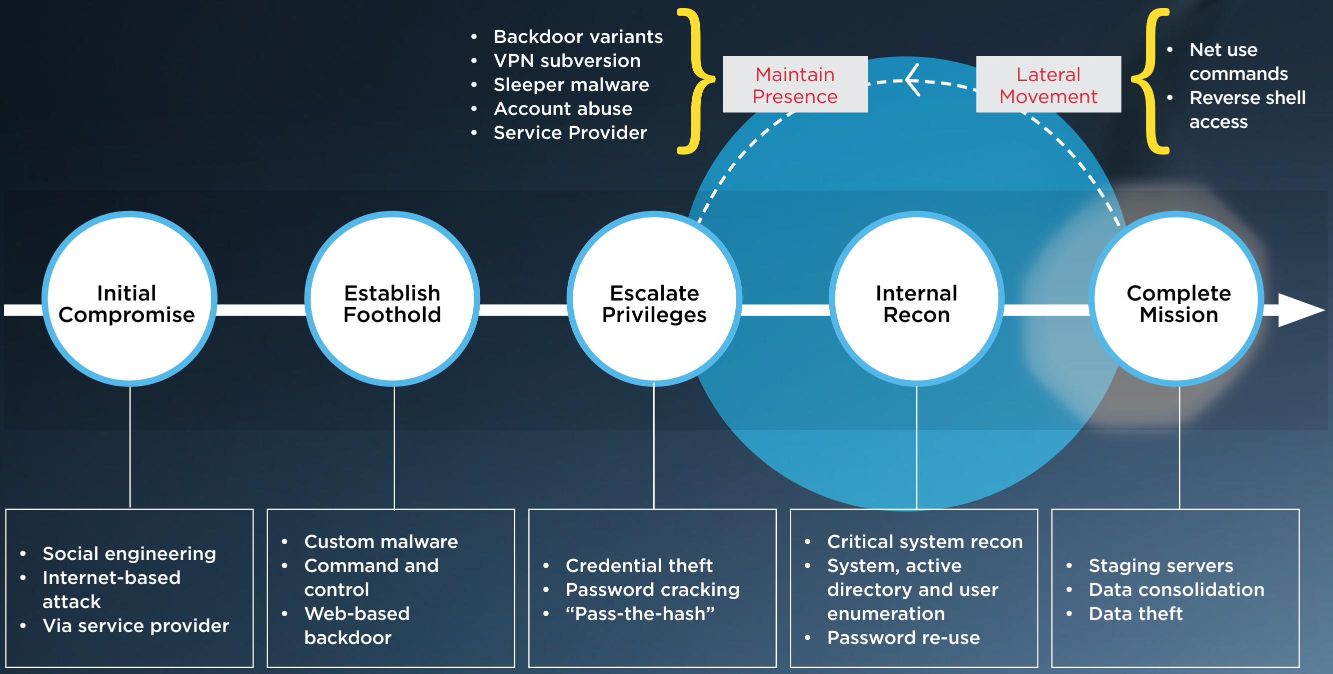


Figure 1. Attack lifecycle model with classic attacker techniques.

BY THE NUMBERS

Diversity and scope of attacks

The M-Trends 2016 global report revealed new developments among breaches. More breaches became public than at any other time in the past (both voluntarily and involuntarily), meaning organizations which were targeted were often put under the microscope by the media, industry regulators and shareholders to minimize 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, many were after intellectual property and military secrets, and others simply wanted to cause embarrassment. Some of these trends were also echoed in APAC. This report discusses details and statistics from APAC region investigations.

Incident investigation statistics from the APAC region in 2015 (Table 1) reveal that existing security controls and capabilities in organizations across APAC are not up to the challenge of detecting and responding to advanced threat actors.

Table 1. APAC incident response investigation statistics for 2015.

APAC INCIDENT RESPONSE CHARACTERISTIC	QUANTITY (AVERAGE)
Number of days compromise went undiscovered (median)	520
Number of machines analyzed in an organization	21,584
Number of internet points	4
Number of machines compromised by threat actor	78
Number of user accounts compromised by threat actor	10
Number of admin accounts compromised by threat actor	3
Amount of stolen data	3.7 GB

[1] FireEye (February 2016). M-Trends 2016.

