EXECUTIVE SUMMARY

In 2018, Gigamon Applied Threat Research (ATR) witnessed high-volume waves of low sophistication and criminally motivated attacks that damage enterprises and impose a significant cost to those involved. The primary intent of this report is to increase the understanding of how the most prolific malware of 2018 traversed enterprise networks without detection. It gives particular focus to the malware’s command and control (C2) and lateral movement, as these behaviors expose opportunities where security professionals can observe network traffic, discover these threats and reduce risk.

This report reveals the behaviors of the Emotet, LokiBot and TrickBot, and illustrates a successful methodology to combating cybersecurity threats:

- **Understand**: Security practitioners must first understand the methods that threat actors use and the context of the threat activity
- **Observe**: Security practitioners then need visibility of the potential threat activity across their enterprise (and possibly outside of their enterprise)
- **Discover**: Armed with 1) the knowledge of what to look for and 2) access to the malware’s field of play, security practitioners can rapidly detect threats, respond and continually improve their understanding

Putting this methodology into action allows CISOs and security practitioners to focus on the desired outcome: a shorter mean time to detection and response, a more mature security program and a balanced approach to mitigating risk to the enterprise.

This report’s secondary intent is to change the cybersecurity narrative. Increased knowledge will help CISOs, security professionals and the industry transition how we speak about cybersecurity:

<table>
<thead>
<tr>
<th>FROM</th>
<th>TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>We are losing the battle</td>
<td>We are a target. We must assume we have or will be breached</td>
</tr>
<tr>
<td>We don’t know what we don’t know</td>
<td>We learn how threats operate and utilize that knowledge to our advantage</td>
</tr>
<tr>
<td>We fear being a headline</td>
<td>We strategically and iteratively gain visibility in our enterprise</td>
</tr>
</tbody>
</table>
The initial trend report in August 2018 found that the most prevalent threats for the first half of 2018 were 1) LokiBot, 2) Pony and 3) TrickBot. LokiBot and TrickBot remained top threats in the second half of 2018 but were overtaken by Emotet.

Most notably, Emotet’s rapid increase began in early November 2018, which continued through late December 2018. During this time, Emotet campaigns appeared daily with different attachment hashes, different attachment filenames and different email subject lines. On or about 21 December 2018, Emotet went silent and remained silent through the first weeks of 2019.

Gigamon ATR observed Emotet exhibit significant experimentation in 2018. Emotet was originally the primary payload for a single threat group called Mealybug, now known to sell “delivery” by dropping other malware families, such as Gootkit (information stealer), Qakbot (worm, instalits backdoor), TrickBot (banking trojan), IcedID (banking trojan) and Zeus Panda (banking trojan) onto their Emotet compromised hosts. Emotet consistently used weaponized Microsoft Word documents to deliver its malicious payload and regularly changed its PowerShell script obfuscation.
**LokiBot**, the most prevalent crimeware in the first half of 2018, placed second in prevalence in the second half of 2018. LokiBot, which has targeted victims since 2015, is now commodity malware sold on various underground crimeware websites. It steals login credentials and other private data from infected machines and exfiltrates data using HTTP POST to C2 servers. This private data includes locally stored passwords, login credentials from several web browsers, admin tools such as PuTTY and a variety of cryptocurrency wallets.

**TrickBot** is a banking trojan, closely related to the banking trojan known as Dyre or Dyreza, with which it shares much of the underlying code and features. TrickBot has undergone periods of experimentation by the threat actors who control it, resulting in various deployment and obfuscation techniques. We observe TrickBot continuing to change its tactics. TrickBot remained a prevalent threat to enterprises throughout 2018.

Emotet, LokiBot and TrickBot may all be considered common, high-volume malware; however, all three are wildly successful in infiltrating enterprise networks and persisting. They pose significant damage potential and cost to organizations and take significant resources to respond to and remediate. The opportunity to learn from their success can lead security teams to a more mature and productive security strategy.
EMOTET

As the most prominent malware threat in the second half of 2018 and despite being well known by the security community, Emotet continues to infiltrate enterprises and evade security prevention tools and security professionals. While often crimeware is looked upon as a commodity threat, CISOs and security professionals should be concerned with Emotet’s ability to seek out and steal sensitive corporate information. Emotet’s ability to move laterally through your organization and spread other damaging malware, such as banking trojans and ransomware, should elevate concerns and mitigation efforts.

