

# *A Look Inside Financially Motivated Attacks and the Active FIN8 Threat Group.*

**SURVIVING THE ONSLAUGHT OF FINANCIALLY  
MOTIVATED THREATS.**

---

## CONTENT

<b>Executive Summary</b> .....	3
<b>The Anatomy of the Financial Threat Actor</b> .....	4
The details .....	5
Who do they target .....	6
What do they target? What tools do they use? .....	7
How do they operate? .....	8
<b>Case Study: FIN8</b> .....	10
An evolving actor .....	10
FIN8's customization .....	10
Additional component details .....	11
<i>Interactive reverse shell – BADHATCH</i> .....	11
<i>Persistent memory implant – ShellTea.B</i> .....	11
<i>POS memory scraper – PoSlurp.B</i> .....	13
Conforming to trends .....	14
<b>Summary: Key Takeaways</b> .....	15
<b>About Gigamon ATR</b> .....	16

As experienced security researchers and responders, Gigamon ATR lives by the **Understand, Observe, Discover** approach to threat response.

---

### UNDERSTAND

ATR is constantly monitoring public and private data sources, including customer data in Insight for threat behavior. Upon discovery, the behavior is analyzed and disseminated as intelligence internally.

---

### OBSERVE

Gigamon customers leverage Insight to gain pervasive network visibility internally and externally. Gigamon's ATR leverages its' knowledge of threat behaviors to steer development efforts to continually observe threats.

---

### DISCOVER

ATR leverages 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.

## Executive Summary

Throughout the last several years, Gigamon Applied Threat Research (ATR) has observed an onslaught of campaigns by various organized and persistent financially motivated threat groups with a singular purpose: profit. This should be no surprise, as the industry at large has seen a continuing increase in breaches associated with these threat groups. Threat actors engage victims with speed and ferocity, often using tailored capabilities that enable them to quickly (and quietly) accomplish their objectives. Statistics gathered across the industry highlight an alarming trend: More than half of all exposed breaches took months or longer to discover and additional days or weeks to contain. It is difficult to isolate the variables that cause such a delayed timeline, but it is clear that improvement is necessary.

The financially motivated threat groups Gigamon ATR has observed and those seen across the industry at large are far from being flawless. Their operational and technical imperfections provide unique opportunities for discovery and detection, provided that an organization is equipped appropriately and understands the threats it faces.

This report provides a detailed view into the inner workings of financially motivated (that is, for-profit) threat actor groups, including their preferred tactics and tools. By exposing the anatomy of these attacks, we hope to empower your teams with the knowledge needed to broadly improve visibility into these threats and expedite rapid detection and response.

In addition, this report highlights specific threats-at-large that pose heightened risk to organizations. To that end, we revisit FIN8, a financially motivated threat group that falls into this category. The group continues to operate and evolve in subtle ways to meet its objectives, and as such, is highlighted within this report.



Percentage of breaches that were financially motivated<sup>1</sup>



Percentage of breaches conducted by organized criminal groups<sup>1</sup>



Percentage of breaches that took months or longer to discover<sup>1</sup>

# The Anatomy of the Financial Threat Actor

It is critical that security professionals ditch the far-fetched imagery often portrayed when discussing threats; for example, shadowy creatures of the night that use sorcery to steal your most prized possessions. The reality is that threat actors, especially the organized groups that seek financial gain, are humans operating a business, and a profitable one at that. As an example, in at least one case, the cybercrime group FIN7 was rumored to have stolen more than 15 million credit cards from 3,600 businesses, estimated to generate billions in profit.<sup>2</sup>

Also, an important distinction needs to be made: The name “financial threat actor” refers to the attacker’s intent (in this case, profit), not the target of the attack (which could be anyone, not necessarily financial organizations). For threat actors who are motivated by profit, targets can be diverse. However, financial threat actors who target their attacks usually focus on the largest or potentially most profitable institutions, which include, but are not limited to, institutions in the financial, retail, food and hospitality sectors.

As proprietors of a profitable business, financial threat actors are both motivated and constrained by the same forces that affect any business: initial investment, resiliency, risk and reward.

## INVESTMENT

Financial threat actors must invest in intellectual property (e.g., malware, command and control (C2) infrastructure, intelligence) and must safeguard their investments at all costs. As such, emphasis is placed on thwarting analysis efforts with obfuscation and other techniques.