Median number of days compromise went undiscovered

The median dwell time (time between compromise and detection) in the APAC region of 520 days — more than 17 months — versus a median dwell time of 146 days globally and 469 days in Europe, the Middle East and Africa (Fig. 2). The lower global statistic includes the U.S., where the security maturity baseline is higher and proactive hunting for malicious activity is becoming a key capability of organizations' security teams.

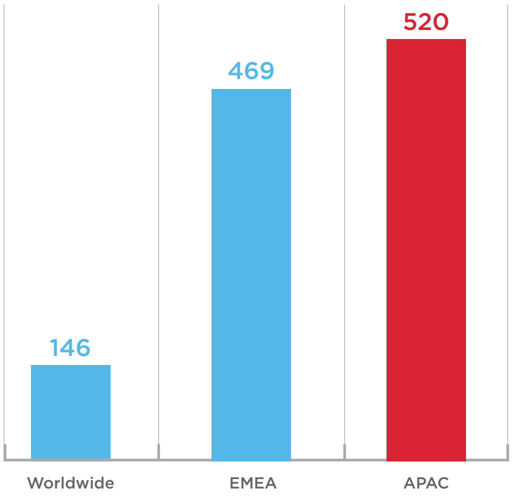


Figure 2. Days until breach discovery (median).

Seventeen months provides 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, a Mandiant red team can obtain access to domain administrator credentials within — on average — 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, gain access to and exfiltrate and steal desired information.

Average number of machines analyzed in an organization

Organizations in APAC typically performed some level of analysis (internally or via a third party) before hiring FireEye. Their investigations usually included only a handful of machines, meaning they did not identify the full scope of the incident. Because the investigations were often led by people who lacked experience responding to large-scale breaches carried out by highly capable and sophisticated threat actors, the investigators inadvertently destroyed critical forensic evidence or tipped off the attackers. Therefore organizations and governments were sometimes re-compromised within hours, days or weeks after an initial forensic investigation.

On average, Mandiant consultants investigated 21,584 machines during APAC breaches in 2015. FireEye advocates a comprehensive investigation using high fidelity intelligence and a rapid, scalable methodology covering every system in the environment. This approach enables the organization to fully understand the scope of a breach, paving the way for successful eradication of the threat actor from their network and remediation of the threat. All systems on a network, not just a subset, must be included in the investigation to discover the full extent of a compromise and remediate it effectively.

In APAC, many organizations use traditional investigation methodology based on a "follow the bread crumbs" approach that analyzes a handful of machines, and "spidering out" from those machines. For enterprise-scale incidents, FireEye considers this approach inadequate, since it is likely to not fully identify all compromised machines, scope the breach or remediate the threat. As a result, attackers often get tipped off and either continue to remain within the environment after the investigation or if removed, rapidly regain unauthorized access to the organization.

Average number of machines compromised by threat actor

Of the 21,584 systems Mandiant consultants investigated on average per client, only 78 (approximately 0.4%) systems were compromised. This reinforces the fact that cyber investigation is a daunting task. Investigators are truly looking for a needle in the haystack when trying to determine the timeline of a breach. To complicate matters, the majority of these compromised systems have no malware installed, rendering antivirus and endpoint protection solutions powerless and providing CIOs with a false sense of security.

While an attacker may theoretically have full access to an environment once they have escalated privileges, it is not in their best interest to operate on or compromise many systems. Attackers normally keep their footprint to a small percentage of the environment to avoid detection.

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

Once an attacker has gained initial access to an environment, they attempt to establish persistent access, often by deploying malware on the initially compromised system. They then start escalating privileges to get domain or local administrator access. They use these accounts for lateral movement, access to applications and databases, remote access or continued access when a set of credentials (Fig. 3) gets changed. Considered forensically, investigators must hunt for threat actors who pose as an "insiders," using legitimate credentials to blend in with normal user activity.

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 organization and blend in with regular users.

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

Figure 3. Threat actors usually require access to multiple sets of credentials to fulfill their objectives.

Mandiant consultants observed that an average of 10 authorized user accounts and three authorized administrator-level accounts were compromised during a breach. The attackers were using legitimate accounts to blend into the environment — and go undetected — while attempting to complete their nefarious tasks. Determining which compromised credentials were used during any one attack is crucial to understanding the full extent of a breach.

During sustained breaches, advanced threat actors tend to migrate from malware for remote access (backdoors and web shells) to legitimate corporate remote access solutions such as VPNs or virtual desktop solutions. This allows them to blend in and persist within the environment undetected. After successfully migrating to remote access, attackers may no longer need to rely on malware in the environment. To hide their tracks, they may remove the malware, along with basic indications of compromise.

