MANDIANT®
A FireEye® Company

# M-TRENDS® 2017

## A View From the Front Lines

SPECIAL REPORT

FireEye®

# CONTENTS

**M-TRENDS® 2017 INTRODUCTION**

# Every year Mandiant, a FireEye company, responds to a large number of cyber attacks, and 2016 was no exception.

For our M-Trends® 2017 report, we took a look at the incidents we investigated last year and provided a global and regional (the Americas, Asia Pacific (APAC) and Europe, Middle East, Africa (EMEA)) analysis focused on attack trends and defensive and emerging trends. For the second consecutive year, we have included insights from our FireEye as a Service (FaaS) teams. FaaS monitors organizations 24/7, which gives them a unique perspective into the current threat landscape. Additionally, this year we partnered with law firm DLA Piper for a discussion of the upcoming changes in EMEA data protection laws.

# Executive Summary

**When it comes to attack trends,** we are seeing a much higher degree of sophistication than ever before. While nation-states continue to set a high bar for sophisticated cyber attacks, some financial threat actors have caught up to the point where we no longer see the line separating the two. Financial attackers have improved their tactics, techniques and procedures (TTPs) to the point where they have become difficult to detect and challenging to investigate and remediate.



**While financial threat actors have come a long way with the tools they use and how they use them,** they have shown innovation in other areas as well. Perhaps the most unexpected trend we observed in 2016 is attackers calling targets on the telephone to help them enable macros in a phishing document or obtain the personal email address of an employee to circumvent controls protecting corporate email accounts. To compound the issue, threat groups have also shown increased sophistication when it comes to escalating privileges and maintaining persistence.

Although our investigations show that inter-banking networks are particularly attractive to financial threat groups, we also saw plenty of activity in 2016 involving the use of malware to drain ATMs of cash.

While there has been a marked acceleration of both the aggressiveness and sophistication of cyber attacks, defensive capabilities have been slow to evolve and respond. We have observed that a majority of both victim organizations and those working diligently on defensive improvements are still lacking fundamental security controls and capabilities to either prevent breaches or to minimize the damages and consequences of an inevitable compromise. Based on our observations of trends from the past several years, organizations must adopt a posture of continuous cyber security, risk evaluation and defensive adaptation or they risk significant gaps in both fundamental security controls and – more critically – visibility and detection of targeted attacks.

Sophisticated intelligence integration, automation, and threat hunting should be the end-state goal for organizations facing significant business risks and exposure to cyber attacks. In 2016, we observed a rise in companies either exploring or implementing such capabilities, which were once limited to government and global financial services organizations. The trend toward enabling these proactive security operations is one we encourage and endorse, but businesses must not lose focus of the foundational security functions that both reduce overall cyber risks and enable the defensive operations to operate effectively and efficiently. With an increased willingness of both nation-state and financial threat actors to operate increasingly blatant business disruption, extortion, and public disclosure attacks, fundamental protections such as data and key application segregation, network segmentation, and continuous visibility and monitoring of critical systems have returned to prominence and should remain a primary focus for many IT and security teams.

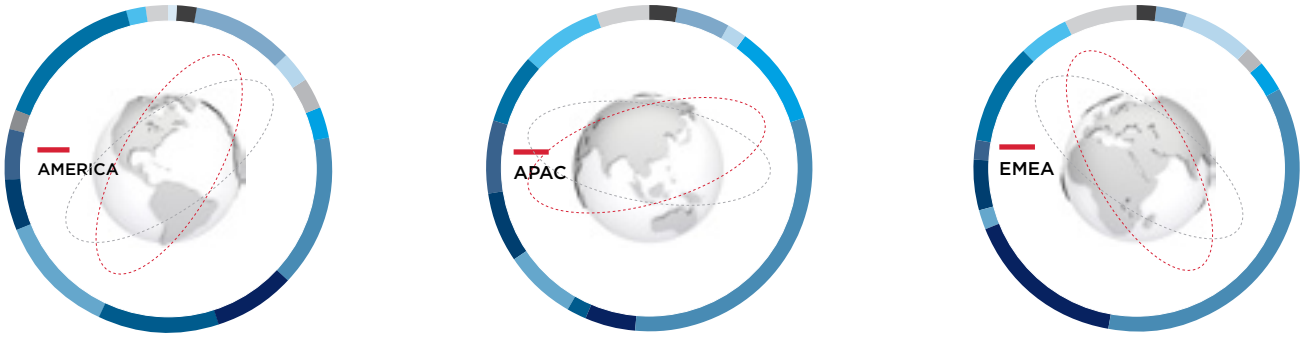
**FireEye believes in an intelligence-led approach to security,** and this focus applies to many of the defensive trends outlined in M-Trends® 2017. CIOs, CISOs and security teams have somewhat become victims of their own successes. With increased investments in security tools and technologies, teams have become overwhelmed with alerts and data and are struggling to prioritize and find the signal in the noise. Cyber defensive operations and investigations, leveraging intelligence, and automation and orchestration can convert manual and time intensive functions into streamlined courses of action that are presented to an analyst in a prioritized manner based on predetermined criticalities and business impacts. These types of use case "mechanizations," combined with accurate and timely intelligence, can save thousands of person-hours of tedious work and enable analysts to focus on investigating and remediating the compromises that truly matter.

In addition to enhancing defensive detection and response functions, threat intelligence is the critical component that enables a truly proactive security posture and a threat hunting function. Cyber threat intelligence allows organizations to develop and maintain a baseline threat profile. This threat profile is the data-driven mechanism (as opposed to fear, uncertainty, and doubt) that informs the business and the security teams of the most likely who, what, where, when, and how of attacks and the best way to begin looking for them. By constantly assuming compromise in the most likely areas of the infrastructure, organizations can focus their hunting and provide an accurate and factual answer to the question at the top of every executive's mind: "Am I compromised?"