## RESILIENCY

Financial threat actors and groups invest heavily in their business, both monetarily and with time and effort. They must also ensure that their business is not destroyed once specific touch-points are discovered. Hence, these groups tend to have a focus on resiliency and are persistent threats that are not removed easily.

## RISK + REWARD

Financial threat actors weigh risk and reward heavily, more so than opportunistic threat actors (stealing the crown jewels, after all, is not easily done, and the penalties for being caught are high). As such, these groups often utilize different methodologies for attack. Targeted financial threat groups craft custom tools; broad or opportunistic financial threat actors take the approach of opportunity, using off-the-shelf tools (often for sale across various sites).

There is a wide spectrum of attack methodologies across threat groups labeled in public reporting as financially motivated. These range from groups like FireEye’s FIN\* actors, commonly associated with highly targeted attacks on organizations, to groups like Mealybug<sup>3</sup> or SamSam,<sup>4</sup> who are associated with more broadly targeted or opportunistic attacks.

It is important to note that classification of threat groups may aid teams in prioritization and categorization of detection and alerts across tools deployed within an organization, but it does little to truly describe what damage a threat actor or group can cause. A broad attack can become a targeted one, and vice-versa, according to the group’s motivation at that point in time. Attacks

(particularly those with financial motivation) are dynamic, ever evolving and always potentially devastating. Hence, with financial threats, security teams mustn't fall into the trap of complacency, equating categorization with level of danger. In practice, teams must be quick to identify any traces of evidence linked to these groups within their organizational networks and respond accordingly, as financial threat actors are all extremely dangerous.

## THE DETAILS

In this section, Gigamon ATR analyzes the who, what and how of these groups at a macro level utilizing ATT&CK data, public reporting and first-party intelligence derived from working with our incident response partners to combat these threat actors. With this data, Gigamon ATR is able to assess common methodology across a subset of actors with the intention of identifying key takeaways and providing recommendations to security professionals.

### FINANCIAL THREAT ACTORS:

Target all groups, utilizing all tools and methodologies



---

## WHO DO THEY TARGET?

As alluded to earlier, it is easy to assume that financially motivated actors primarily target a single industry or vertical, but this over-simplification is a dangerous one. In reality, these actors seek to gain access to any industry and vertical that regularly transacts in information of value. Much of the public reporting indicates that prominent target verticals for these actors include hospitality, food, retail and entertainment, all of which regularly conduct transactions using payment card data through point-of-sale (POS) terminals. Consequently, security teams have placed emphasis on securing these systems, with some degree of success. However, though these groups have primarily targeted POS systems, their target objectives dynamically change according to difficulties encountered.

Within the last year, there has been an increase in public reporting indicating a shift to alternative threat actor objectives and, therefore, security professionals should not limit the scope of their understanding of these groups to only POS compromise. It is critical to understand, especially with the proliferation of technology to mitigate against POS scraping, that these groups can and have evolved to continue to make money in other ways. Other monetization schemes include the theft of private information for trading and extortion, ransomware, access to gift card mechanisms and injection of web skimmers into online stores, among several less prominent tangential mechanisms.<sup>5</sup>

Monetization schemes also evolve. As an example, alternative monetization methodologies were observed with the deployment of Ryuk and LockerGoga ransomware, which were possibly associated with FIN6 through 2018 and 2019.<sup>6</sup> These lesser-known monetization methods are becoming more prevalent as defenses evolve and intelligence shapes defensive technology and research to combat attackers.

Credit card transactions are targeted primarily through institutions operating on information of value



---

## WHAT DO THEY TARGET? WHAT TOOLS DO THEY USE?

Across the snapshot of financially motivated threat actors, and primarily in our first-hand interactions with these actors, we observe a number of high-level themes regarding what these groups target (insofar as assets), what architectures are more vulnerable and what tools are used.



### COMMON TECHNIQUES: POS IS STILL A TARGET

While there is more reporting starting to emerge on alternate monetization techniques, there is a steady targeting of companies for the purpose of gaining access to POS devices.



### UNIQUE ARCHITECTURE CONSIDERATIONS

POS breaches often occur in hub-and-spoke networks. Numerous retail branches and individual stores contain POS systems, and sometimes controllers, which link back to the corporate environment. In some cases, stores have internet access and employee systems that present an entry point for attackers looking to setup a foothold. This unique architecture presents a perfect venue for attackers.