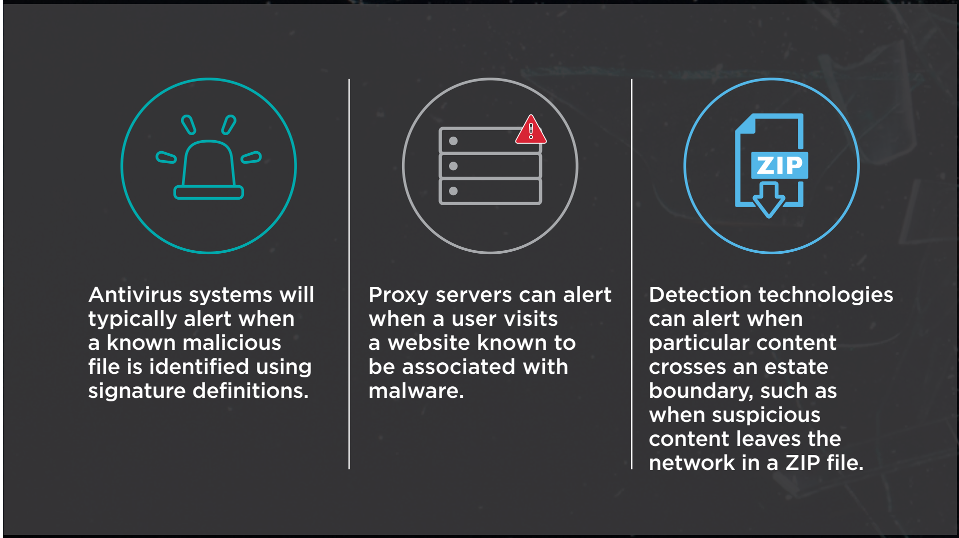
Average amount of stolen data

Across our investigations in APAC, we found forensic evidence identifying an average of 3.7 GB of data stolen per client. The particularly high dwell time (520 days) in APAC mixed with logs rolling over time (the process of security logs being overwritten routinely due to size constraints) reduced the amount of evidence available to investigators and inhibited their ability to understand the full scope of data loss. This likely indicates that the average 3.7 GB of data stolen per victim is an optimistic figure, and the reality is probably much worse.

Threat actors continue to circumvent existing security defenses of APAC organizations and remain largely undetected for long periods of time (Table 1). Security postures of APAC organizations have room for improvement. The global dwell time statistic shows that better security posture is achievable, and effective, for organizations that choose to embark on the journey to better safeguard their assets.

BREACH NOTIFICATION

Breach notifications are events or activity that alert an organization to security breaches. FireEye differentiates between internal (Fig. 4) and external breach notifications to clarify and respond appropriately to challenges.



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.

Figure 4. Internal notifications are typically identified by existing security controls.

External notifications typically originate from regional law enforcement agencies or computer emergency response teams (CERTs) that use threat intelligence to monitor critical national infrastructure for signs of compromise. The mandate for these organizations has expanded in recent years to include entities not traditionally categorized as critical national infrastructure.

Challenges created by internal and external notifications

Few organizations have the right combination of intelligence, technology and expertise to establish and maintain strong internal detection systems. There are several reasons they are difficult to manage:

- Detection technologies are often misconfigured or misplaced in the network, and periodic network changes reduce the likelihood of detecting threat activity. This is especially relevant because attackers are now using more communications channels with encryption such as HTTPS. Organizations also rely on antiquated signature-based detection sets, which rarely catch advanced threat actors.
- Organizations lack appropriate technologies to perform effective computer and network forensics.
- Many organizations lack a threat intelligence capability, and must therefore outsource it to a third party and rely on the fidelity of that intelligence.
- Organizations are unable to hire and retain highly sought-after incident responders and forensics experts.
- Organizations do not have the budgets to hire an entire security staff that should include security analysts, incident responders, intelligence analysts, malware researchers, malware reverse engineers, and many other security professionals.

By their nature, external notifications have a delayed response. The information has to be discovered, vetted for accuracy and then conveyed to the properly identified point of contact (POC) at each victim organization. The main challenge is convincing the POC that a situation exists and action must be taken based on the data provided. A POC's typical first response is to disbelieve an external notification or to verify the notifying individual. This does not provide an immediate response to the incident and makes it difficult for notifiers to rapidly scale their operations. By the time relevant security professionals meet, the threat actor could be far along into the attack lifecycle and close to completing their mission objective.