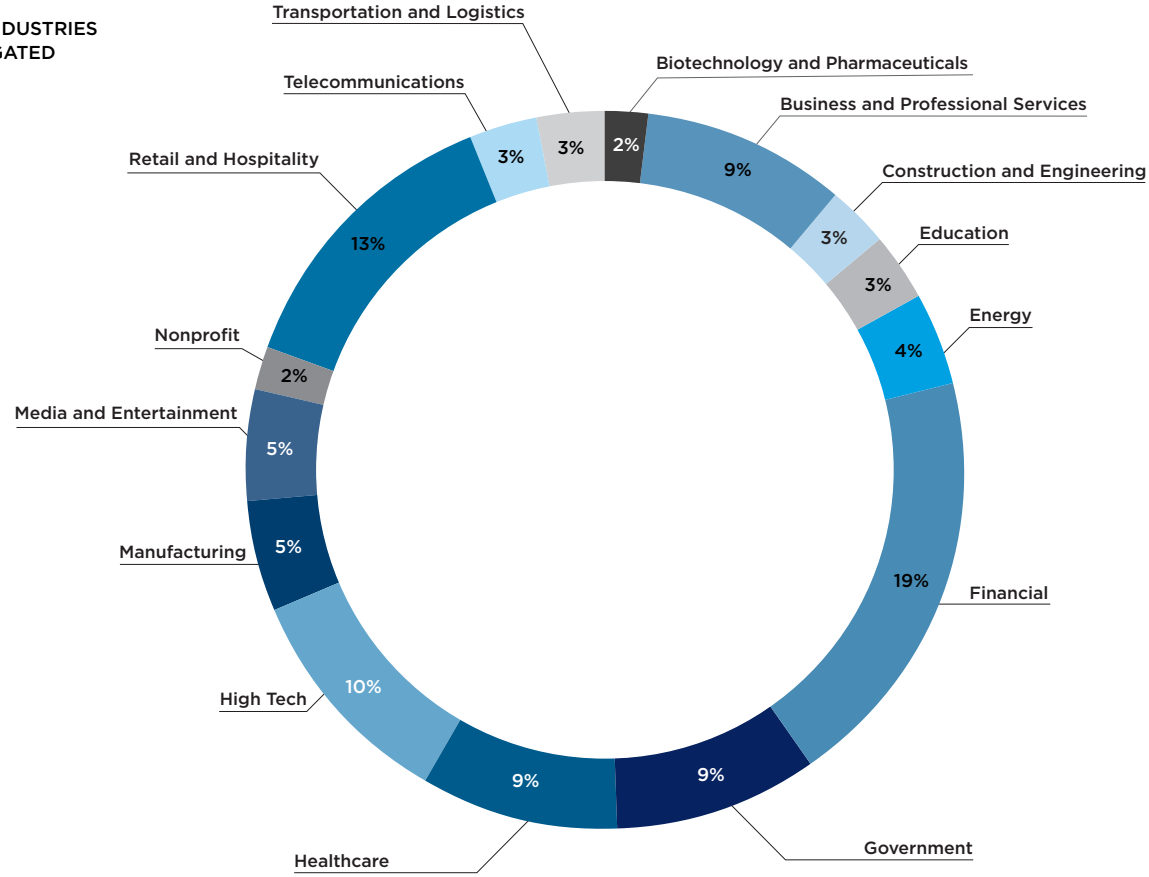
# By The Numbers

PROVIDED BY FIREEYE iSIGHT INTELLIGENCE

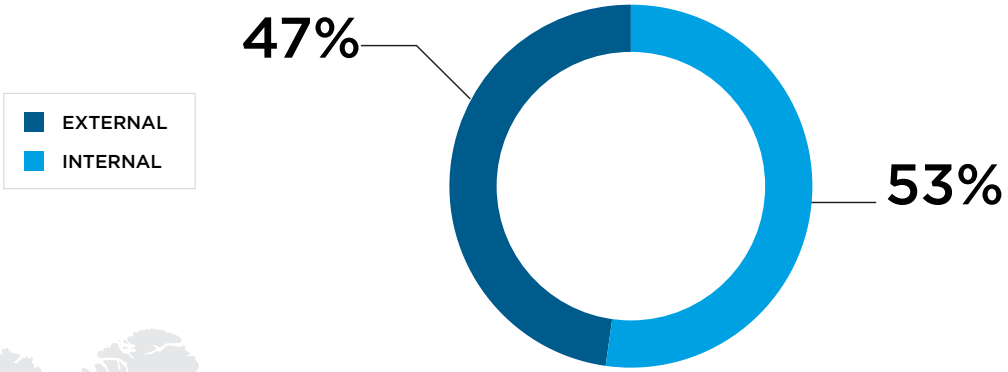
## INDUSTRIES INVESTIGATED



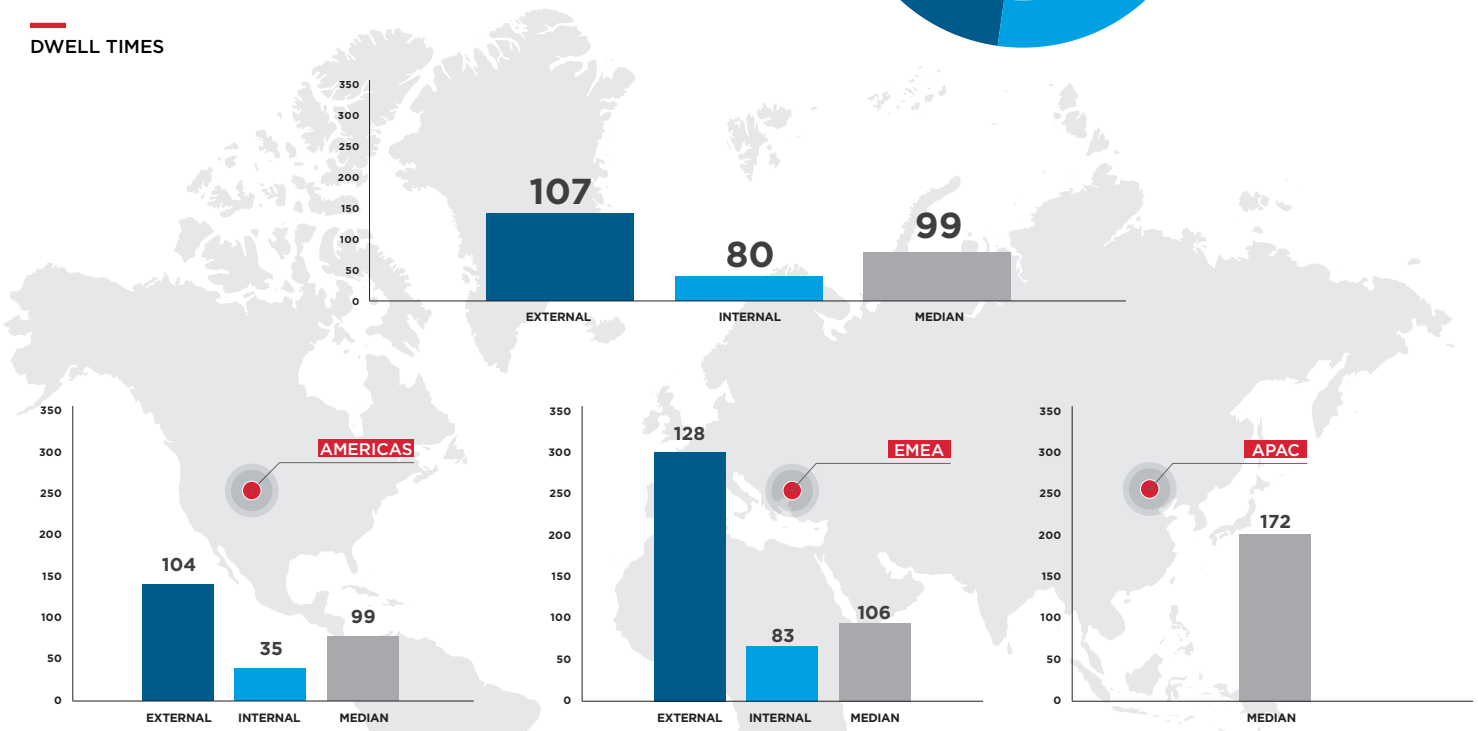

## TOTAL INDUSTRIES INVESTIGATED



## NOTIFICATION SOURCES TOTAL




## DWELL TIMES




## KEY: INDUSTRIES INVESTIGATED

| Industry | America | APAC | EMEA | Total |
|---|---|---|---|---|
| Financial | 15% | 31% | 36% | 19% |
| Retail and Hospitality | 15% | 7% | 10% | 13% |
| High Tech | 12% | 7% | 2% | 10% |
| Healthcare | 12% | 2% | 0% | 9% |
| Business and Professional Services | 10% | 5% | 3% | 9% |
| Government | 8% | 5% | 16% | 9% |
| Manufacturing | 5% | 7% | 5% | 5% |
| Media and Entertainment | 5% | 7% | 2% | 5% |
| Energy | 3% | 10% | 3% | 4% |
| Construction and Engineering | 3% | 2% | 7% | 3% |
| Education | 3% | 0% | 2% | 3% |
| Telecommunications | 2% | 9% | 5% | 3% |
| Transportation and Logistics | 2% | 5% | 7% | 3% |
| Nonprofit | 2% | 0% | 0% | 2% |
| Biotechnology and Pharmaceuticals | 2% | 3% | 2% | 2% |
| Other | 1% | 0% | 0% | 0% |

This year we have seen a marked decrease in the average dwell time in the EMEA and APAC regions. We deem that a number of factors have played a part in reducing this number.

While many organizations have been establishing better testing methodologies such as Red Teaming and Response Readiness Assessments to proactively understand their security posture, we suspect the changing nature of attacks has had a significant effect.

Victims in the regions are still experiencing lengthy breaches, but we believe a significant rise in attacks that are intended to be identified quickly, such as ransom and destructive wiper attacks, are impacting the statistics for EMEA and APAC.

Overall, APAC continues to have one of the highest dwell times for adversaries because of the basic lack of investment in security.

# Attack Trends



## Less Smashy, More Grabby

Prior to 2013, Mandiant categorized the attacks carried out by actors targeting financial information (ACH, PCI, direct deposit, tax return, etc.) as "smash and grab". The attackers did not hide their actions and did not demonstrate an intent to maintain access to an environment once detected. The attacks were loud and recovery was straight forward. The targets were largely opportunistic, the tools rudimentary and the skill of the attacker – in all but a few cases – was limited. We often advised our consultants preparing to investigate financial attackers for the first time: "The case will be straight forward. The tools are noisy – often scripting languages converted to compiled code with tools such as Perl2Exe, which will generate a lot of forensic artifacts and makes the attacker activity stand out. You will block a few IP addresses, and the attack will be over."

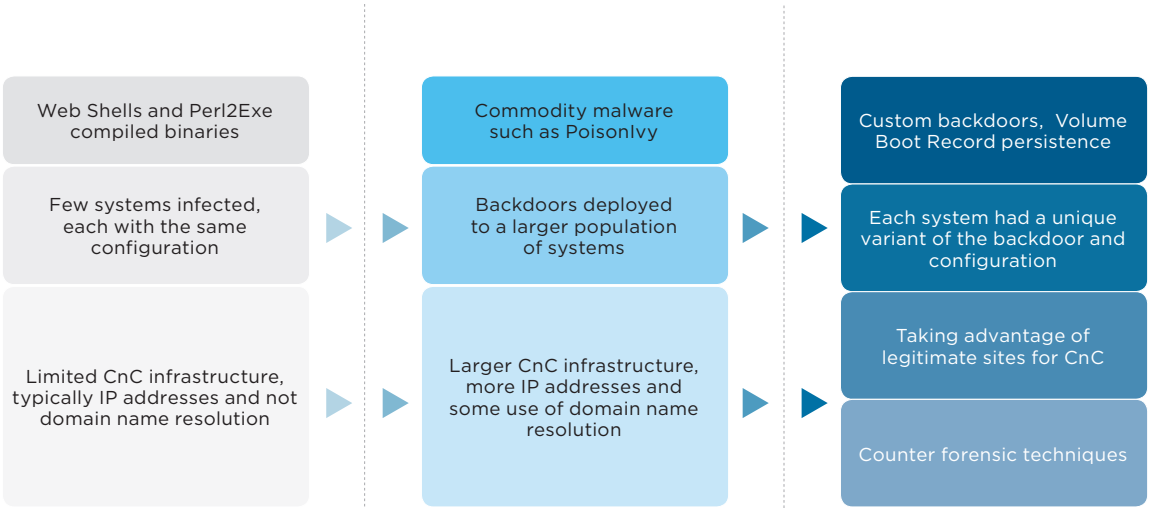
As early as 2013, we began to speak publicly about witnessing a rise in the sophistication of the financial attacker. Mandiant investigations from 2014 (discussed in M-Trends® 2015), showed that "the lines are blurring between run-of-the-mill cyber criminals and advanced state-sponsored attackers". However, the maturation at the time was modest. Attackers used compiled binaries more often (less Perl2Exe) and they started to maintain a larger command and control (CnC) infrastructure designed to allow the attackers to persist following a modest eradication event.

Today, the line between the level of sophistication of certain financial attackers and advanced state-sponsored attackers is not just blurred – it no longer exists. In 2016, financial attackers moved to custom backdoors with a unique configuration for each compromised system, further increased the resilience of their CnC infrastructure, and employed improved counter forensic techniques.

While state-sponsored attackers will continue to set the bar for capabilities and sophistication, financial attackers can no longer be categorized as smash and grab. An attacker that is harder to detect, investigate and remediate is inherently more likely to remain in an environment to accomplish their mission, which means the theft of greater volumes of financial information.

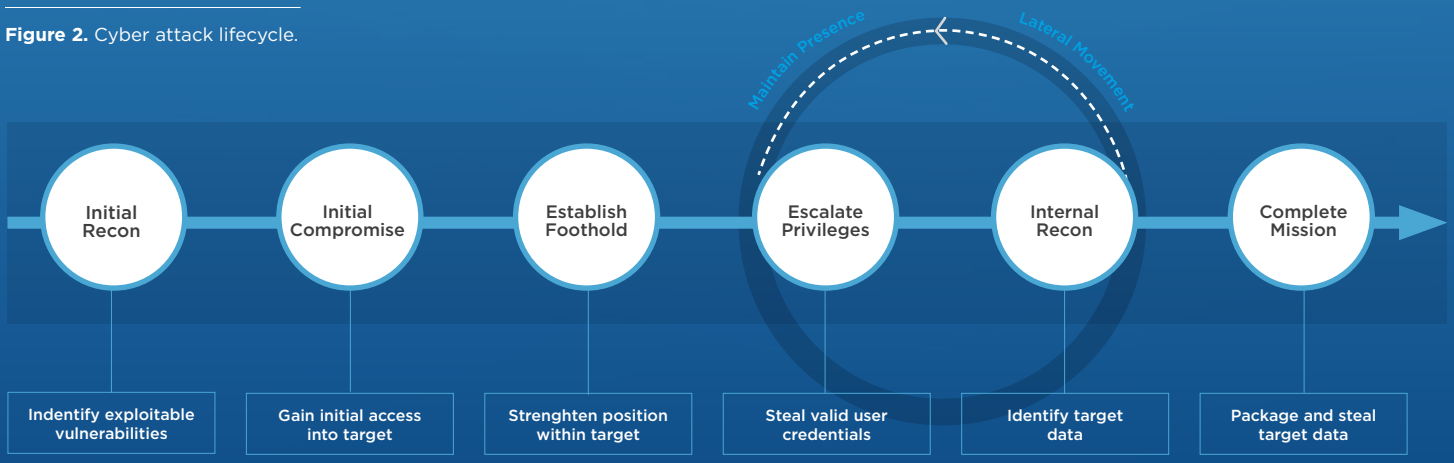
Figure 1 below illustrates the increase in sophistication of financial attackers we have seen over the past three years.

**Figure 1.** Increase in sophistication of financial attackers.



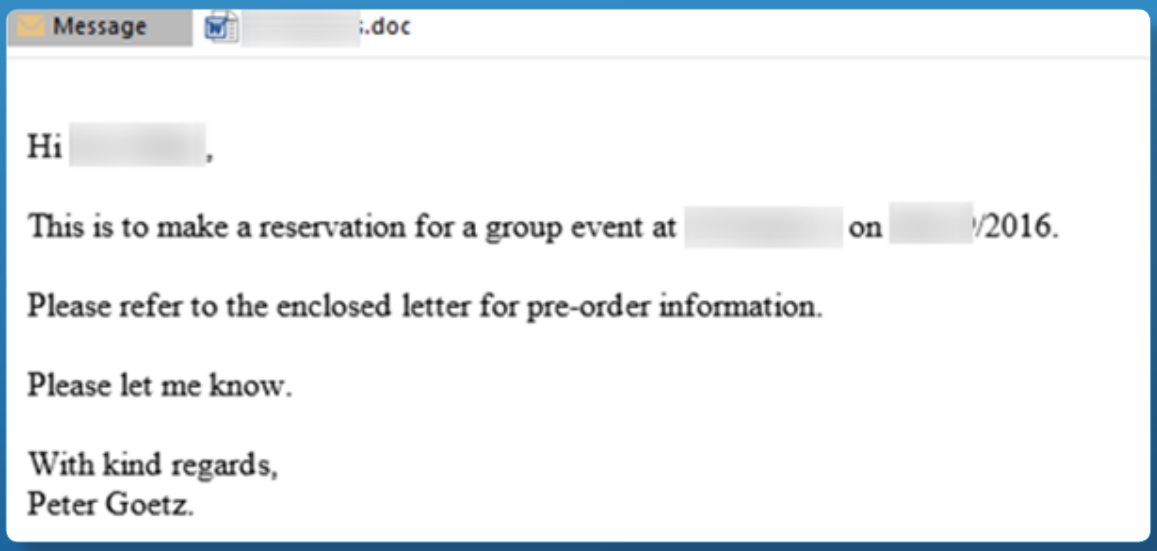
The following section details the more significant changes we have witnessed while investigating financial attackers. The changes are grouped in accordance with the attack lifecycle diagram.

**Figure 2.** Cyber attack lifecycle.



**Initial compromise**
Instead of using generic themes or subjects for phishing emails such as "invoice" or "delivery confirmation," which are still used in many attacks, sophisticated financial attackers tailor their phishing emails to a specific client, location or employee.

**Figure 3.**
Tailored phising email.




Perhaps the most unexpected trend we saw in 2016 was identifying that attackers had called victims on the telephone to help them enable macros in a phishing document, or to obtain a personal email address where the phishing document could be sent to avoid controls protecting corporate email. When a phishing email did not result in access to a target environment, the attackers sought to circumvent controls, even when it required a conversation.