Due to Emotet’s polymorphic nature, it is difficult to detect by signatures alone, so organizations must be able to identify Emotet’s network communications behaviors to mitigate its rapid proliferation. Security teams should examine both north/south C2 traffic as well as east/west lateral communications.

Emotet Kill Chain
(TROJAN) PREVALENCE: 45.8%

**RECONNAISSANCE**
- Gathers information from public data sources to gather email addresses of specific and generic targets

**WEAPONIZATION**
- Builds out infrastructure, including previously compromised hosts and creates weaponized malicious documents for upcoming campaigns

**EXPLOITATION**
- After document/dropper is downloaded and opened, victim either clicks on a link or is tricked to “Enable” features inside the program to allow malicious code to execute
  - **Example:** Word documents droppers include Office 365 themed lure to convince victim to “Enable Editing” and “Enable Content” > allowing malicious macro to execute in the background
  - Uses native Windows scripting languages for initial code execution, often PowerShell
  - When dropper is executed, it uses a variety of host based evasion techniques to avoid sandboxing and command line detection

**COMMAND + CONTROL**
- C2 proxies typically previously compromised infrastructure – often appear to be residential ISPs
- Communicates to its’ command and control servers in a high volume manner, usually every 1-2 seconds. It will cycle through the C2 server list in a round robin fashion
- Communicates over the HTTP protocol with encrypted payloads inside of the protocol

**DELIVERY**
- Generic Spear Phishing > wide infection base in large scale campaigns
- Spear Phishing emails most prevalently include attachments/documents as droppers, but some contain links to malicious documents/droppers
- Emails often contain spoof “From” header as a lure
- Emails themes: Payroll | Banking | ACH | Invoices | Overdue Notice | IRS/Gov | US Holiday
- Little regard for prevention or detection

**INSTALLATION**
- Once active, the dropper will check in with a C2 to obtain the payload URL (often multiple external site locations for redundancy
- The dropper will also query an IP Checker site to obtain its infected machine’s Public IP address
- The dropper downloads the Emotet malware from payload URL
- Downloads typically via HTTP protocol & sometimes over a series of ports that are not default for HTTP, often with minimal HTTP headers as is being executed in a scripting language
- Often the payload URLs are tied to low reputation residential ISPs

**ACTIONS ON OBJECTIVES**
- Primary: Steals sensitive corporate information and credentials
- Secondary: Proliferates itself and other threats/malware throughout your organization
- Lateral: Brute force with stolen credentials

*Figure 4: Emotet kill chain activity*
Emotet’s Malicious Objectives

Emotet serves many objectives: Information stealer, credential theft, spam and malware distribution are amongst its top offenses. As Emotet persists on its victim machines, it continues to pull down modules that execute independently to carry out the threat actor’s objective. These include:

- **Information theft**: Steals information from various programs on the machine that might provide sensitive financial information.
- **Credential theft**: Steals passwords from multiple sources on the machine.² The blatant use of public freeware utilities by the actor continues the common theme of using off-the-shelf methods to accomplish their objectives with as little work as needed. The threat actor takes minimal effort to evade or disguise the capabilities.
  - NetPass.exe (NirSoft) recovers network passwords for currently logged on user
  - Outlook Scraper scrapes names and emails from victims' Microsoft Outlook inbox
  - WebBrowserPassView (NirSoft) is a password recovery tool for modern browsers
  - Mail PassView (NirSoft) is a password recovery tool for several popular mail clients
- **Spam**: Emotet will utilize stolen address book details to send additional spam and propagate using its’ standard campaign methods.
- **Malware distribution**: Once Emotet persists on a victim machine, it often provides access to other malware families such as TrickBot, Qakbot, ICEID and GootKit.

Emotet’s C2 Activity

Emotet’s malware communicates using the HTTP protocol to egress a network by appearing as normal browser activity. However, the malware uses encrypted payloads inside the HTTP protocol to allow the actors to evade direct network monitoring of their communication activity. Hardcoded within the payloads are the ever changing C2 lists and necessary ports to avoid detection and provide redundancy. Oddly enough, Emotet does communicate over ports such as 22, 8080 and 443 where unencrypted HTTP transmissions are not common and yet still often evades detection.