How different security approaches impact breach notifications

Last year we found that organizations 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 (IDS) devices). This approach misses opportunities to identify malicious outbound network traffic originating from desktops and servers, often from malware command and control. Proxy servers and external DNS services provide protection from "common threats" and low-risk malware; however, their detection capability is similar to antivirus technology, where a set of signatures is used to block only known malicious activity.

A 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 customized malware that is often unknown to antivirus solutions and proxy server black lists and can remain undetected for some time. Detection of advanced attacks can be challenging because attackers are constantly developing new malware, new infrastructure and new techniques to evade detection. Most organizations use only antivirus products for host based protection and do not monitor the security of internal network communications to sensitive areas such as customer databases, repositories for intellectual property documentation and critical infrastructure.

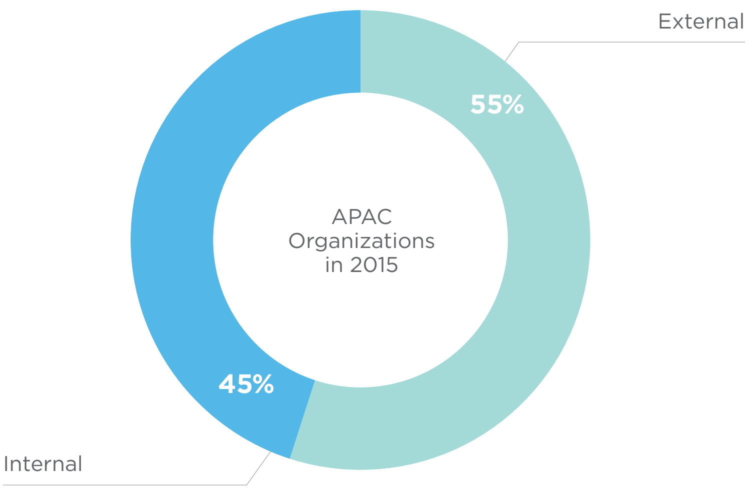


Figure 5. Incident notification in APAC organizations in 2015.

Mandiant investigations in APAC (Fig. 5) revealed the region to be split almost equally, with 45% of incidents discovered internally and 55% of notifications coming from external sources. These statistics are closely aligned with observed global averages of 47% internal discovery and 53% external notifications. However, even if the sources of breach detections follow international trends, the dwell time (time between compromise and detection) does not. There is a three-fold increase for the APAC average (520 days) over the global average (146 days), indicating that cyber incidents are detected far too late.

PERSISTENCE MECHANISMS

Threat actors want to maintain access to their victims' networks even after discovery. 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. Attackers have many ways (Fig. 6) to ensure that malware persists across reboots.

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.

Figure 6. Common malware execution persistence techniques.

Attackers are constantly innovating in this space to find more creative and harder to detect persistence mechanisms, such as the infamous DLL Search Order Hijacking persistence mechanism.[2]

Why APAC struggles to defend against persistence mechanisms

During investigations we observed that most organizations depended only on antivirus software to detect malicious persistence mechanisms. Antivirus software is a signature-based technology that cannot detect every malicious event across an entire estate. A number of commercially available tools can monitor persistence mechanisms; however, we often found that APAC organizations had not reached the security maturity to introduce this kind of technology. Because they struggled with these and other security issues, deployment of tools to monitor persistence mechanisms were not prioritized in their roadmap.

In APAC breaches, Mandiant investigators observed a range of mechanisms used by attackers to maintain long term access to compromised environments. Some of the more common mechanisms are malicious backdoors, web shells and virtual private networks (VPN) access.

[2] FireEye (September 1, 2010). "DLL Search Order Hijacking Revisited." https://www.fireeye.com/blog/threat-research/2010/08/dll-search-order-hijacking-revisited.html

Backdoors

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

Web shells

Web shells are a form of backdoor, but we tracked them separately because a significant number of breaches we investigated relied on a web shell to maintain persistence in a compromised environment. Both web shells and backdoors 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 (CnC) server, whereas the attacker has to initiate an inbound connection to a web shell for remote access. Web shells usually involve a simple ASP, JSP or PHP page uploaded to a compromised web server by exploiting a vulnerability, such as a missing patch. Malicious code is loaded on to victim systems by the web server, which the attacker then accesses to obtain remote connectivity. We also see attackers add malicious code to a pre-existing web page (one example is the China Chopper web shell) to make the web shell even harder to detect. In some cases web shells are easier to hide than traditional executable malware.