Figure 4 is a sample email that was sent to our client after the attacker had spoken with an employee.

**Figure 4.**
Email sent after attacker called an employee on the telephone.

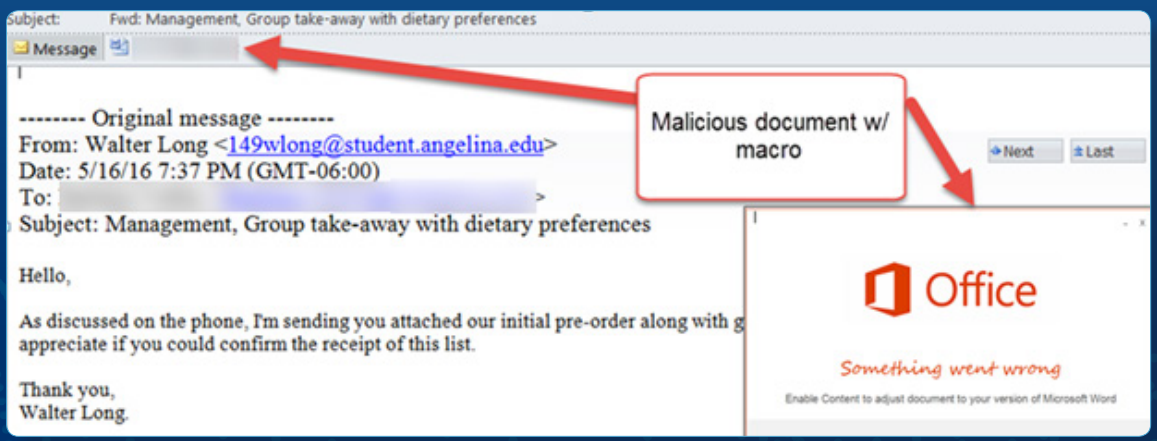
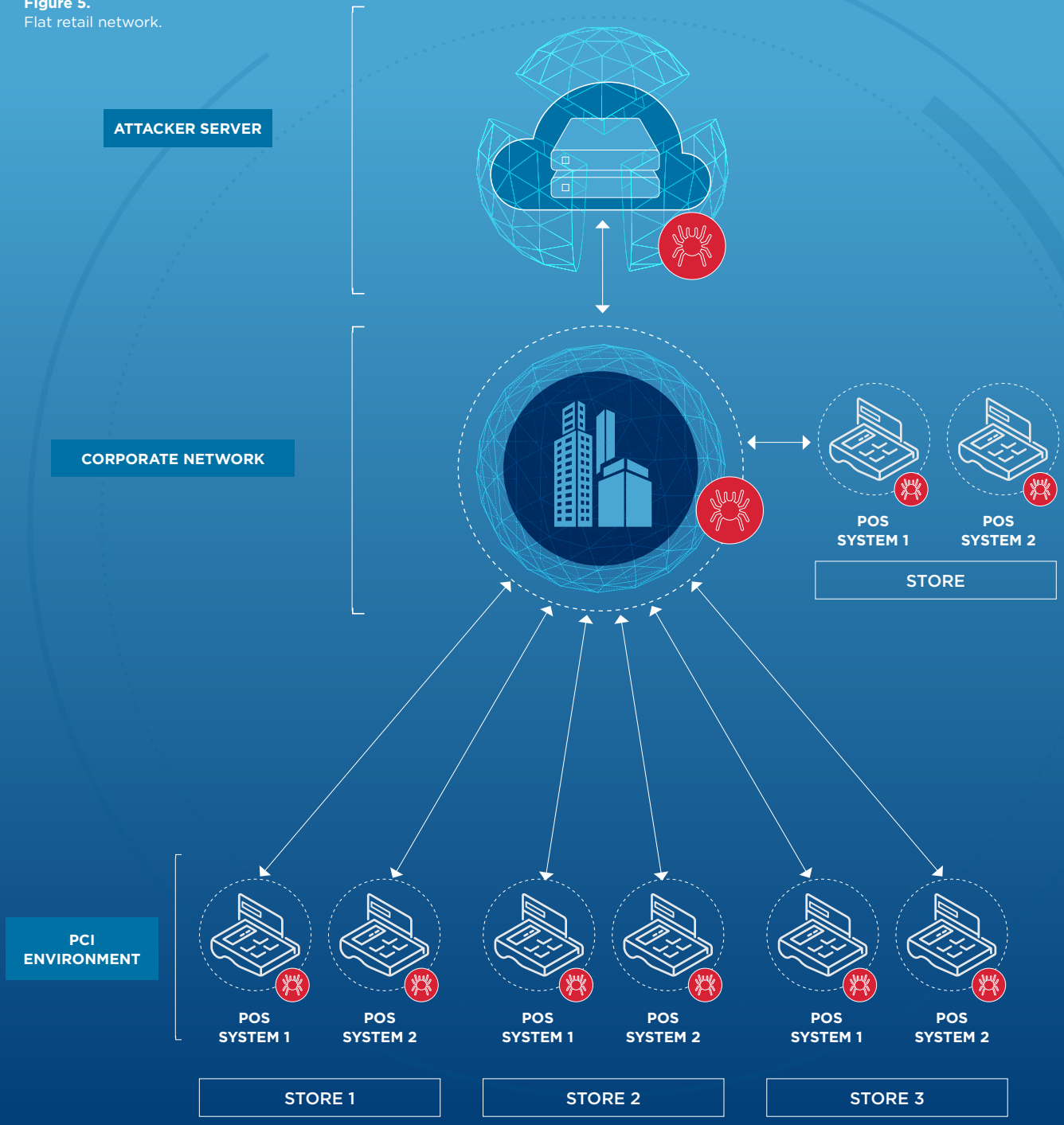


**Figure 5.**
Flat retail network.

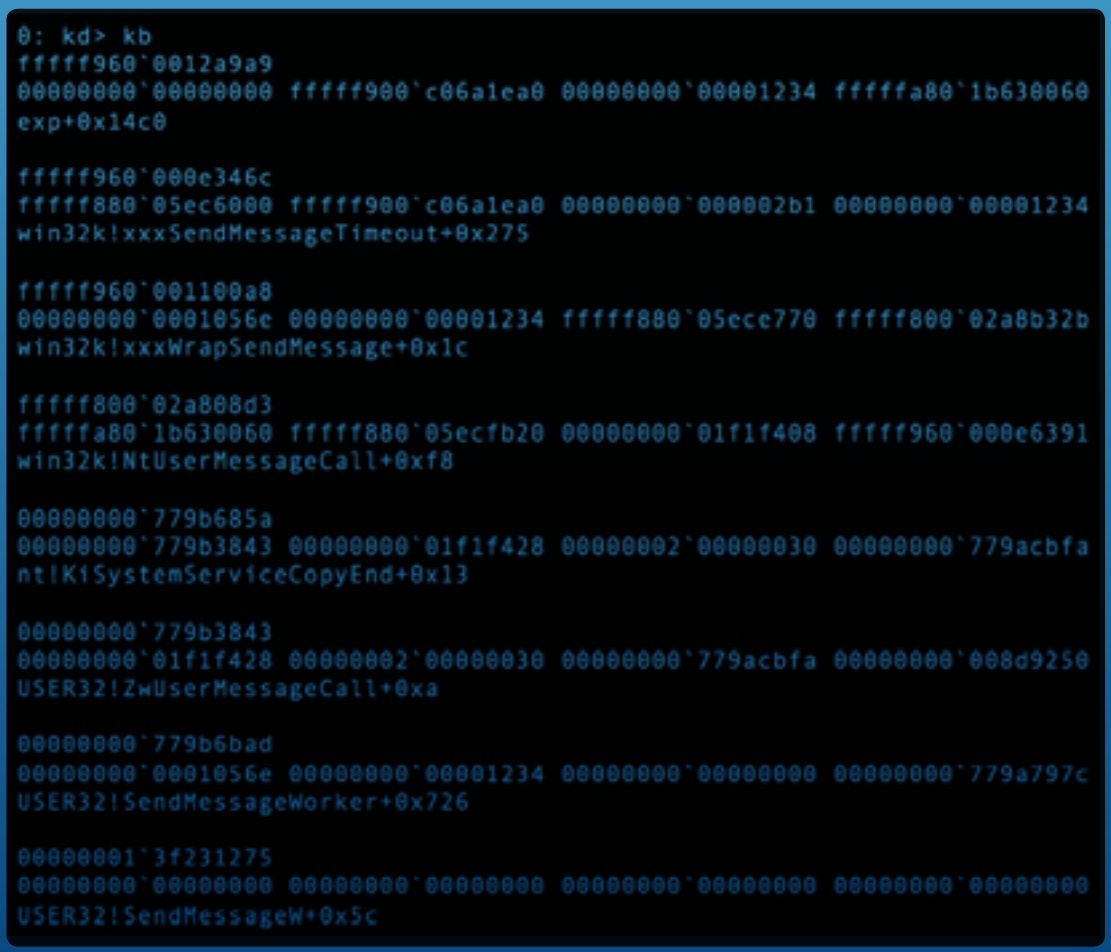



Unfortunately, most networks, including those with payment card information, are not segmented. The compromise of a single retail location often leads to the compromise of the larger PCI environment, making customer-facing employees in these retail environments the low-hanging fruit sought by attackers.

**Escalate Privileges**

Financial attackers also demonstrated their increased sophistication through the use of new tools and exploit techniques. A privilege escalation tool was identified during a number of investigations, though seldom used. The tool leveraged CVE-2016-0167, a previously unknown vulnerability. The tool allowed attackers to obtain elevated privileges in environments where the initially compromised user did not have them. Figure 6 shows an excerpt from a FireEye blog post which explained the privilege escalation technique.[1]

**Figure 6.**
Attacker privilege escalation technique.




1 https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html.

### Maintain Persistence

To ensure continued access to victim organizations, the attackers avoided reputational scoring built into web proxy and IDS/IPS solutions. This was done by storing backdoors and tools on legitimate sites, some hosted by vulnerable hosting providers or code repositories such as GitHub. Unfortunately, with sites such as GitHub, the connection is SSL encrypted, so in addition to being hosted on a legitimate site the payload is encrypted, preventing deep packet inspection.

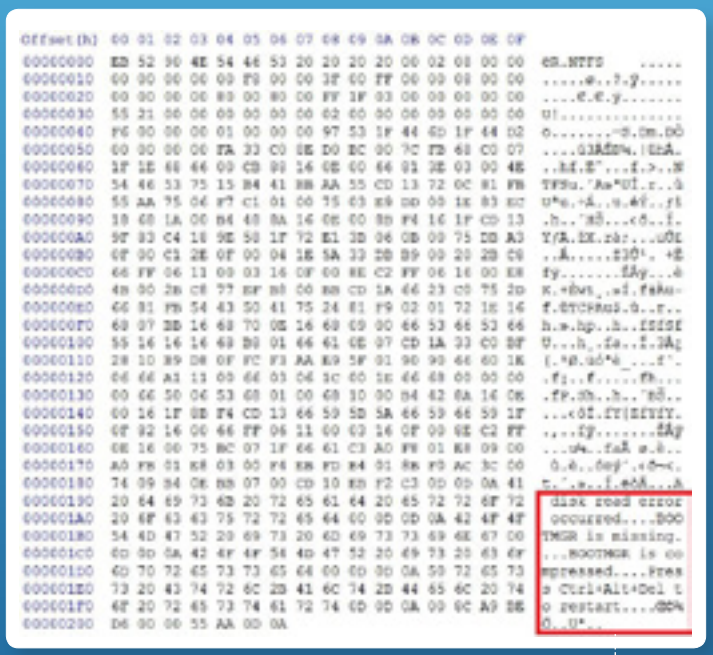
Attackers also took counter-forensic measures to further hide their presence and impair investigations. Figure 7 is an excerpt from a batch script used by a financial attacker to delete Prefetch entries, clear Microsoft Windows event logs and securely delete a file. The batch script was run to hide the execution of malware that was scraping payment card information from memory. The technique is simple, but the attacker's concern for and knowledge of forensic artifacts demonstrated increased sophistication, as well as their intent to persist in the environment.