Emotet’s C2 behavior is noisy, with active communication attempts in the order of every one to two seconds to varying C2 server URLs. Compromised host machines will cycle through C2 server lists in a round-robin fashion. Most often, Emotet uses C2 servers within Residential ISP IP blocks. Despite what seems like clear C2 communications to identify, enterprises that do not have pervasive network visibility and tools to identify these behaviors are left blind to Emotet’s north/south communications.

Emotet’s Lateral Activity

While identifying a single victim machine with Emotet is important, Emotet’s ability to spread laterally throughout the network creates a challenge to identify its full presence and eradicate Emotet from an enterprise’s network.

Emotet achieves its primary lateral movement activity by using the stolen passwords it has accumulated to brute-force internal network resources. Emotet will first enumerate the network to identify systems with SMB (server message block) open and accessible. It will then attempt to authenticate to the discovered systems using the credentials stolen by Emotet’s credential theft module. If successful, the malware will copy over a malicious tool and install it as a service on the remote host. The service, upon launching, will write Emotet to disk and continue with the standard infection process. These secondary infections will continue to carry out Emotet’s objectives as well as spread other threats.

In the above scenario, security professionals with pervasive network visibility to east/west traffic would be able to observe a one-to-many pattern of attempted authentications with frequent failures and occasional successful authentications, followed by services being created over the network.
LOKIBOT

LokiBot’s prevalence through all of 2018 illustrates that simple capabilities can enable threats to be quite successful at infiltrating enterprises. On the surface, LokiBot appears to be a run-of-the-mill information stealer; however, the fact that its code is now open-sourced raises a much greater risk to enterprises. LokiBot has proven its ability to successfully exploit and install, earning attention from other threat groups who can use LokiBot to get in and then carry out their own objectives.

Once installed, the LokiBot code enables an opportunistic actor to easily download and execute other malicious code. The following reports have shown other actors using LokiBot to their advantage. Palo Alto Networks Unit 42 reported that the Nigerian threat actors notorious for their Nigerian Prince scam have evolved their efforts into business email compromise (tricking recipients into wiring money to phony companies or real estate escrow firms) scams using LokiBot, along with other commodity malware. Attackers tied to the ransomware outbreak in the Ukraine targeting major banks, utilities and telecommunication companies also installed a variant of LokiBot to not only make the compromised machine inoperable, but to also steal credentials and information.

Lokibot Kill Chain
(TROJAN) PREVALENCE: 11.8%

- RECONNAISSANCE
  - Gathers information from public data sources to gather email addresses of specific and generic targets

- WEAPONIZATION
  - Builds out infrastructure, including previously compromised hosts, and creates weaponized malicious documents for upcoming campaigns

- EXPLOITATION
  - If a ZIP or packaged format of some kind is used, the user will first open the package to access the dropper
  - The actors have been observed using various methods to gain execution with the included weaponized document:
    - User driven methods such as macros
    - Widely known vulnerabilities in common applications (CVEs 2017-0199, 2017-8570, 2018-0802, 2017-11882): This results in a low-interaction method of executing code

- INSTALLATION
  - After code is executed, the full Lokibot trojan will be downloaded and installed on the host. This installation has been observed occurring over plain text HTTP as well as using SSL/TLS

- COMMAND + CONTROL
  - C2 infrastructure diverse, including shared hosting environments and previously compromised nodes
  - Communicates over plain text HTTP to C2 with custom pre-defined ‘structure’ in HTTP payload
  - Infection traffic is periodic in nature and volume depends on the data being exfiltrated
  - C2 exchange protocol includes protections against researchers attempt to manually poke at the infrastructure through verifying a cryptographic hash of the header information in the exchange

- DELIVERY
  - Generic Spear Phishing to create wide infection base in large scale campaigns
  - Spear Phishing emails typically include attachments/documents as droppers that are either office documents or ‘packaged formats such as zip, likely to evade automated analysis
  - Emails tend to have varying themes: Notifications from well-known companies | Financially motivated themes with calls to action | Fake orders or offers

- ACTIONS ON OBJECTIVES
  - Primary: Steals sensitive corporate information & credentials
  - Secondary: Keylogger
  - Lateral: None

Figure 5: LokiBot kill chain activity
LokiBot’s Malicious Objectives

LokiBot by itself has three primary objectives: information stealer, credential theft and keylogger. LokiBot includes functionality to carry out several different post-exploitation actions on the target host. Highlights include:

- Information theft from more than 100 applications
- Credential theft from the Microsoft Windows Credential Manager
- Download EXE and execute
- Download DLL and load
- Keylogger

LokiBot’s C2 Activity

LokiBot’s C2 capabilities are effective by using a diverse mix of C2 infrastructure (C2 Proxies) that include both shared hosting environments (rented infrastructure), as well as the use of previously compromised nodes. LokiBot uses plaintext HTTP to communicate to the C2 servers and a custom pre-defined structure in the HTTP payload.