VPN

VPN credentials are highly desired by threat actors. If an attacker has VPN credentials they don't need malware to remotely access the target's network. The attacker can 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 they take advantage of regional jump points or proxies.

VPN credentials, web shells and backdoors allow a threat actor to communicate with infrastructure outside of the network and maintain a foothold in the target network. But these persistence mechanisms will always leave evidence of malicious activity that monitoring or hunting activities can detect. Communications from malware backdoors, web shells and external VPN connections cross the network boundary and likely go through proxy servers, firewalls and IDS systems, all of which contain log data that can be analyzed for threats (or can be used to facilitate the proactive detection of malicious activity). Businesses must seek out technologies to capture these events, analyze them and alert on specific behavior. However, the complexity of modern networks and the vast quantities of data to analyze are significant challenges.

LATERAL MOVEMENT

Threat actors will often move laterally from the initial infected machine to other neighboring hosts within the network to perform reconnaissance activities and infect additional machines to help maintain persistence. Lateral movement often occurs without the use of malware, making detection of those newly compromised systems more difficult. Lateral movement is frequently facilitated by legitimate, but compromised, user credentials.

Technology and budgetary challenges

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 organizations, because it requires analyzing the logs of multiple internal hosts and sometimes large quantities of internal network traffic. Helpful critical technologies, such as log data centralization are prohibitively expensive for most organizations.

Using Windows default network administration shares and the legitimate Windows Task Scheduler to remotely install malicious files.

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

Using a remote desktop application to log in to remote machines and copy and install malicious files onto them.

Figure 7. Lateral movement attack methods.

Most targeted organizations we responded to were not familiar with these attacker techniques.

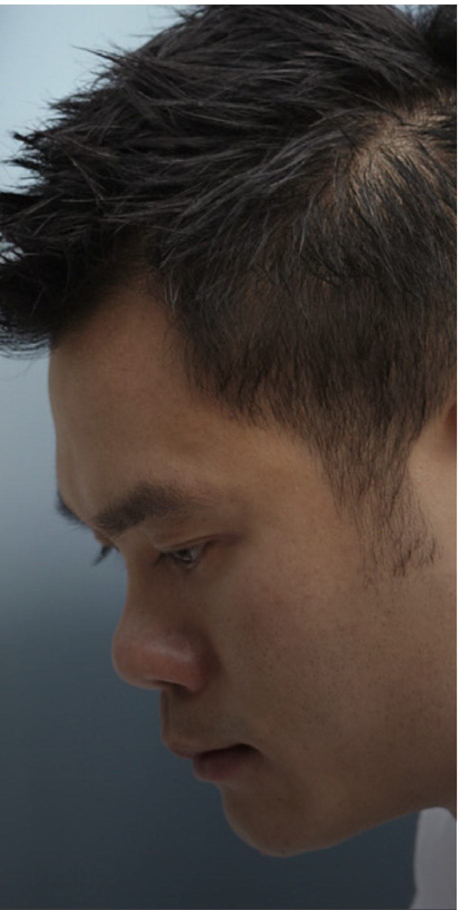
Why APAC organizations are vulnerable to lateral movement

Threat actors move from machine to machine using a variety of methods (Fig. 7). Most targeted organizations we responded to were not familiar with these attacker techniques.

Although many other lateral movement techniques exist, these are the most common because they are required for system administration purposes. Organizations often did not impose security controls around these activities and most of them did not monitor or alert on lateral movement.

In addition, organizations typically did not vary the local administrator account password across systems in the environment. When credentials were compromised, attackers could easily and remotely log in to most hosts across the estate. There were few obstacles in the way of the attacker intent on installing malicious software across the network.

INFORMATION STOLEN



Stealing information is often a primary objective 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, financial data or information relating to a competitive bid.

High-value attack targets

Organizations struggle to securely store company data because it is a complicated task that requires constant management and involves many systems.

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

SharePoint sites are used for 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.

Email servers are often a primary channel for sharing and discussing business and data.

Figure 8. Data stores used by FireEye clients in APAC organizations.

There are many challenges associated with securing data and managing access controls for these high-value data stores, and a large user base only makes them more difficult to protect.

Common theft methods and goals

Mandiant found that compromised organizations were surprised to learn how easy it was for attackers to access many 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 favored tool.