### FREQUENT PUBLIC TOOL/TRADECRAFT USE

Across many of the financially motivated threat groups, we observe the use of off-the-shelf offensive toolsets such as Empire, Metasploit and Cobalt Strike. We have also seen the use of pirated licensed commercial tools that contain indicators of nefarious use. In addition to these remote access Trojans (RATs), threat actors use public tradecraft from offensive security researchers verbatim (with little to no modification of underlying code or example commands). Public tools and tradecraft present many benefits to a threat actor (e.g., development and maintenance savings) and allow them to rapidly bootstrap programs.



### RAPID ACTIONS INVOLVING OBJECTIVES

While the dwell time in some of these breaches is extensive, in many of the observed cases, actions taken toward objectives were en masse and swift, seemingly attempting to get as much value from the breach as quickly as possible. This rapid and mass action introduces a useful detection heuristic, but also means that it is occurring too late within the kill chain<sup>15</sup> for detection. Detection of the different pre-strike actions are more important to prioritize in the case of financial threat groups.



### INFRASTRUCTURE REUSE

On multiple occasions, Gigamon ATR has observed firsthand that attackers reuse their infrastructure between campaigns. This allows for the use of atomic indicator matching with context, resulting in early detection.

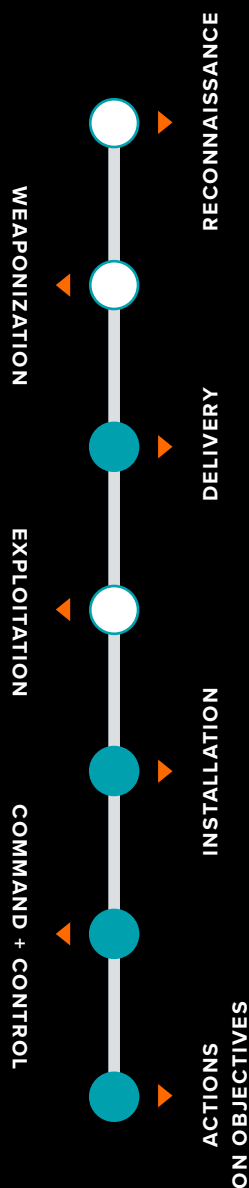


### REDUNDANCY AND REINFECTION

Gigamon ATR has also observed financial threat actors deploying multiple toolsets and establishing secondary or even tertiary access to victim environments. This is a method of maintaining a strong foothold in the case of response actions. In some cases, we have also observed actors re-infecting victims after failed containment actions, primarily via credential reuse or through alternate backdoors.



## KILL CHAIN



## HOW DO THEY OPERATE?

In order to empower security teams against these threats, observation and discovery is critical; knowing how the actors operate is crucial toward this end. ATT&CK is a framework developed by MITRE to characterize and model tactics and techniques utilized by threat actors. In the framework, MITRE leverages open source reporting to directly tie identified threat groups and malware families to known techniques.<sup>7</sup>

ATT&CK does have its drawbacks. Open source reporting, by its very nature, represents a subset of truth, which results in a bias in its findings. Gigamon ATR utilizes ATT&CK to cross-reference findings and identify patterns of behavior most closely associated with the identified threat group. The framework acts as a filter of sorts, allowing research groups to narrow search areas and concentrate efforts in specific directions.<sup>8</sup>


Looking across a subset of known financially motivated threat groups identified in the ATT&CK dataset, Gigamon ATR conducted analysis to identify the most common techniques used by the subset of actors. Gigamon ATR specifically identified aspects of the adversary lifecycle that involve network communications and identified the following common techniques.

- DELIVERY** Preferred methods: spearphishing with links or spearphishing with attachments  
Preferred targets: customer service and back office corporate personnel
- INSTALLATION** Preferred methods: user execution  
Preferred delivery: embedded file within a document or a macro-laden document
- COMMAND + CONTROL** Preferred communication methods: standard application layer protocols (HTTP, TLS, SSH or DNS), commonly used ports (80,443) and remote access tools (e.g., Microsoft Remote Desktop)  
Notable characteristics: use of self-signed certificates or ones provided by low-cost issuers

### *Actions on Objectives*

- ENUMERATION** Goals: remote system discovery and network service scanning  
Notable characteristics: often carried out en masse, easily observed
- LATERAL MOVEMENT** Preferred methods: remote file copy (using various execution methods), use of Remote Desktop Protocol (RDP), then deployment of new service(s)  
Examples of utilities used: schtasks.exe, sc.exe, wmic.exe, psexec.exe





It is important to highlight that the themes related to how these threat actors operate, to a degree, suffer from the same availability and victim biases as the technical analysis using ATT&CK data. It is also important to note that although there is a fair amount of general public information related to these groups, there also exists a lag between publicly available data and observations from teams such as Gigamon ATR.