- A series of different requests contain various pieces of information from the host:
  - Application data
  - Decrypted credentials
  - A request for C2 commands
  - System information

NOTE: This payload may include compression but often contains recognizable details of infection, such as the computer name or unique BOT ID. The user-agent used in these requests are unique.

C2 traffic from infected systems is periodic in nature and volume depends on the data being exfiltrated.

The C2 exchange protocol includes protections against researchers attempt to manually poke at the infrastructure through verifying a cryptographic hash of the header information in the exchange.

Periodicity in C2 communications is simple behavior to be able to identify compromised systems, but most organizations lack the network visibility or analysis capabilities to quickly detect the presence of these behaviors.

LokiBot’s Lateral Activity

To date, Gigamon ATR has not observed lateral spread or attempts to extract information from peripheral devices from the compromised host by LokiBot.
TRICKBOT

TrickBot pulled in front of Pony in the second half of 2018 to come in as the third-most prevalent crimeware. It uses many of the same techniques used by Emotet. Since its inception in 2016, TrickBot continues to evolve and counteract defensive measures of the security community. As enumerated by Malwarebytes Labs, TrickBot has varying modules responsible for persistence, propagation, credential stealing and encryption. TrickBot is efficient and pervasive, using existing infected machines within an organization to re-infect previously cleaned machines when they rejoin the network.

Figure 6: TrickBot Kill Chain Activity

(TROJAN) PREVALENCE: 10.5%

RECONNAISSANCE
- Gathers information from public data sources to gather email addresses of specific and generic targets

WEAPONIZATION
- Builds out infrastructure, including previously compromised hosts, and creates weaponized malicious documents for upcoming campaigns

DELIVERY
- Generic Spear Phishing to create wide infection base in large scale campaigns
- Observed being deployed through Emotet as a secondary infection
- Spear phishing emails typically contain attachments that are XLS or DOC files with malicious macros embedded in them
- Emails range in themes and sophistication
- Little regard for prevention or detection
- Possible campaign based geographic targeting

EXPLOITATION
- Often after document/dropper is downloaded and opened, victim is tricked to “enable” features inside the program to allow for malicious code execution
- Trickbot has been noted going through extraordinary measures to evade sandboxing and implementing execution triggers to prevent analysis. Examples include the malware only executing upon an image zoom event in Microsoft word

INSTALLATION
- The malicious macros executes PowerShell code to stage the full Trickbot payload
- Multiple HTTP requests may be performed checking in to various command and control servers
- The HTTP requests are made directly to the server IPs resulting in Host headers of the IP addresses
- During installation, Trickbot has been observed checking its’ public IP address by making a request to various external public services

COMMAND + CONTROL
- C2 proxies typically previously compromised infrastructure – often appear to be residential ISPs
- Communicates to its’ command and control servers in a high volume manner, usually every 1-2 seconds. It will cycle through the command and control server list in a round robin fashion
- Communicates over the HTTP protocol with encrypted payloads inside of the protocol

ACTIONs ON OBJECTIVES
- Primary: Steals sensitive corporate information & credentials
- Secondary: Email harvesting for later spam use
- NOTE: Includes many other capabilities
- Later: Brute forcing using stolen credentials and at times using the ETERNALBLUE Exploit
TrickBot’s Malicious Objectives

TrickBot includes the ability to push down modules that execute independently of the primary RAT (remote access Trojan). Several different modules have been observed associated with TrickBot infections:

- **Credential theft**: Steals passwords from the infected machine. It leverages a custom capability dubbed pwgrab32 to steal credentials from browsers (including autofill data), and other clients on the host, including Outlook, FileZilla and WinSCP. Additionally, there has been a module observed that leverages the popular open-source hacking tool mimikatz to steal windows credentials.
- **Email harvesting**: TrickBot scans the drive for the ability to steal all email addresses that can be later used in the spam module.
- **Point-of-sale (POS) reconnaissance**: This very recent new feature tries to identify if the infected system is a POS device or part of a POS network of some kind. At this time it is unknown how the information will be used.
- **Proxy module**: TrickBot proxies external network traffic through victims. Frequently used in ad-fraud scenarios.
- **Spam module**: TrickBot uses stolen contacts to send additional spam messages.