We observed that attackers often used three simple commands (Table 2) to perform internal reconnaissance tasks, find a list of servers, identify shares and mount them to gain access to company information.

Table 2. Examples of Net commands often observed during APAC 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, our investigations showed that an average of 3.7 GB of data was exfiltrated from breached organizations in APAC (Fig. 9). The majority of attacks observed by Mandiant consultants targeted email, sensitive documents, infrastructure documents and personally identifiable information (PII). Although investigators attempted to accurately assess data loss, attackers routinely covered their tracks, evidence eroded over time and most organizations lacked appropriate visibility. Therefore, it is likely that the total average volume of data stolen per breach was significantly more than 3.7 GB.

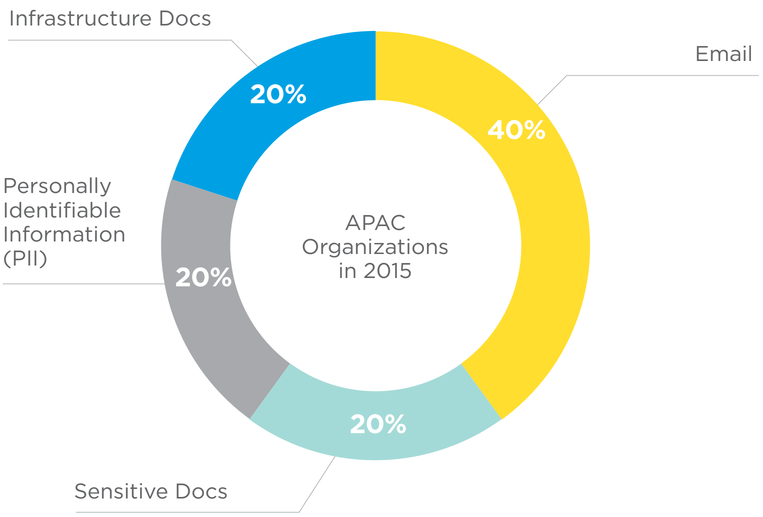


Figure 9. Classification of information stolen from APAC organizations in 2015.

Breach-facilitated data theft is predominantly linked to one or more of the following informational goals:

- **Environment reconnaissance:** This high-value information often reveals where valuable assets are within the corporate network, how networks are segmented and what key jump points attackers need to use to reach their goals.
- **Economic gain:** Sensitive documentation such as intellectual property designs and customer data records can be sold or used to gain industry advantage over international rival organizations (sometimes observed in the biotechnology, pharmaceutical, aerospace and defense sectors).
- **Strategic intelligence:** Email conversations between senior executives and high-level planning documents can reveal company purchasing strategies, long-term road maps and financial decisions of interest to nation states.

The data sources targeted in APAC are not unique to this region. Attackers in all regions will pursue any tactically and strategically valuable data sources.

STEPS TO IMPROVE YOUR SECURITY POSTURE

Checking for evidence of compromise

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

1. Review network ingress/egress points and use appropriate monitoring on each application service (web browsing, email, remote virtualized 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 behavioral analysis detection approach with log data to identify high-risk security threats (such as APTs) because signature detection will only find known threats.

Responding to a security breach

The initial reaction plan for a cyber security incident should include the following:

Assemble a crisis management team with representatives from security, IT, communications, legal, risk and compliance and any directly affected business lines. This helps synchronize each part of the business to implement a coordinated response to the incident.

Fully scope the incident to detect all threat actor activity and effect successful remediation (remove the threat actor from your environment). Organizations with an effective incident response team, appropriate methodologies and supporting technologies should scope the incident as quickly as possible to keep pace with the information requirements from their crisis management team.

Avoid premature remediation to reduce errors by first responders. Attempting to remediate a breach before fully scoping an incident (understanding the full extent of the breach) often leads to a false sense of security and enables threat actors to continue their intrusion undetected.

Reach out for professional incident response support when required: While many organizations 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. Traditional incident response methodologies and technologies that rely on following breadcrumbs to map threat actor activity will fail on large security breaches or when facing skilled threat actors. The only way to reliably respond to these scenarios is by deploying specialized technology that provides the incident response team with real-time enterprise-wide forensic visibility into endpoints and network traffic. At a minimum, organizations should have an incident response retainer signed with a trusted provider.

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

FireEye, Inc.
8 Shenton Way
#38-01 AXA Tower,
Singapore 068811
+65-3158-5588 / APAC@fireeye.com

fireeye.com