Threat actors often seek to maximize return on their investments and dynamically change portions of their attack methodology (be it tools or techniques) to extract additional longevity from their toolset and infrastructure. As is the case with any business, the incentives for profit are the driving force behind any such changes, and as such, threat actors avoid changing too many elements of their campaigns. This leaves telltale traces of their established techniques, tactics and procedures that provide agile security and research teams a means by which to detect and combat them. In the next section, we take a deeper look into the FIN8 threat group's profile.

# Case Study: FIN8

Within the financially motivated threat groups researched by Gigamon ATR, one group stands out for their unique methods of implementing tradecraft and use of custom malicious capabilities: FIN8. FIN8 is a financially motivated threat group, originally identified by FireEye<sup>9</sup> with capabilities further reported on by root9B<sup>10</sup> and Palo Alto Networks.<sup>11</sup> The group conducts targeted operations against the retail, hospitality and food industries to exfiltrate POS data from victims. FIN8 and some of their malicious capabilities have also been covered in depth by multiple intelligence providers.<sup>12</sup>

## AN EVOLVING ACTOR

Gigamon ATR has observed multiple intrusions by this group, and while we have identified numerous small and large changes across the attacker's toolchain, there remains a significant amount of shared code and a similar modus operandi between distinct observations of this threat group. There are numerous key differences between our observations and the publicly available reporting, which lead us to believe that this actor continues to evolve over time. We share these findings to ground the larger analysis presented in this paper in technical truth and to provide security practitioners with meaningful information that can be used to combat this threat.

## FIN8's CUSTOMIZATION

There are three distinct toolsets we have observed that are largely custom in nature (or adapted with pieces of public source code): the interactive reverse shell, the persistent memory implant and the POS memory scraper.



INTERACTIVE BACKDOOR	PERSISTENT BACKDOOR	POS MEMORY SCRAPER
<b>BADHATCH</b>	<b>ShellTea.B</b>	<b>PoSSlurp.B</b>
Execution begins with a PowerShell script that loads shellcode into memory and executes it. Once executing, the shellcode extracts an embedded DLL, the actual backdoor, and loads it.	The primary purpose of the persistent backdoor is to establish remote asynchronous access to the network and maintain a foothold on target systems through a persistence mechanism.	The primary goal of these actors is to gain access to payment card information from point-of-sale terminals. This component of their toolkit is deployed onto terminals to stage credit card numbers that it gets by scraping memory.



## BADHATCH CAPABILITIES

- BADHATCH possesses no anti-analysis or anti-sandbox features
- The threat has no built-in persistence capability
- A TLS-encapsulated custom protocol is used for C2
- It has the ability to spawn and inject into processes
- It can start an interactive shell

## ADDITIONAL COMPONENT DETAILS

### Interactive Reverse Shell – BADHATCH

The reverse shell appears to be most closely related to the PowerSniff variant discussed in previous analysis,<sup>13</sup> but with significant differences in code and functionality, enough so that it is likely an entirely different tool with shared code or a significant evolution. While it is possible that this backdoor is related to PowerSniff, we were unable to ascertain the exact nature of the relation and therefore decided to independently name the capability BADHATCH.

The variant of PowerSniff previously associated with FIN8 has a small number of similarities to BADHATCH, primarily in the loading and injection techniques, including the use of the same function hashing code from Carberp. There are a significant number of technical and functional differences in BADHATCH, as seen in the sidebar.

BADHATCH communicates back to hardcoded command and control servers via directly hardcoded IP addresses, using a non-HTTP compliant TLS-protected channel. This provides the actor numerous capabilities including the ability to:

- Download files to an attacker-specified path
- Spawn and inject into a svchost.exe host process
- Upload files from the victim system
- Start an interactive reverse shell

The shell, identified as “SUPER REMOTE SHELL v2.2 SSL” in the banner that is passed back upon established communications, provides the actor the ability to execute commands and retrieve output.