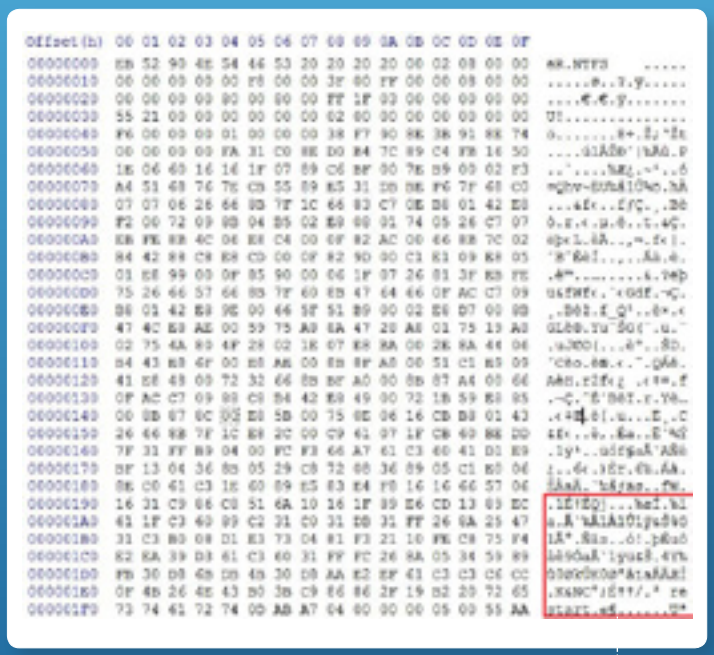
**Figure 7.**
Batch script to hide malware execution.

```
del /f /q /s %windir%\prefetch\*
reg delete "HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache" /va /f
reg delete "HKLM\Software\Microsoft\Windows\ShellNoRoam\MUICache" /va /f
reg delete "HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache" /va /f
reg delete "HKLM\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache" /va /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU" /va /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist" /va /f
wmic nteventlog where LogFileName='File Replication Service' Call ClearEventlog
wmic nteventlog where LogFileName='Application' Call ClearEventlog
wmic nteventlog where LogFileName='System' Call ClearEventlog
wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog
ren %1 temp000 & copy /y %windir%\regedit.exe temp000 & del temp000
```

The most significant evidence that the sophistication of financial attackers had left the realm of smash and grab was their use of persistence mechanisms such as Volume Boot Record (VBR) modification. This persistence mechanism allowed attackers to load their backdoor prior to the operating system. This enabled them to hide their backdoors and tools from investigative tools reliant upon the Microsoft Windows API. This marks a change as targeted attackers have often relied on the host operating system for persistence due to its ease of use and stability. The downfall of relying on the host operating system for persistence was that it created forensic artifacts that make even the most sophisticated backdoors detectable using indicators of compromise (IOCs) or hunting techniques. VBR modification does not have this drawback. While VBR modification was sparingly used at the beginning of 2016, by the end of the year it had become the attacker's go-to method for maintaining access to some environments. In one environment, the sole persistence mechanism used was VBR modification, making the backdoors loaded by the VBR modification extremely difficult to find.

**Figure 8.**
Visible changes between infected and non-infected VBR.





```
 disk read error
 occurred....BOO
TMGR is missing.
...BOOTMGR is co
mpressed....Pres
s Ctrl+Alt+Del t
o restart....
Ö..U
```

**Non-infected:**
Standard ASCII strings are clearly present.

```
.1É†ÈQj...‰æÍ.%i
a.Ã`‰Â1À1Û1ÿ&Š%G
1Ã°.Ñäs..ó!.þÊuô
âê9óaÃ`1ÿu&Š.4Y%
ûØøkÛK0Ø ªâïaÃÃÆÌ
.K&NC°;É††/.² re
start.«$.....U
```

**Infected:**
ASCII strings have been replaced with binary data.

## The Takeaway

Financial attackers go where the money is. Targeting financial information has been lucrative so organizations with this type of data need to be vigilant in the face of the rising sophistication of financial attackers.

## Bypassing Multi-Factor Authentication for Corporate Email Theft

When we talk about email, the discussion tends to revolve around phishing emails that are used to initially compromise an environment. Something we have not discussed as much is the fact that the volume of email stolen through the years is likely greater than all other forms of electronic data theft combined.

The 2016 United States presidential election brought email hacking and theft back to the forefront as a major cybersecurity issue. During the past year, Mandiant conducted many investigations that highlighted how attackers obtained access to email while bypassing network segmentation and multi-factor authentication when necessary.

### OAuth Phishing and Delegation

OAuth is an open standard used by applications to authorize the sharing of information without a password. Since 2015, Mandiant has observed an increase in phishing campaigns targeting OAuth tokens for cloud service providers, especially those that provide email services. While these OAuth attacks are not new, we have observed an increase in the use of these techniques to access the email and documents of targeted users as more businesses move to cloud-based providers.

With an OAuth token, an attacker has the ability to bypass multi-factor authentication to access a target user's cloud resources such as email, calendar and shared documents. Mandiant discovered that attackers used the following techniques to compromise users of an organization that used Google's G Suite for email:

1. The attacker registered and created a malicious Google application.

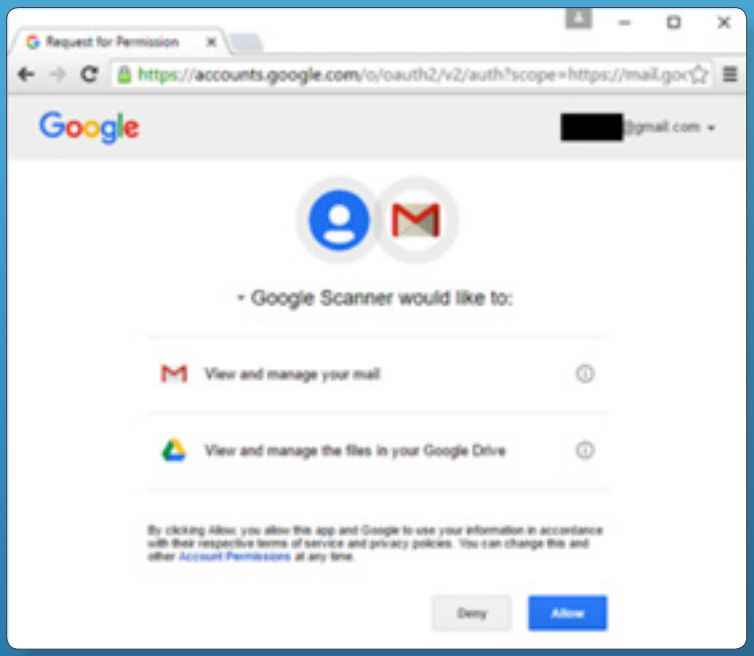
2. The attacker sent phishing emails containing a link to register the malicious application to their Google account.

3. Once the attacker's malicious application had permission, it could access the user's data, even after an account password reset.

Figure 9 is an example of an APT28 phishing email that Mandiant discovered during an investigation, which claimed to be from Google Support.

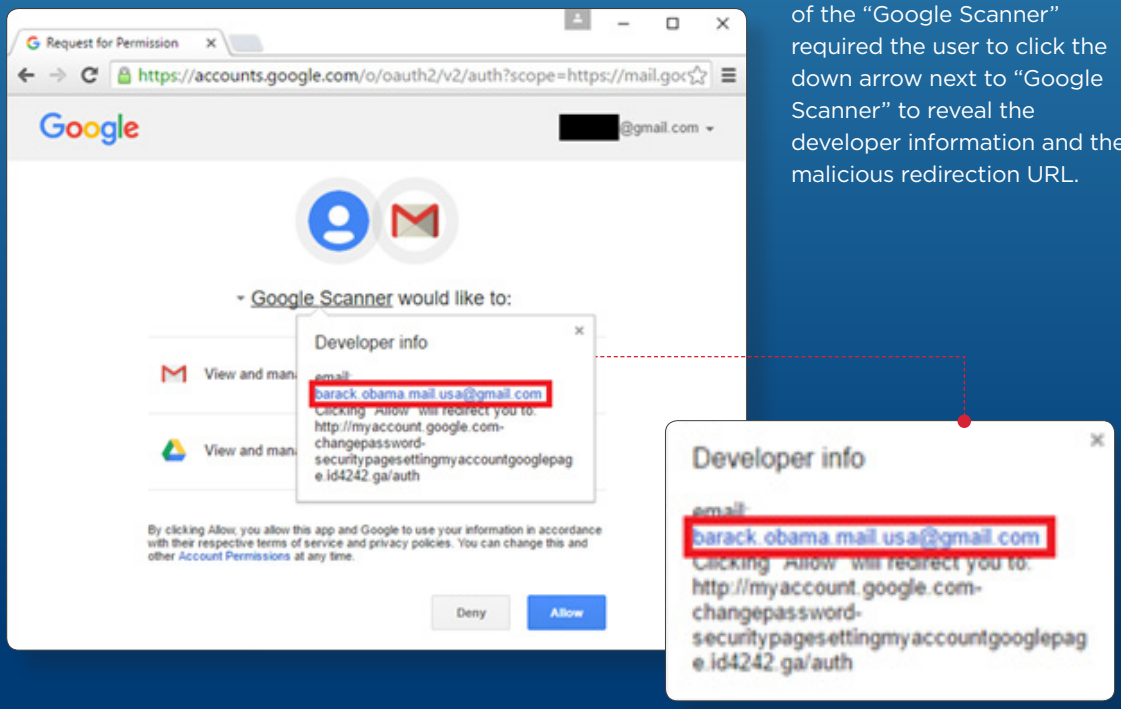
Figure 9.

**Figure 10.**




The "Permit Scanning" link in the email used a URL shortening service to hide the more suspicious full URL and evade link content inspection. When clicked, it launched the legitimate Google Accounts site. In this case, the user sees default images, the name Google Scanner and the confirmation that the site is secure in the address bar.

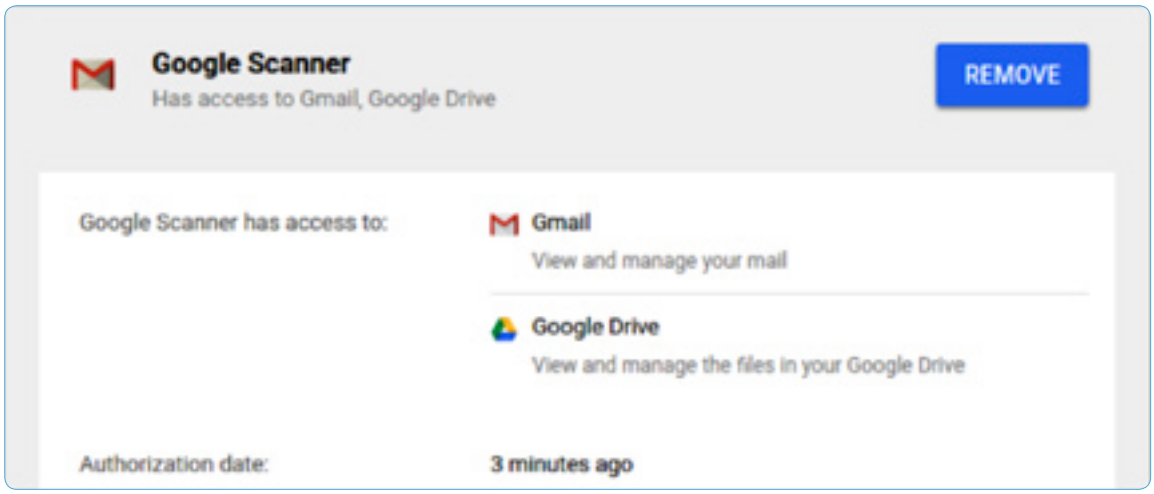
**Figure 11.**




Assessing the legitimacy of the "Google Scanner" required the user to click the down arrow next to "Google Scanner" to reveal the developer information and the malicious redirection URL.

When the user clicked the "Allow" button, the malicious application was granted an OAuth token with full access to read, write, and delete content from the user's Gmail and Google Drive.

Figure 12.




Monitoring for this type of activity on a host level is nearly impossible and detecting it on the network is also extremely difficult because most authorizations occur over an encrypted connection. In some cases, such as in the example above, the authorization occurred over HTTPS.