TrickBot’s C2 Activity

TrickBot’s C2 activity exhibits little regard for stealth or evasion, thumbing its nose at many enterprises’ lack of network detection capabilities.

The C2 activity has the following communication behaviors:

- **Volume**: TrickBot communicates to its servers in a high-volume manner, most often to compromised home routers in residential broadband networks acting as C2 proxies.
- **Encrypted communication**: TrickBot’s C2 operates primarily over SSL/TLS on ports 447 and 449. The SSL certificates are self-signed, non-valid SSL certificates. The self-signed properties match the defaults of common servers.
- **HTTP requests**:
  - Within the SSL activity, the requests do not use hostnames (only IPs), with regular GET requests on predictable paths on a periodic interval. Further, the user-agent is consistent and unique. SSL interception would significantly enable detection of this activity. During C2 activity, there will occasionally be plaintext HTTP communications as well.
  - HTTP POST messages contain system information in plain text, including exfiltrated details. Example data that occasionally is exfiltrated over HTTP includes process lists, system information, passwords and credit card details.
- **Additional malware**: Staging of additional malware is performed using a GET request to a URI that attempts to disguise the download as an image file with names like table.png, radiance.png and toler.png. In reality, the downloads are Windows executable files that are modules of TrickBot.

Like Emotet, TrickBot infections are relatively easy to discover with comprehensive network visibility and examination of network behaviors.

TrickBot’s Lateral Activity

TrickBot, like Emotet, has very automated lateral movement. TrickBot uses brute force password lists in combination with passwords stolen from the infected devices to move between networked windows machines. TrickBot has been observed using the EternalBlue exploit as well, but it is not a standard element used in all campaigns. Security professionals can look for one-to-many failed authentication attempts to uncover the lateral movement of TrickBot.

**EternalBlue**

The EternalBlue exploit was created by the NSA and was leaked April 14, 2017, by the Shadow Brokers hacker group. Subsequently the threat actor community has improved upon its ability on different windows platforms and its overall reliability.
DETECTION AND MITIGATION ACTIONS

Gigamon ATR recommends that detection and mitigation strategies should take into account adversary behavior across the kill chain and leverage comprehensive network visibility to minimize mean time to detect and respond. Gigamon ATR observed the below behavioral network communication characteristics that can be leveraged by security professionals to rapidly detect and mitigate Emotet, TrickBot and LokiBot based on the later stages of the kill chain. These indicators and detection strategies derived from researching these three threats may apply generically to detect threat activity from other actors and malware.

Emotet Behaviors

Installation:
- **Executables retrieved with minimal HTTP headers**: It is common among crimeware families to stage follow-on malware using barebones scripting-language capabilities native in the operating system. The programmatic retrieval of binaries over plaintext looks significantly different than normal web browsing behavior and can be detected.
- **Public IP address check**: While not unique to malware, the observation of a public IP check clustered with other suspicious behavior could potentially elevate the confidence of interest.

Command and Control:
- **IoCs**: Signature-based detection of known Emotet indicators:
  - Known identified C2 proxies
  - Format and specific indicators associated with network traffic
- **HTTP communications over non-standard ports**: Emotet communicates out over ports generally reserved for other protocols and ports.
- **High volume and periodic communication to low reputation host**: The regular communication to foreign residential ISPs on common ports used by internet services.

Actions on Objectives and Lateral Movement:
- **One-to-many authentication failures**: Authentication failures — identifying credential brute forcing.
- **Service creation with suspicious or unknown binaries**: Remote service creation should be performed only by administrators from authorized locations. Unknown binaries being executed using remote services from unauthorized hosts present a unique detection opportunity.

LokiBot Behaviors

Installation:
- **Minimal**: LokiBot’s simplicity leaves very little to detect on installation.

Command and Control:
- **IoCs**: Signature-based detection of known LokiBot indicators. There are numerous publicly available IDS signatures, as well as easily predictable patterns that can be used for metadata-based detection.