#### Example

```
-----  
* SUPER REMOTE SHELL v2.2 SSL  
-----
```

```
OS: %s SP %d %s
```

```
HOSTNAME: %s
```

```
Press i+enter to impersonate shell or just press enter
```

### Persistent Memory Implant – ShellTea.B

This component is one of the most complicated custom modules observed in use by the actor and is the only one with a built-in persistence mechanism. The versions of this component observed by Gigamon ATR seem to be most closely related to, and likely a variation of, ShellTea as reported by root9B.<sup>14</sup> For the purpose of this report, we title this component ShellTea.B.

The backdoor provides typical remote access capabilities to the attacker, such as the ability to download executables and DLLs and run them, load DLLs or shellcode into memory and run them, and persistence via the well-known registry Run key.

The primary difference between ShellTea and ShellTea.B is how the backdoor was observed communicating. ShellTea.B, as observed by Gigamon ATR, communicated to the command and control servers using an SSL/TLS protected HTTP-compliant channel, whereas ShellTea was noted as communicating using “a custom binary protocol” in previous analysis.<sup>10</sup> As such, the networking libraries utilized by the backdoor differed as well. Within the communications, the same underlying XTEA protocol identified in public reporting was utilized as the HTTPS payload body. The command and control servers utilized a standard self-signed “Internet Widgets” Apache SSL certificate.

#### Example

Subject and issuer of certificate exchanged during communications matches that of the known Apache default certificate

Subject DN: C=AU, ST=Some-State, O=Internet Widgets Pty Ltd  
 Issuer DN: C=AU, ST=Some-State, O=Internet Widgets Pty Ltd

## PERSISTENT BACKDOOR: COMPARISON

	SHELLTEA	SHELLTEA.B
<b>COMMUNICATION</b>		
Connects over port 443 using a custom binary protocol	✓	
Communicates over HTTPS		✓
<b>NETWORK FUNCTIONS</b>		
Imports network functions from Ws2_32.dll (connect, send, etc.)	✓	
Imports network functions from wininet.dll (InternetConnectA, HttpSendRequestA, etc.)		✓
<b>OBFUSCATION</b>		
Uses a custom function resolver with 4-byte hashes and seed 0x463283F5, multiplier 0x19660D, increment 0x3C6EF35F	✓	
Use of a custom function resolver with 4-byte hashes and seed 0x3C1AD0A6, multiplier 0x19660D, increment 0x3C6EF35F		✓
The use of a unique and custom function hash resolution routine to obfuscate API function names	✓	✓
Near identical use of low-level undocumented API functions	✓	✓
Identical obfuscated format string utilized in a mutex	✓	✓
Same anti-analysis and process detection techniques	✓	✓
100% overlap in CRC32 process hash list	✓	✓

## POS Memory Scraper – PoSlurp.B

In engagements with FIN8 Gigamon ATR observed possible variants of PoSlurp, based on comparisons with public reporting. PoSlurp.B begins with execution of a PowerShell script on the target host that is responsible for initializing the environment, unpacking the embedded DLL, and then cleaning up artifacts through overwriting and self-deleting.

### Example

Wmic.exe command used to execute the scraper on a target POS device

```
wmic /node:"@t.txt" /user:"<USERNAME>" /password:"<PASSWORD>"  
process call create "powershell -ep bypass -c <PATH\SCRIPT>.ps1"
```

The key similarities between PoSlurp and PoSlurp.B are the custom search algorithm for identifying track 1 and track 2 credit card data, as well as the same encryption method and constants utilized for exfiltrated information. There are several key differences in the scraper component:

- PoSlurp.B has additional command line arguments to control injection options, such as running the scraper without injecting, or spawning and APC injecting into a svchost.exe process
- It lacks some anti-analysis features utilized in PoSlurp (such as the use of anti-analysis techniques)
- It also uses high-level API functions in place of the low-level equivalents in PoSlurp (e.g., VirtualAlloc in place of ZwAllocateVirtualMemory)
- It lacks built-in cleanup of encrypted data dropped for exfiltration

While there was a lack of automated cleanup observed, incident response partners observed the actors performing this cleanup manually.