The most effective way we have found to identify these types of attacks is to use the service provider's administration panel to audit the authorized applications connected to an account and the OAuth token authentications. In Google's G Suite, this information exists in the OAuth token audit log. Once an investigator has identified the compromised accounts, they can investigate further to determine how the attacker gained access to the account.

**Microsoft Exchange Web Services**

Microsoft Exchange Web Services (EWS) provides the ability to access data stored in Microsoft Exchange programmatically over HTTPS. While Outlook Web Access (OWA) supports multi-factor authentication and Microsoft Azure-based Office 365 implementations support multi-factor authentication through the "Modern Authentication" feature, internally hosted Exchange instances do not have this option. This means that EWS and ActiveSync on internally hosted Exchange instance are single-factor only. Some organizations have not enabled the new authentication mechanism in Office 365 because some legacy clients on desktops and mobile devices do not support it.

**PowerShell Mailbox Harvesting Using EWS**
Mandiant has observed attackers abusing single-factor authentication in EWS to harvest emails from user mailboxes. For internally hosted instances, it is possible to do this from the Internet. In cases where attackers cannot directly access an email server from the Internet, Mandiant has observed attackers move laterally to Exchange servers to harvest emails. This lateral movement often occurs through a web shell backdoor that attackers place on the server, such as malicious active service pages (ASP) content or Internet Server Application Programming Interface (ISAPI) extensions for Internet Information Services (IIS). Mandiant has also observed attackers install remote desktop protocol (RDP) tunnelers to connect out from the Exchange server, which allowed them to bypass the perimeter security controls and establish an RDP connection to the server from the Internet.

APT29 used a custom PowerShell script to harvest the contents of Exchange mailboxes using EWS. The attackers tunneled traffic through intermediary servers to the Exchange server and used EWS API methods that the attacker exposed to the Internet to dump the contents of user mailboxes.

Figure 13 shows the command line of this PowerShell script, which allowed the attackers to target specific users and specify the days of email to dump from the server.

**Figure 13.**
PowerShell command line of EWS mailbox dumping script.

```
C:\\windows\\system32\\cmd.exe /c "powershell -ep bypass -f Dump.ps1 -Domain [DOMAIN] -User [USERNAME] -Password [PASSWORD] -Mailbox [EMAIL ADDRESS] -Days 1 -OutputFolder [OUTPUT FOLDER] -EWSUrl [EWS URL]"
```

In a default configuration, this technique leaves very little forensic evidence for investigators to follow, especially if the attacker securely deletes the output of the command.

### Mailbox Delegation

Mandiant also discovered APT29 attackers using mailbox delegation to access to the mailboxes of other users. This allowed one account to harvest the email for multiple accounts.

Investigators should review the MSExchange Management application log for successful cmdlet executions of Add-MailboxPermission with Event ID 1. This event identifies the permissions, target and recipient of the delegation. Typical indicators of malicious activity are a single account that has delegated access to more than one mailbox within a short timeframe or if an account has been delegated Full Access.

Figure 14 shows an example of a successful delegation from the event log.

**Figure 14.** Example event log entry for successful Add-MailboxPermission cmdlet with Full Access.

```
Cmdlet succeeded. Cmdlet Add-MailboxPermission-++-{AutoMapping=False, User=[Email Address],
AccessRights={FullAccess}, InheritanceType=All, Identity=[AD Distinguished Name]}-++-
```

**Tactical Recommendations**
Tactical recommendations to detect these attacks include enhanced auditing of changes to email or multi-factor authentication infrastructure.

- **Enable Multi-Factor Authentication (MFA) for Email:** Mandiant recommends using a time-based one-time password (TOTP) hardware token smartphone-based application as a second factor of authentication. Avoid technologies that use SMS or device certificate-based authentication, as these solutions are easier to bypass.

  If your organization uses Microsoft Office 365, ensure that the "Modern Authentication" option is enabled and clients are using the Azure AD Authentication Library (ADAL). Note that this option will prevent legacy desktop and mobile clients from authenticating to the service. Avoid exposing internally hosted Exchange servers directly to the Internet since EWS and ActiveSync on these systems do not support MFA. Require users to VPN into the corporate network using a VPN that requires MFA before accessing their email.

- **Conduct Dynamic Link Analysis:** Conduct dynamic link analysis for email content inspection. Users are generally more likely to recognize a malicious URL in its expanded form.

- **Educate users on the security risks of connecting applications to their accounts:** Additional security awareness training should focus on teaching users how to validate whether an application is requesting excessive permissions to their account or if that application might be malicious. Teach users how to check the authorized applications and devices that can access data in their accounts. Sites such as Google and Facebook periodically remind users to check their security settings and connected applications and devices.

- **Audit Connected Applications:** Periodically audit applications that use OAuth to access user data. Ensure that the authorized applications are legitimate and have a business need.

- **Enhance PowerShell Logging:** PowerShell usage has very little logging in its default configuration, but there are options to increase this logging. Mandiant has previously written about PowerShell's enhanced logging on the FireEye Threat Research blog.[2] Module Logging and Script Block Logging can help forensic investigators determine the malicious PowerShell commands run by attackers.

- **Audit Multi-Factor Enrollment:** Generate alerts when users enroll devices for multi-factor authentication. Mandiant recommends monitoring the following events:

  - Token or device registrations. Determine if users have multiple devices connected to their account(s).
  - Users with emergency bypass codes or PIN-only mode.
  - Location data of connections such as country and IP address. Determine if the source of the authentication requests are anonymization services or VPN/hosting providers.

- **Audit Exchange Mailbox Delegation:** Periodically audit and review the delegation permissions assigned to mailboxes within Exchange.

2 https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

## Target: Banking Networks

Banking network fraud incidents have spread around the world. Incidents have struck banks in Asia, Ukraine, Ecuador and India with losses totaling more than $100 million. These widespread events indicate that financial criminals see these networks as ripe for manipulation.



**Case Study - Banking Compromises in Asia**
In early 2016, the staff at a bank in Asia was unable to access a domain controller – a server that responds to security authentication requests within a Windows Server domain. An internal investigation discovered that a suspicious account had been created with domain administrator privileges, enabling unrestricted access to thousands of Windows systems – both servers and clients – across the enterprise. The bank quickly realized that many host systems had been compromised using a malicious logon script that distributed and executed the attacker's malware.

The initial intrusion occurred two months prior to initial detection, originating from a remote location within a wholly-owned subsidiary's network. The attackers found a system that had trusted access to the bank's enterprise infrastructure and leveraged this to access the bank network undetected. After establishing persistence in the Microsoft Windows environment, they obtained Domain Admin access across multiple hosts. The attackers leveraged Remote Desktop and Tivoli Remote Control along with built-in Microsoft networking tools (all genuine enterprise management tools used by the bank's IT staff) and were able to blend in to the bank's environment, making it difficult to detect their presence or differentiate malicious behaviors from the bank's legitimate activities.

We uncovered evidence indicating that after planting backdoors, the attackers utilized screen grabbing and keylogging capabilities to capture passwords from authenticated users. There were 30 hosts identified with screen grabber malware artifacts and more than 50 user profiles were compromised by key logging software.

The attackers had access to credentials and information that included Lotus Notes, the decoding of National Payment Message Standard (NPMS) format files, the Export-Import Bank of the U.S (IMEX) data and Customer Information Control System (CICS).

Altogether, the presence of breach artifacts was confirmed on 96 systems – 26 servers and 70 workstations – and 30 systems were found to have active malware running at the time of investigation.

**PRESENCE OF BREACH ARTIFACTS CONFIRMED ON**

| 96 | 26 | 70 |
|---|---|---|
| SYSTEMS | SERVERS | WORKSTATIONS |

**ACTIVE MALWARE ON**

| 30 |
|---|
| SYSTEMS |

**Banking Network Compromise in Europe**

During 2016, Europe and Middle East-based financial institutions were targeted by attackers. In one investigation, the attackers used PowerShell and Metasploit to move laterally into the banking network environment. Once in the banking network environment, the attacker modified a compromised banking network user account to no longer require "four-eyes" approval on transfers. Four-eyes approval is the requirement that two sets of eyes are needed for every transaction – one set of eyes to initiate the transaction and another set of eyes to approve the transaction. The attacker compromised both an account used to initiate transactions and an account used to approve transactions. Mandiant investigators surmise that the attacker had significant knowledge of banking network transactions, in part evidenced by knowledge of the four-eyes process and how to circumvent that requirement by escalating the privileges of a targeted banking network account. If the attacker had utilized both accounts, the "approver" would have likely been notified of the transactions through the normal alerting processes and the transactions would likely have been noticed sooner.

Once the attacker had control of the process, they began to make a series of banking network transfers worth millions of dollars. Banks typically have a grace period on banking network transactions and can recall transfers during that grace period. To circumvent the grace period, the attacker wiped event logs and then reformatted system volumes on systems in and out of the banking network environment. This caused outages that delayed the bank's identification of the fraudulent transactions, giving the attacker more time to withdraw funds that had been transferred.

In total, we confirmed 45 affected systems — 29 servers and 16 workstations.

**TOTAL AFFECTED SYSTEMS**

45
SYSTEMS

29
SERVERS

16
WORKSTATIONS

### Comparing the Banking Breach Investigations

After comparing the TTPs and decode scripts from the aforementioned banking breach investigations, it was clear that we were dealing with the same threat group. Several similarities emerged.

#### MALWARE NAMING

The threat actors were good at blending into an environment and using naming conventions to suit the environment. However, they seemed to favor the use of tools named "hkcmd.exe", "igfxpers.exe" and "msdtc.exe". Just because a binary was named "hkcmd.exe" did not mean it was always the same malware. They often used C:\Windows for the malware and it was unsigned.

#### REGISTRY RESOURCES

We observed the use of "MsOutData" (which stored an encrypted binary blob) in both environments as well as the "SOFTWARE\Classes\NR\Content Setting" registry value, which stored the configuration data for their malware. They used the identical 4-byte XOR key in all cases. We first observed this "Content Setting" in a 2014 banking breach investigation.

#### ENCRYPTION

We observed consistent use of the same 4-byte XOR keys for the malware configuration. We identified some RC4 keys that were used consistently across the engagements for the NESTEGG malware that was deployed. We also observed that the attackers used the same command line passwords for launching tools in all engagements. For example "[2016-02-24 14:25:04] At3 | | | c:\windows\msdtc.exe | -x nf300karjfs9e8rhtQJ3u9gh -e Nla" at some and "At1 | | | C:\windows\hkcmd.exe | -x nf300karjfs9e8rhtQJ3u9gh -e LogonHours" for others.

#### OTHER TTPS

In all engagements, we observed that the attackers configured their malware to execute at SAFEBOOT (SAFEBOOT registry keys were updated). The attackers used "Windows Firewall Remote Management" or "Microsoft Update" as their firewall rulename for updating the firewall rules to allow network access. The events followed a common timing pattern (no doubt because of they were using the same backdoor family). Attackers commonly deployed screen grabber / keylogger malware. The output files used the same naming conventions.

We also observed some changes over time. Initially, keylogs were in ".cache" files within the Internet Explorer directory. Later, they switched to using ".cer" files. Attackers made use of an "sdelete" type functionality where they renamed the file with a random name (same length, just random alpha chars) and also overwrote the file content. These artifacts were seen in all engagements.

The capabilities exhibited by the threat actors — including the unique malware customization, attack sophistication, and the CnC infrastructure infiltration — indicated that they are a well-funded, highly organized group and that the attacks were structured and specifically targeted.

# FireEye as a Service – A View Into Emerging Threats

FireEye as a Service (FaaS) provides managed detection, investigation and response capabilities to help organizations fully understand the threats with their environment, assess risk and take recommended action. Due to its ongoing monitoring of organizations around the globe in all industries, FaaS has a unique perspective into emerging threats and evolving attacker TTPs.

**FaaS: Providing Answers, Not Alerts**

FaaS analysts look at compromises across all regions and industries to ensure our customers are seeing the full threat picture behind each attack, thus helping deliver executive risk awareness in addition to advanced threat protection and response capabilities.

## OBSERVATION 1
## New Campaigns, Old Techniques

Not all new attacks utilize techniques analysts have never seen before. Some attackers still utilize old school tactics to gain access. Threat actors are increasingly targeting executives and other high-level employees, tricking them into activating malware that gives criminals access into their companies' environments.