Lateral Movement:
- **Not applicable**
TrickBot Behaviors

Installation:
  • **Public IP address check:** While not unique to malware, the observation of a public IP check clustered with other suspicious behavior elevates confidence of an infection.
  • **Executable downloaded from a Dotted Quad:** During the staging of modules, the executables are downloaded with no hostname (IP address as host header).
  • **Executable downloaded as an image:** During the staging of modules, the executables are downloaded with image based URIs.

Command and Control:
  • **IoCs:** Signature-based detection of known TrickBot indicators:
    – Known identified C2 proxies
    – SSL certificate patterns used by the trojan
    – The format and specific indicators involved with POST traffic with exfiltrated data
  • **Behavior:** High volume and periodic communication to a low-reputation host. The regular communication to foreign residential ISPs on common ports used by internet services.

Lateral Movement:
  • **One-to-many authentication failures:** Authentication failures — identifying credential brute forcing.
  • **One-to-many exploitation behavior:** Exploitation may employ attempts and successes from unauthorized source using publicly available signatures for EternalBlue.
CONCLUSION

As illustrated throughout this report, non-targeted yet high-volume criminally motivated attacks can move throughout your network without your knowledge and cause significant damage and cost to enterprises. To shift the balance from the attackers to the defenders, we must:

1. Be dedicated to studying the behavior of successful threats
2. Apply what we have learned to create a robust set of indicators and detection mechanisms
3. Leverage these new indicators and detection mechanisms across comprehensive network visibility
4. Use our gained insight to properly respond to reduce risk

Gigamon ATR’s intent for this report is to assist analysts and responders with this first step by sharing our knowledge how Emotet, LokiBot and TrickBot operate.

Then when CISOs and security practitioners apply the foundational methodology of UNDERSTAND | OBSERVE | DISCOVER they will achieve:

- Shorter mean time to detection and response
- A more mature security program and posture
- A balanced approach to mitigating risk the enterprise.

At that point we can change the cybersecurity narrative to one of winning the battle through knowledge, a mechanism for rapid adaptation and improved detection and response.
ABOUT GIGAMON APPLIED THREAT RESEARCH (ATR)

MISSION

Gigamon ATR serves to dismantle the ability of an adversary to impact our customers. Our team of expert security researchers, engineers and analysts focuses on continuous research of threat actors and emerging attack techniques while building detection and investigation capabilities leveraging the Gigamon Insight network telemetry and intelligence datasets.

<table>
<thead>
<tr>
<th>THREAT INTELLIGENCE</th>
<th>DETECTION ENGINEERING</th>
<th>SECURITY ENGINEERING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research threats to inform detection engineering efforts</td>
<td>Research, build, and maintain high quality detection capabilities for Gigamon Insight</td>
<td>Prototype and validate future functionality for detection and investigation capabilities</td>
</tr>
</tbody>
</table>

ATR was established on the principals of building a team and a culture around understanding adversaries and engineering innovative capabilities to counter their activities. Equally important was the ability to funnel this innovation directly into our product, Gigamon Insight, and help empower our customers, while continually raising the bar for attackers.

ATR actively hunts for threats and studies their behavior in the wild and throughout customer environments. They develop detection capabilities and conduct security research to advance the state of detection with curated rule sets —complete with full rule descriptions, justifications and logic — to help protect Gigamon Insight customer environments.

As experienced security researchers and responders, ATR lives by the Understand | Observe | Discover methodology to threat response.

- **Understand**: ATR is constantly monitoring public and private data sources, including anonymized customer data in Gigamon Insight for threat behavior. Upon discovery, the behavior is analyzed and disseminated as intelligence internally.
- **Observe**: Gigamon customers leverage Gigamon Insight to gain pervasive network visibility internally and externally. Gigamon ATR leverages its knowledge of threat behaviors to steer development efforts to continually observe threats.
- **Discover**: ATR uses internal intelligence to engineer detection capabilities, including a curated rule set, into Gigamon Insight. This is performed continuously on the backend delivering instant value to Insight customers.

Gigamon Insight

Gigamon Insight is the pioneer in cloud-based network threat detection and response (NDR).

Powered by Gigamon ATR, Insight provides rapid detection of threat activity. It enables incident responders to investigate and validate other identified suspicious behavior. Insight serves as a hunting platform for advanced risks through real-time and historical view of all network activity. Insight provides full visibility across physical, virtual, public and private clouds to eliminate blind spots. Insight directs fast and effective response to active threats.