## POS MEMORY SCRAPING PROCESS



### Initialize the Environment

- Set environment variable for command line parameters



### Load and Execute the Scraper

- Scraper loaded and executed
- Injection into target process performed
- Data scraped and saved to an encrypted log file



### Cleanup

- PowerShell script moved to temporary file and overwritten with a copy of regedit.exe
- Overwritten file is then deleted

### Example

Command line log examples of how the actor retrieved exfiltrated information back to a bastion host and attempts to delete associated artifacts manually

```
for /F %i in (<FILENAME>.txt) DO attrib -h \\%i%c$\users\<LOCAL ADMIN  
USER>\appdata\local\temp\<FILENAME>.tmp  
  
for /F %i in (<FILENAME>.txt) DO net use \\%i%c$ /user:%i\<USERNAME>  
<PASSWORD>  
  
for /F %i in (<FILENAME>.txt) DO copy \\%i%c$\users\<LOCAL ADMIN  
USER>\appdata\local\temp\<FILENAME>.tmp %i.tmp  
  
for /F %i in (<FILENAME>.txt) DO del \\%i%c$\users\<LOCAL ADMIN  
USER>\appdata\local\temp\<FILENAME>.tmp
```

---

## CONFORMING TO TRENDS

It is easy to look at all the custom capabilities employed by FIN8 and classify them as deviating from the trend of the “average actor.” However, the FIN8 group marries these custom tools with methodologies and tradecraft that conform significantly to the trends identified in the previous section. In our first-party observations, FIN8 utilizes almost all of the trending ATT&CK techniques throughout their lifecycle and matches with some of the higher-level items. This is highlighted to demonstrate that even with deviating groups, appropriately abstracted trends add significant value to a security program. Tactically, by leveraging detections that not only look for specific tools or campaigns, but also focus generically on the techniques employed across campaigns and even across groups, security programs will increase resiliency.

## Summary: Key Takeaways

Intelligence analysis must drive action. In this case, understanding financially motivated threat groups should drive efforts to increase visibility into an adversary's field of play. This strengthens detection efforts and helps to determine strategic, operational and tactical priorities across a security program. Teams should remember that while this report focused on understanding a specific type of threat, defending against one threat often results in overlapping coverage against other threats, presenting a defensive economy of scale.

Based upon our broad analysis and the glimpse at FIN8, Gigamon ATR offers the following takeaways for security professionals seeking to defend against these attacks:

Details	Key Takeaway	Actions
Visibility across the enterprise and at various layers of the enterprise is critical to effectively defend. Network visibility enables a breadth of coverage while endpoint visibility (to include logging such as PowerShell Logging) enables deep ground truth.	<b>ENTERPRISE WIDE VISIBILITY IS CRITICAL</b>	Architectures must be built, or improved upon, to enable such visibility into gaps (e.g., POS environments with egress locations at branches).
In many cases, communication encryption can act as an indicator of compromise. A balanced strategy of "breaking" encryption where appropriate and leveraging the metadata involved in encryption is often successful. In the case of FIN8, the use of self-signed default certificates presents a considerable opportunity to observe the command and control traffic, but in general, it represents a way to use elements of the encrypted traffic to identify it as suspicious.	<b>ENCRYPTION DOES NOT DEFEAT DETECTION</b>	In cases where encryption does in fact present a challenge, teams should fall back on successful detection strategies and enterprise visibility (to include the endpoint).
Administrative tools (e.g., WMIC, PowerShell Remoting, PSEXEC, etc.) provide a great channel for administrators to take actions across a network, but an overly permissive configuration that allows administrative behaviors between endpoints and network segments provides huge opportunities for attackers.	<b>ADMINISTRATIVE FUNCTIONALITY IS DOUBLE-EDGED</b>	In any organization, there should be a limited authorized subset of users and/or systems performing these actions. Teams should focus on minimizing these.
For each technique or tradecraft element identified in our analysis, there are multiple methods of detection that vary in implementation effort.	<b>VARIED DETECTION STRATEGIES SUCCEED</b>	Defenders must fully utilize the detection spectrum to ensure early threat discovery, minimizing chances of evasion through alteration.
The use of off-the-shelf tools is beneficial to the adversary; understanding these tools is even more beneficial to defensive teams, as it removes the "unknown" aspects of detection, provided that a team is properly observing, collecting info on and studying the evolution of public tradecraft.	<b>LEVERAGE INTELLIGENCE TO INFORM DEFENSE</b>	As adversaries continue to use off-the-shelf tools and tradecraft, monitoring for and understanding such tradecraft is critical for any team performing detection and response.
The practice of detection and response has been discussed at length over the last decade. Performing high-quality response in a timely manner is a very effective way to save on the cost of a breach. Simply stated, failed containment results in a longer response time and a higher risk of a costly breach.	<b>RESPONSE FUNDAMENTALS ARE KEY</b>	To respond appropriately, ensure you have qualified personnel with exercised and tuned processes who are supported by the right technology.