### EXAMPLE 1
### New APT29 Spear-Phishing Threat

In August 2016, the FaaS team discovered evidence of a new APT29 spear-phishing event against one of our U.S.-based clients in the technology industry.

APT29 is a Russian group that engages in cyber operations where the primary goal appears to be data theft. APT29 targets include Western governments, foreign affairs and policymaking bodies, government contractors and universities.

The FaaS team initiated proactive network hunting efforts for all FaaS customers and conducted forensic services (sweeps) at clients that had previously been targeted by APT29 actors.

As a result, the FaaS team submitted multiple malware samples to the FireEye Labs Advanced Reverse Engineering (FLARE) team.

This analysis led to the identification of three new APT29 malware families: the malicious macro documents (VERNALDROP) that drop a stage one downloader, which retrieves a second stage backdoor (TADPOLE); and the second stage backdoor (SPIKERUSH).

### EXAMPLE 2
### Financial Cyber Threat Phishing

In March 2016, the FaaS team observed attacks against FireEye and FaaS clients in the retail, hospitality and entertainment industries as part of a phishing campaign.

FireEye was able to attribute these attacks to FIN8,[3] a financially motivated group that had previously conducted several tailored spear-phishing campaigns. The group used email attachments that were Microsoft Word documents containing an embedded macro which downloaded a payload from a web-based cloud storage service or actor controlled website. The loader then installed a PUNCHBUGGY variant providing the actors with remote access to the victim machine.

In the course of the investigation, the FaaS team also observed that the threat group modified their phishing techniques and started masquerading as a Mandiant consultant by modifying the title and content of the phishing email to indicate the actors knew they were detected in client environments.

**NEW PHISHING TEXT**

I have been advised to contact you in reference to the dispute that took place at on Tuesday. Kindly refer to the attached document for comprehensive details about the incident.

Would you mind to view the complaint and get back to me with your thoughts on this?

Thank you.

**END PHISHING TEXT**

Spear-phishing attacks continue to rise and be successful, as these emails are created with enough detail to fool even experienced security professionals.

3 Financially motivated advanced persistent threat groups are categorized by FireEye as FIN, while state-sponsored advanced persistent threat groups are APT.

## OBSERVATION 2
### Common Techniques Found from Analysis of Industry Level Data

Constantly analyzing network data enables the FaaS team to quickly identify new threat and attack campaigns.

## OBSERVATION 3
### Existing Knowledge Aids in Finding New Evil

Staying up to date on the latest activities and trends in the threat landscape will help you identify attacks before they happen. New threats are born daily. Having the right intelligence in place and minimize the damage if a breach does occur.

## EXAMPLE
### New Threats in High Tech

In June 2016, FaaS performed in-depth cyber security event investigations at U.S.-based clients within the high tech industry which involved different actors and malware, but had similar characteristics in the way they used legitimate services to gain access.

One technique common to both threat groups was the use of legitimate web services such as GitHub and Microsoft TechNet to communicate with backdoors. These communications were either complete command and control instructions to their victims or were used to utilize the associated backdoor to update CnC infrastructure.

Based on our observation of separate threat groups using legitimate services to infiltrate environments, the FaaS team refined the NetFlow analytic and ran it across all of our customers in the technology industry to identify any suspicious connections to GitHub or TechNet indicative of these backdoors. FaaS has not identified any new compromises for our customers to date.

## EXAMPLE
### SHAMOON Malware

In November 2016, FireEye observed destructive activity at a client that was indicative of the SHAMOON malware seen in previous destructive attacks.

The client is in a critical infrastructure-related industry in a Middle Eastern country. The identified malware exhibits destructive behavior on Windows-based operating systems, uses a signed RawDisk driver from EldoS and renders a disk unbootable once fully executed.

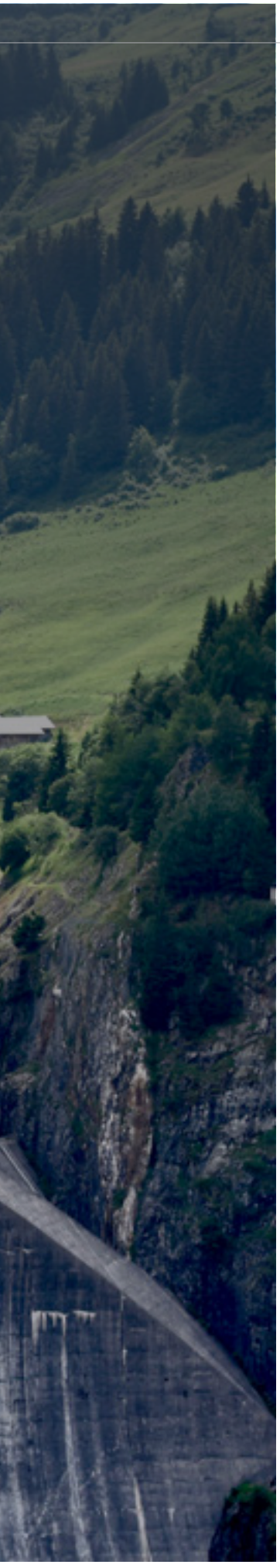
While being a fully functional backdoor, SHAMOON has primarily been used to destroy data on disk, and render systems inoperable. Based on the design of the SHAMOON malware family, it is believed that the implant is leveraged in later stage operations after actors have gained and secured access to a victim network and at least possess network credentials. Upon execution, SHAMOON leverages network credentials to propagate a dropper to systems on the same network that contains multiple subcomponents. One of these components, the wiper, will destroy data on the target system. Destructive features of the malware are supported by a secondary and legitimate driver component used to access the hard disk, which has become a trademark characteristic of the malware family.

Initial forensic evidence exhibits several similarities to the SHAMOON malware used against Saudi Aramco in 2012 and other targets.

**Tactical Recommendations for Staying Protected Based on These Three FaaS Observations:**

- Ensure all of your certificates and software are up to date.
- Control software installation from one central location to ensure only authorized software gets installed.
- Use application whitelisting to better control what programs can be run on a host.
- Configure web proxy in whitelist mode and block uncategorized sites.
- Consider reviewing Office settings and disabling macros from running.
- Educate employees of the risks involved with social engineering and phishing attacks.
- Restrict administrative permissions associated with user accounts.
- Enable host-based firewall.
- Ensure backup of data is enabled for high valued assets.
- Ensure production systems are installed with latest updates.

# Defensive and Emerging Trends





## Adapting Foundational Defenses for the New Normal

As attackers innovate and threats evolve, security organizations need to re-examine the fundamentals of their information security programs to ensure they are adapting to the realities of the evolving threat landscape and related risks. Based on our investigations and strategic assessments, we have identified four key fundamentals that should be re-evaluated on a regular basis.

**Maintaining Visibility**

"Visibility" in the cyber security context refers to an organization's ability to detect, alert on, and investigate attacks – as in,"seeing" the malicious cyber activity. It is a fundamental capability for any effective security team, and blind spots in the infrastructure can lead to major problems. A relatively common example of a visibility gap is the lack of security data from an organization's endpoints. As the cyber threat landscape evolves, visibility gaps can emerge where once there were none. The use of cyber threat intelligence is critical for organizations to identify potential blind spots as threat actor techniques change.

Windows PowerShell is a good example of a relatively new attack vector that many organizations are not monitoring and logging. Attackers are increasingly leveraging Windows PowerShell to conduct their operations when undertaking malicious activity within a victim's environment. In many environments, PowerShell does not leave artifacts indicating its usage. In fact, most organizations do not even have visibility of who is accessing it or when it is used. This situation can be improved by upgrading older versions of PowerShell (such as 2.0) to later, more robust logging versions (5.0 offers a much broader range of security information) and by implementing additional logging features such as Sysmon. The bottom line from an incident response perspective is that while PowerShell logging was not a typically monitored event to maintain effective cyber threat visibility five years ago, it most definitely is now.[4]

Cloud security monitoring is another area of environment monitoring that is required for effective cyber threat visibility, and one that many organizations still struggle to undertake successfully.

### Some questions to consider for cloud security:

Can the organization see what files are being downloaded from a cloud based storage site?

Are administrator logins tracked and reviewed?

Can you detect unauthorized provisioning of cloud infrastructure?

What security event information can the cloud provider produce for your organization that will allow correlation or additional context during an incident?

There are numerous ways to improve visibility for cloud transactions, but they require adjusting the security team's focus as the threats expand beyond the perimeter. While visibility is not the silver bullet of cyber security, it does increase the capability of any organization to detect and respond to those threats that substantially increase risk.

With organizations supporting a more mobile workforce, the notion of the network perimeter has dramatically shifted. Networks that traditionally had clean borders and limited demarcation points are expanding. Visibility is required not only within the network, but also in vendor connection points, mobile endpoints, subsidiary organizations and other interconnections. The capability for endpoints to be monitored, updated and forensically queried while off the network has grown in importance. These issues have spurred a rising need for flexible sensor architectures that scale detection, investigation, data collection and processing in a cost-effective manner.

4 "Greater Visibility Through PowerShell Logging" (https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html)

**Rethink What is Critical to the Business (Understanding the Infrastructure)**
Headlines and regulations focus on sensitive data (PII, PHI, PCI) and data breaches. However, every organization should also consider their resilience to a cyber threat by asking, "What internal systems and data flows must be protected for the business to continue to function?" Mandiant teams have seen a rise of business disruption attacks where the attackers are not motivated to steal data, but rather to damage core business processes. Even when an attack such as ransomware is not necessarily motivated by disruption, business operations can quickly suffer collateral damage. Ransomware that locks a business-critical system can quickly and seriously damage business operations and requires different mitigation approaches rather than preventing the exfiltration of sensitive data. Organizations need to examine every possible scenario and have playbooks ready to implement.

**Companies should be assessing the controls in place that can mitigate business disruption risks:**

Are business-critical systems (not just data stores) identified, patched regularly, and hardened against attack?

If a destructive malware attack occurs, and the infrastructure is rendered inoperable, how will key personnel work? Are contracts in place to enable rapid deployment of virtual desktop infrastructure (VDI) for key personnel and virtual server farm if needed?

Are critical systems such as business databases backed up, and are those backups secured against malware that might infect other parts of the network?

Are there manual processes that can temporarily replace critical business systems for a short period of time while reconstitution of networks are occurring?

Is maintaining business operations accounted for in the Incident Response (IR) Plan?

### Network Segmentation and Data Segregation

In incident response and security program assessments, Mandiant still finds that the familiar concept of network segmentation and data segregation has been overlooked. When customers overlook these fundamentals, detection and remediation are much more difficult and the resulting impact of the breach is significantly higher. Lack of segmentation (both data and network) leads to easy lateral movement as illustrated in the APAC and EMEA financial sector breaches.

Segmentation can be effective in restricting threat actor movement within the victim environment and can help limit access to sensitive data. Typically, firewalls and VLANs are used to separate the network into trust zones. One trust zone may contain PII, another may contain proprietary data and the next zone may hold point of sale terminals. Network segmentation helps reduce the ability of a threat actor to move within the environment once they gain a foothold by limiting their access to a single trust zone and limiting the amount of data that can be accessed. Segmentation increases the level of expertise a threat actor needs to acquire access and requires additional time and movement, providing organizations additional opportunities to detect threat activity. Authentication and authorization controls provide further segregation at the system or data level, ensuring that there is separation of duties and applying "least privilege" to individual user credentials. Data segregation helps reduce the ability of a threat actor to access the organization's data with a single compromised credential.

Monitoring the network traffic across segmented trust zone boundaries gives organizations the ability to detect anomalous traffic patterns that could indicate a compromise. Applying user behavioral analytics across individual trust zones can give organizations more granular visibility into logon patterns, potentially making it easier to identify malicious credential use and allowing organizations to focus advanced monitoring tools on their most critical data assets.

Compromises are inevitable, but segmenting networks, segregating data and ensuring there is visibility to detect anomalous patterns between trust zones can help an organization detect threat actors and reduces the impact and risk resulting from compromises.

### Elevating Risk Awareness

In the past, boards of directors may have received an annual or biannual report on the state of security in their organization. As the number of breaches escalated among all industry sectors, cyber security became an important business risk that demanded to be incorporated into business strategies and new channel offerings.