The Insight functionality minimizes mean-time-to-detection and response (MTTD/MTTR), while its SaaS delivery model reduces complexity and slashes Total Cost of Ownership (TCO).

**Gigamon Insight — Accelerate Threat Response**: Rapidly hunt, detect, investigate and respond with confidence to threats without wasting time aggregating contextual evidence or the headache of tool maintenance and cost.
APPENDIX: METHODOLOGY AND DATA

Methodology

To better understand patterns and changes to campaign volume and detection, the Gigamon ATR collected a sample of malicious email attachments delivered to our customers during the second half of 2018 (2H 2018). This practice of collection and analysis helps validate our observations and suspicions about threat-actor behavior patterns, as well as observe campaign beginnings, periods of possible experimentation and occasionally campaign ends. Additionally, this collection and analysis cycle assists the Gigamon ATR in staying ahead of evolving campaigns for detection and investigation purposes.

Data

Our dataset consists of samples attached to malicious spam attacks from July through December of 2018 with the distribution of threats shown in Figure 7. The file type distribution (Figure 8) demonstrates that the malspam attachments are primarily documents, straight executables and archives, with a few outliers such as an internet query file (IQY).

Mean anti-virus detection history for all samples is plotted in Figure 9. Instead of averaging the samples and fitting the average, we chose to individually fit each sample and average the fitted curves because each sample has a different amount of measurements and the measurements were all taken at varying times in the sample lifetime. This avoids over- and under-representing samples based upon how many times they were scanned.

Ideally, we would see high initial detection rates, and for those that are not well detected, sharply increasing detection rates as security vendors adapt to the threat. Visually, up and left is better.

Figure 7: Threat family distribution 2H 2018 (Insight customers)

Figure 8: Filetype distribution for threats observed 2H 2018 (Insight customers)

Figure 9: Detection percentage over time for observed samples 2H 2018 (Insight customers)
We can see that, on average, 37.9 percent of anti-virus products detected samples on the first day, with 51.3 percent detecting samples by the end of the first week. Some attacks are more challenging than others to analyze in isolation. For example, second or later stages in attacks may require code or data, like encryption keys, from earlier stages to run. However, this dataset contains exclusively first stage malware. While not without its own challenges (e.g., legacy or uncommon file formats, uncommon features, obfuscations and evasions, remotely included data), a 37.9 percent initial detection rate is concerning.

In comparing data from 1H and 2H 2018, we observed the following trends:

- 9.3 percent increase on first day detections from 1H 2018 to 2H 2018
- 7.4 percent increase after one week for detections from 1H 2018 to 2H 2018
- Increase in proportion of Microsoft Word Documents and Excel Sheets in 2H 2018
- Decrease in proportion of archives and DOS Executables in 2H 2018
- Increase in proportion of Emotet samples
- Decrease in proportion of LokiBot samples
- Proportion of TrickBot samples stayed roughly the same

**Emotet**

We witnessed only Microsoft Word Documents as the first stage of Emotet (Figure 10). Thus, compared to the other most prevalent families, Emotet delivered the least diverse set of filetypes. More preventative-based solutions detect Emotet samples than the mean malspam sample, even on the first day of an observed new sample (Figure 11).
LokiBot

Like 1H 2018, LokiBot delivers the most diverse set of filetypes in its initial attachments (Figure 12). Despite this, it is detected both initially and during each subsequent campaign by more preventative products than the baseline (Figure 13). We find this true for the majority of the most prevalent families, which makes sense under the intuition that the loudest campaigns will be caught, shared and tracked more frequently.

![LokiBot Filetypes](image1)

Figure 12: LokiBot filetypes observed 2H 2018 (Insight customers)

![LokiBot Detection Percentage Over Time](image2)

Figure 13: Detection percentage over time for observed LokiBot samples 2H 2018 (Insight customers)

TrickBot

TrickBot comes almost exclusively in various common Microsoft Office document formats (Figure 14). Although detection rates on the first day of submission slightly outperform those of the mean, they begin a trend of underperformance after the first few days (Figure 15).

![TrickBot Filetypes](image3)

Figure 14: TrickBot filetypes observed 2H 2018 (Insight customers)

![Trickbot Detection Percentage Over Time](image4)

Figure 15: Detection percentage over time for observed TrickBot samples 2H 2018 (Insight customers)
RESOURCES