We are observing increased risk awareness based on threat intelligence, as well as the media coverage of cyber breaches, ransomware attacks and other destructive attacks. All organizations are at risk and recognition of this by business leaders, senior executives and boards is usually critical for the implementation and maintenance of effective mitigation strategies to reduce the impact of attacks. New regulations being introduced are requiring board members to monitor and acknowledge in writing that they accept the security risks in their organizations and accept the cyber programs in place. As cyber attacks become more frequent and sophisticated, organizations of all sizes across every industry must make cyber risk management a priority, going beyond the IT department. C-level executives, business line leaders and boards of directors need to take an active role in cyber risk management and data breach preparedness.

Boards, senior executives and business line leaders should develop a cyber risk playbook.[5] Organizations need to develop a post-assessment action plan to help prepare for future risks and attacks

5 https://www2.fireeye.com/cyber-risk-playbook-web.html

## A Look Forward - An Intelligence-Led Approach to Security

**Threat Intelligence Taking the Driver's Seat**

We have seen that the incorporation of threat intelligence contributes to the success of an information security team. Previously, most organizations considered threat intelligence a "nice to have" rather than a "must have." This resulted in organizations not truly understanding the benefits that intelligence provides for risk reduction, prevention, detection and response. Increased complexities in business delivery channels, market strategies and attacker methodologies have significantly increased the need for effective threat intelligence, even in organizations that historically may not have felt the need.

**Moving from Reactive to Proactive Defense with Threat Intel**

Operationalizing cyber threat intelligence (CTI) is a trend we are starting to see take a prominent place within enterprise security operations. This is ultimately a good thing; however, there are a lot of misperceptions within the marketplace. It is important to reinforce that:

CTI is **not** an appliance, a data feed, or raw information, without supporting analysis and judgement.

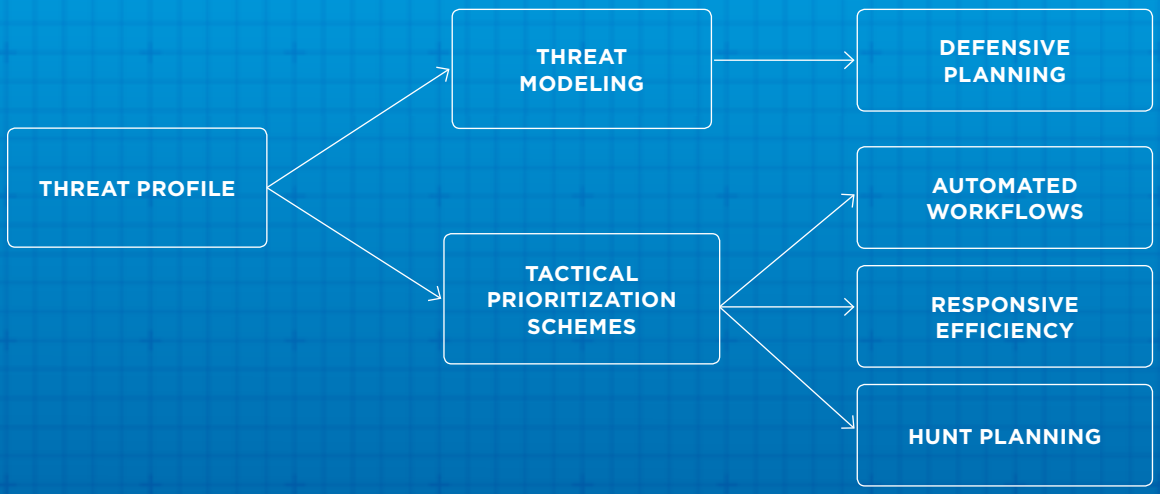
CTI is accurate, timely, and relevant knowledge about an event or series of events decision-making.

CTI should be based on some type of attributional understanding of the event(s). Attribution should include an understanding of the motives, intentions, and capabilities under which the individual(s) operate.

CTI should ultimately be derived from sound human analysis of observables gathered across a diverse set of sources.

We are seeing CTI play a significant role within many of the defensive trends outlined in this section, including automation and hunting. Organizations are increasingly using threat intelligence to build and update their own organization's baseline threat profile. Whether through analysis of malicious trends within their network, analysis of threats affecting their sector, businesses carrying similar assets, or doing business in similar regions, or a hybrid of all of these, CTI is being leveraged to characterize and contextualize threat activity specifically relevant to their business concerns. Executives and senior management are using this knowledge to better understand and plan for the risks facing the business. In turn, this enables more efficient tactical operations in terms of hunting, identification, prioritization and response. The following graphic outlines how the flow of intelligence can inform these operations.

Figure 15.




## THREAT PROFILE

A baseline of the most relevant threats to the organization – why the threat activity is occurring, what assets are targeted, and what the operations look like. This knowledge enables you to identify risk more clearly, align defensive posture with capabilities actors bring to bear, and set tactical prioritization schemes.

## THREAT MODELING

Informed by knowledge gained from the threat profile regarding assets targeted and attacker motivation, threat modeling exercises provide clear insight into what is occurring within threat landscape and what specific portions of that landscape your organization needs to be concerned with. Understanding adversary capabilities surrounding organizationally relevant threats gives you higher fidelity that the measures taken to align and strengthen your defensive posture are linked to business concerns and are therefore justified.

## TACTICAL PRIORITIZATION SCHEMES

The threat profile should also make it clear which threats present the highest impact to the organization and how they should be prioritized.

- **Automated Workflows:** Automation of event handling. Escalating only those events potentially related to high priority threats improves operational efficiencies, ensuring investigation and response time is spent in the right areas and lowering security operational costs.
- **Response Efficiency:** Intelligence properly integrated into these workflows informs response activity by readily providing knowledge of implicated threat actor operations – tools used, supporting infrastructure, tactics, techniques and procedures. This tells responders where to look and what to look for, enabling more effective response.
- **Hunt Planning:** Hunt missions can be designed to specifically focus on the capabilities linked to high priority threats, adding efficiencies by informing efforts to identify specific tactics, techniques and procedures, communications, tools and other operational indicators – rather than relying on personal expertise.

**Automation / Orchestration**

Most organizations have developed an IT and security infrastructure over a long period of time with numerous security technologies and software incorporated as point solutions. The data from those systems has typically been tied to some type of security incident and event management (SIEM) system where security operations center (SOC) analysts review alerts seeking to correlate logs from those disparate sources across the enterprise. This has led to a huge uptick in what security professionals refer to as "alert fatigue". Critical alerts are hidden in a deluge of false positives and non-useful data. Finding the important signal of a compromise in the noise of alerts has become an increasingly significant challenge in 2016.

To counter this data and alert overload, organizations are relying more on tools and processes to filter data and automate analysis to redirect valuable security resources to more complex incident investigations and response. This is especially true in smaller organizations that may only have one or two security resources. Automation can eliminate time spent on smaller and repeatable events, allowing redirection of resources for hunting, proactive defense and other tasks. Creating playbooks for repeatable events can enable automation of disposition of false positives, minor alerts, and informational alerts allowing time to focus on the critical alerts in the environment and decreasing response time.

## Threat Hunting

Active threat hunting is a human-centric process by which security practitioners search through data to find evidence of intrusion using a variety of techniques. While the investigation process remains the same after evil has been found, hunting differs from typical alert-driven investigations in that a human is responsible for generating their own investigative leads to pursue.

In the not too distant past, actively hunting for intruders on your network was something reserved for the most experienced practitioners in the most well resourced security operation centers. More recently, we've seen smaller organizations and less experienced analysts electing to participate in hunting activities and actively seeking tools, technology and staff to support this function.

It is common for relatively scarce and innovative techniques to flow down into more common practice over time as techniques become better codified and automation tooling becomes available. It is not surprising that hunting followed suit as well. We attribute the rise of hunting operations to three things: the evolution of opportunistic attacks, enhanced security operation center visibility and a collective experience increase amongst practitioners.

Threat hunting is to incident response as event correlation is to incident detection. Threat actors are humans, and as such, exhibit behavioral patterns in their methods that can be used to identify origin of attack, identity of attacker, motivations, methods or toolset. By uncovering similarities and patterns in attack instances by combining these TTPs, IOCs and similar trends, these correlations solidify into actionable data that can be used to identify, respond to and thwart future attacks.

### Opportunistic Attacker Evolution

Several attacker techniques are inherently hard to detect because of their reliance on compromising legitimate user accounts. Additionally, many of these techniques are focused on latter parts of the attack lifecycle — after gaining an initial foothold and often avoiding the use of malware, instead relying on built-in operating system tools such as PowerShell. Traditional detection mechanisms generally fail at detecting these techniques without a plethora of false positive alerts, requiring a more human-centric approach.

Threat hunting provides an opportunity to detect such scenarios, as it affords analysts the ability to perform manual searches and aggregations against known normal activity to find outliers based on attributes such as the time the activity occurred or the expected behavior of the user who conducted it. For example, if a user in the finance department uses PowerShell, that might be unexpected. Furthermore, if that user logs into multiple machines at an odd hour, that too might be worth an investigation. Mature security organizations invest in threat hunting, because traditional machine-centric detection tools don't effectively help in many of these scenarios.

### Increased SOC Visibility

Many organizations have spent time thinking about visibility and have invested in it accordingly. This includes deploying more network sensors, switching to distributed sensor models to encompass branch offices and deploying endpoint agents for host-level visibility.

As the amount of data SOCs can interact with increases, more use cases are enabled that can be used to uncover malicious activity. Simple aggregations such as selecting HTTP user agents observed in network traffic and sorting that list by least frequently seen occurrences can yield a number of interesting data points. However, such analysis is often better suited to manual analysis than automated detection.

Additionally, use cases where network and host data can be correlated to provide a clearer picture of compromise are becoming better enabled as endpoint detection and response tools gain favor. By correlating the execution time and hash value associated with the file to network logs, a SOC analyst could determine where the file was obtained and how it came to exist on the system. Analysis of the source will yield additional data points that could lead to discovery of further infection. This is an ideal hunting scenario made possible by increased visibility.

### Increasing Skills

While threat hunting used to be a niche skill, it has become better codified and accessible to less experienced analysts as more training and tooling to support the skill has become available. We have observed an increase in the number of talent acquisition requests for threat hunting expertise from security mature organizations. We've also seen far more resumes coming into organizations from individuals who claim to have threat hunting experience. Threat hunting is now among the most commonly sought skills in defensive security and the associated training and education markets are shifting to meet this demand.

We anticipate these trends will continue. The sophistication of opportunistic attackers will grow and security conscious organizations will attempt to defend themselves with more visibility, which will breed threat hunting skills in analysts with a willingness and curiosity to explore data to find evidence of compromise.

# Spotlight on APAC Regional Trends

## CONTINUED FOCUS ON FINANCIAL CRIME

FireEye observed a continued focus on financial services organizations in APAC. Headline breaches dominated the financial services industry for 2016, and Mandiant continues to respond to significant sophisticated compromises in these industries as well as many others driven by financial motivation.

## ATM ATTACKS

2016 brought a notable increase in attacks against ATMs and ATM networks using various types of malware. Similarities between ATM compromises with significant financial losses in Thailand and Taiwan strongly suggest these were linked to actors and activity in Eastern Europe.

## NATION-STATES ON THE HUNT FOR PII

Various regional nation-state-sponsored APTs continued to harvest vulnerable commercial and government systems for PII for influence, intelligence and political gain.

## ESPIONAGE TARGETS ON CHINA'S PERIPHERY

Geopolitical events within APAC seemingly continued to drive nation-state-sponsored espionage across the region with some telecommunication companies continually targeted.

# APAC Notable Breaches

**Early 2016**

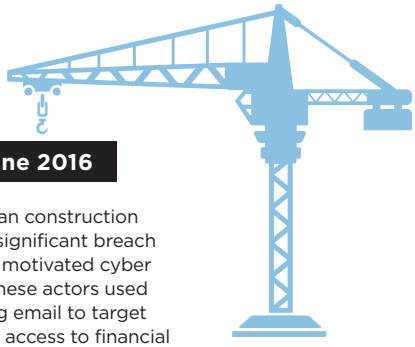
Threat actors targeted the banking networks of several financial institutions in South and Southeast Asia, including Bangladesh and Vietnam.

**March 2016**

The Commission on Elections in the Philippines suffered a breach involving the personal information of 70 million people. The breach included fingerprint data and passport information and occurred just weeks before a national election.

The website of Taiwan's Democratic Progressive Party (DPP) was compromised. The threat group was able to profile the systems used by visitors to the website. FireEye previously observed multiple China-based cyber espionage groups using the same tool. Its use against Taiwanese political targets suggests that the actors behind the identified campaign are supported by mainland Chinese sponsors.

**April 2016**



**June 2016**

A large Australian construction firm suffered a significant breach from financially motivated cyber threat actors. These actors used a spear-phishing email to target employees with access to financial systems. The attacker was able to steal $1.2 million AUD, but the total potential exposure was more than $2 million AUD. During the investigation, Mandiant uncovered a second attack group within the network. The second threat actor had been active since late 2015 and was focusing heavily on internal reconnaissance and ensuring persistent access. This second actor was utilizing malware with debug code written in the Russian language, but no attribution has been confirmed at this stage.

**$2**
BILLION USD

**July 2016**

The South Korean government accused cyber threat actors based in North Korea of releasing PII of customers of a large online shopping site. The organization only learned of the breach when they received a ransom demand of more than $2 billion USD.

**August 2016**

**90%**

Mandiant investigated a breach of a large subsidiary company that spread to the conglomerate parent company through lateral network accesses, and continued to compromise the parent company systems across several APAC countries. An interesting aspect of this case is that company turnover of approximately 90 percent was directly attributed to this compromise. After the Mandiant investigation, there were strong leads indicating involvement of a disgruntled former employee.

A large hospital was compromised using Andromeda malware and the Dark Comet remote administration tool. This compromise had been undetected for more than two years. The communication between the hospital environment and the cyber threat actors had been consistent via an internet facing server from within the hospital environment. While we have no attribution for this threat actor group, the use of this hospital by many tourists for medical procedures highlights the risk of cyber threat activity against health systems that hold personal health information across the globe.

**August 2016**

## Major Industries in the APAC Region Susceptible to Cyber Threats

| INDUSTRY | MOTIVATION | TARGET |
|---|---|---|
| **Construction and Engineering** | With engineering powerhouses such as Japan, South Korea, Hong Kong and Singapore, the region is home to innovations that are highly coveted by nations with less advanced engineering capabilities. Designs, blueprints, formulas and equipment specifications are typically prized by threat groups that steal data in support of domestic industries. | • Advanced materials<br>• Chemical engineering<br>• Industrial equipment<br>• Marine engineering<br>• Oil, gas and nuclear engineering |
| **Financial** | The Asian financial services sector has been a top target for cyber criminals and nation-state actors from around the world. Recent incidents involving banking network fraud highlight the risks to the region's banks, which may lack the rigorous security measures of their Western counterparts in securing key systems such as transactions, internal banking documents and mobile banking apps. In addition, China-based cyber threat groups have been interested in regional economic development to ensure access for Chinese firms to lucrative contracts. | • Credentials<br>• Payment cards<br>• Personally identifiable information (PII)<br>• Transactions |
| **Governments** | Regional governments and militaries are a continuous target of cyber espionage activity. Territorial disputes and evolving defense policies drive threat activity. We continue to observe China-based cyber threat groups targeting regional militaries — especially navies and coast guards — almost certainly because of Beijing's concerns about sovereignty in the region. We are seeing significant threat activity involving India, and we have seen ongoing targeting of the Indian government. | • Alliances<br>• Diplomacy<br>• Foreign policy<br>• Territorial disputes |
| **High Tech and Electronics** | Japan is host to the world's largest electronics industry. Innovative countries such as Japan that are strong in advanced technologies make these countries' private sectors a priority target for threat actors seeking access to intellectual property and competitive intelligence. Threat actors use this information to advance the capabilities of domestic companies and enable national champions to better compete in the global market. | • Advanced electronics<br>• Cloud and IT service providers<br>• Computing and hardware Semiconductors<br>• Software and gaming |

# Spotlight on EMEA Regional Trends

## VULNERABILITY OF PERSONAL IDENTIFIABLE INFORMATION

This region experienced several massive breaches that compromised the confidentiality of personal information, from legal documents and contact information to financial data. The leaks — whether for embarrassment or cyber crime — exposed how large and small companies must secure even basic information about clients.

## RUSSIAN CYBER THREAT ACTORS INFLUENCE ELECTIONS, TARGETING FOREIGN POLITICIANS

In 2016, FireEye observed Russian cyber threat groups with strong interest in the U.S. presidential election, and early signs that these groups may target various European elections. Germany announced that two political parties were hacked in 2016, a likely precursor to Russian operations to influence elections in the EU.

## RISE OF FINANCIAL CRIME

In 2016, FireEye has observed a rise in financial crime in Europe and the Middle East. Less security mature financial services organizations are a top target for sophisticated cyber criminals with experience attempting to breach some of the world's largest, most secure conglomerates. Cyber criminals have turned to leveraging vulnerable financial messaging systems in the region.

# EMEA Notable Breaches

**January 2016**

Bank networks suffered security breaches from multiple malicious actors from Asia, Eastern Europe and South America. The cyber criminals gained access to the interbanking network messaging environment to conduct illicit transactions.

**March 2016**

Mossack Fonseca, a law firm, suffered a massive breach of confidential client information. Although the law firm is located in Panama, the breach is notable in EMEA because it revealed private information about the financial dealings of politicians in Europe, the Middle East and around the world.

**1.5GB**

**April 2016**

Qatar National Bank, the Middle East's largest bank by assets, suffered a massive data breach involving a 1.5GB trove of leaked documents, including bank details, telephone numbers and dates of birth.[7]

**September 2016**

Two German political parties and the Bundestag reported that they were alleged victims of a targeted attack in an attempt to influence the upcoming election.[8]

**20,000**
**ACCOUNTS**

Tesco Bank, a Scotland-based bank, revealed money was stolen from 20,000 accounts and that the bank had detected suspicious activity in another 20,000 accounts.[9]

**November 2016**

7 http://www.reuters.com/article/us-qatar-ntl-bank-cyber-idUSKCN0XS16V
8 http://www.telegraph.co.uk/news/2016/09/21/russia-blamed-for-hacking-attack-on-german-mps/
9 http://www.databreachtoday.com/tesco-bank-confirms-massive-account-fraud-a-9501

## Major Industries in EMEA Susceptible to Cyber Threats

| INDUSTRY | MOTIVATION | TARGET |
|---|---|---|
| **Energy** | APT groups and other cyber threat actors extensively target the energy sector in the Middle East for cyber espionage and computer network attacks because of the sector's economic and strategic importance.<br><br>The European energy sector faces a high risk of intrusion by advanced threat actors seeking proprietary information to advance the capabilities of domestic companies. Additionally, cyber threat groups could target European industrial control systems for potentially disruptive or destructive operations. | • Oil and gas exploration and production<br>• Clean energy technology<br>Industrial control systems |
| **Government** | State and non-state cyber threat actors and cyber proxies commonly target governments and defense organizations in the region because of their contentious geopolitics and ongoing conflicts in the Middle East.<br><br>European governments are targeted by both state and non-state-sponsored actors. State-sponsored actors seek information for purposes that align with the states' interests, including intelligence on foreign affairs and diplomatic and defense networks. | • Foreign and defense ministries<br>• International operations<br>• Military alliances |
| **Financial services** | Advanced threat actors target the financial sector in Europe for economic gain. Notably, increased digitization of European financial institutions has rendered this sector a substantial target for financially-motivated cyber criminals.<br><br>The Middle East's growing financial services community – retail banks, investment banks, sovereign wealth funds – are a prime target for financially motivated threat actors from around the world. Regional banks have not made the same investments as Western financial institutions in cyber security, threat detection, and cyber threat intelligence. In addition, Iran-based threat actors likely view the region's financial industry as a top critical infrastructure target. | • Retail banks<br>• Investment banks<br>• Sovereign wealth Funds<br>• Credentials<br>• PCI, PII |
| **Telecommunications** | We have observed state-sponsored actors from China, Russia, and the West targeting EMEA telecommunications firms. Motivations include obtaining information on the European Union and collecting signals intelligence to benefit domestic military forces. | • Cellular and mobile carriers<br>• IT business service providers<br>• Telecommunications devices<br>• Satellite operators |

## How GDPR is Changing Business in EMEA

In 2016, European legislators finalized the General Data Protection Regulation (GDPR). Fully effective in May 2018, the GDPR brings major reform to European data protection laws, creating a new compliance regime for the handling of personal data relating to EU based citizens.

At the heart of the GDPR is an expectation that organizations adopt a proactive approach to information security governance. Measures should be implemented to effectively control the processing of EU citizens' personal data within their business in a manner that is fair and transparent to the individual, consistent with security best practices, and aligned to the statutory requirements of the legislation. Failure to comply with these rules creates a potentially significant exposure - fines for non-compliance may be levied at up to 4% of annual global group turnover.

The rigor with which the new regulation has been designed is intended to provide EU consumers with enhanced confidence that they can safely share information and interact within the global digital marketplace. Mandiant partnered with law firm DLA Piper UK for an assessment of the legal considerations of GDPR.

A key requirement of the new regulation is that organizations must notify local privacy regulators — and in some cases individuals — of cyber incidents involving the loss of personal data within 72 hours of having become aware of it. Of course awareness is subjective, it is a function of the complex interactions of an organization's incident response capabilities. Subsequently, the GDPR regulation goes as far as defining the window of notification, but not the trigger that starts the clock ticking. The onus for this falls to the respective processing organization, and thus it is prudent for affected organizations to incorporate an appropriate GDPR breach notification provision into their existing incident response plans.

In addition to the discussion of what constitutes awareness, there is a further need for more clarity around the exclusion of breaches which are "unlikely to result in a risk" to the individual. Both points are open to interpretation and it is expected that the precise scope and process for handling breach notifications will come in over the next 18 months as member state regulators expand on the GDPR with more detailed local guidance. The intent of the new regime is clear: the EU is moving towards, and will soon have, mandatory breach notification regulation with a strict requirement to notify regulators of personal data breaches.

Organizations should be preparing now, ensuring not only that they have an effective incident response plan in place to escalate, manage and report potential data breaches, but that this sits within a coherent governance framework that supports compliance with all other aspects of the GDPR. If a breach occurs, expect the regulator to look at the adequacy of the wider security measures adopted by the business, and the overall approach to information management and privacy compliance. Organizations that have a clear story to tell will be best placed to mitigate the risks of major fines. Those operating without a set of clearly defined incident response governance processes and accompanying appropriate security controls will come under direct scrutiny and could be subject to material exposure risk.

Given the magnitude of the potential fines it is advised that organizations take the time to not only assess how they monitor and protect EU citizens' personal data, but also undertake tabletop exercises to stress test their ability to effectively comply and respond to GDPR breach notification regulation requirements.


Legal considerations provided by DLA Piper UK

# Conclusion

We frequently say that organizations must always be adapting to an ever-changing and evolving threat landscape, and that continues to be true as we move deeper into 2017. Last year saw attackers greatly improve their level of sophistication, with some financial threat groups leaving very little evidence behind and making it extra challenging for analysts to investigate and remediate. Additionally, tactics such as calling targets directly show that threat actors are thinking outside the box and have become more brazen.

Security operations teams can now better identify, prioritize and address some of these threats with intelligence-led automation and threat hunting, but they cannot overlook the core fundamentals and best practices such as network segmentation and data segregation. Nowadays simply protecting critical business assets isn't good enough – some attackers are looking to disrupt business until a ransom is paid, so organizations must focus on securing what is needed for regular operations to continue.

Fortunately, we're seeing that organizations are becoming better at identifying breaches. The global median time from compromise to discovery has dropped significantly from from 146 days in 2015 to 99 days 2016, but it is still not good enough. As we noted in M-Trends 2016, a Mandiant Red Team can obtain access to domain administrator credentials within roughly three days of gaining initial access to an environment, so 99 days is still 96 days too long.

With media coverage of cyber attacks and compromised data at an all-time high, even people who don't work in the security industry know that breaches are inevitable. It is just as important to be ready and able to respond to an incident as it is to protect against threats. Organizations should consider partnering with organizations that specialize in defending against threats specific to the business.

For more information on FireEye, visit:
**www.FireEye.com**

**FireEye, Inc.**
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

**www.FireEye.com**

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.



FireEye