## About Gigamon ATR

The Gigamon Applied Threat Research (ATR) team's mission is 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.

---

### THREAT INTELLIGENCE

Research threats in order to inform detection engineering efforts

---

### DETECTION ENGINEERING

Research, build, and maintain high quality detection capabilities for Gigamon Insight

---

### SECURITY ENGINEERING

Act as user zero for Gigamon Insight. Research, prototype and validate future functionality for detection and investigation capabilities

Gigamon 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 Gigamon Insight through detection capabilities and curated rule sets — complete with full rule descriptions, justifications and logic — to help protect customer environments.

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

**Accelerate Threat Response:** Rapidly *Hunt, Detect, Investigate & Respond* with confidence to threats without wasting time aggregating contextual evidence or the headache of tool maintenance and cost.

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.

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

[LEARN MORE ABOUT GIGAMON INSIGHT AT GIGAMON.COM/INSIGHT](https://www.gigamon.com/insight)

# References

- <sup>1</sup> Verizon. "2019 Data Breach Investigations Report." Verizon. 2019. Accessed July 9, 2019. <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>.
- <sup>2</sup> United States Department of Justice. "Three Members of Notorious International Cybercrime Group 'Fin7' in Custody for Role in Attacking Over 100 U.S. Companies." United States Department of Justice, Office of Public Affairs. August 1, 2018. Accessed July 9, 2019. <https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100>.
- <sup>3</sup> Malwarebytes. "Emotet Revisited: Pervasive Threat Still a Danger to Businesses." Malwarebytes Labs. March 14, 2019. Accessed July 9, 2019. <https://blog.malwarebytes.com/cybercrime/2019/03/emotet-revisited-this-pervasive-persistent-threat-is-still-a-danger-to-businesses/>.
- <sup>4</sup> CISA. "SamSam Ransomware." United States Department of Homeland Security CISA. December 3, 2018. Accessed July 9, 2019. <https://www.us-cert.gov/ncas/current-activity/2018/12/03/SamSam-Ransomware>.
- <sup>5</sup> Mainor, David, Nick Richard, Charles Prevost, and Charles Carmakal. "FIN10: Anatomy of a Cyber Extortion Operation." <https://www.fireeye.com/blog/threat-research/2017/06/fin10-anatomy-of-a-cyber-extortion-operation.html>; Team RiskIQ. "Inside Magecart: RiskIQ and Flashpoint Release Comprehensive Report on Cybercrime and the Assault on E-Commerce." RiskIQ. November 13, 2018. Accessed July 9, 2019. <https://www.riskiq.com/blog/external-threat-management/inside-magecart/>.
- <sup>6</sup> McKeague, Brendan, Van Ta, Ben Fedore, Geoff Ackerman, Alex Pennino, Andrew Thompson, and Douglas Bienstock. "Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware." FireEye. April 5, 2019. Accessed July 9, 2019. <https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html>.
- <sup>7</sup> MITRE. "ATT&CK." 2019. Accessed July 9, 2019. <https://attack.mitre.org/>.
- <sup>8</sup> MITRE. "ATT&CK Sightings." 2019. Accessed July 9, 2019. <https://attack.mitre.org/resources/sightings/>.
- <sup>9</sup> Kizhakkinan, Dhanesh, Yu Wang, Dan Caselden, and Erica Eng. "Threat Actor Leverages Windows Zero-day Exploit in Payment Card Data Attacks." FireEye. May 11, 2016. Accessed July 9, 2019. <https://www.fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html>; FireEye. "Know Your Enemy: New Financially-Motivated & Spear-Phishing Group." FireEye. August 18, 2016. Accessed July 9, 2019. <https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html>.
- <sup>10</sup> root9B. "ShellTea + PoSlurp Malware." R9B. June 19, 2017. Accessed July 9, 2019. <https://www.root9b.com/newsroom/shelltea-poslurp-malware/>.
- <sup>11</sup> Grunzweig, Josh, and Brandon Levene. "PowerSniff Malware Used in Macro-based Attacks." Palo Alto Networks Unit 42. March 11, 2016. Accessed July 9, 2019. <https://unit42.paloaltonetworks.com/powersniff-malware-used-in-macro-based-attacks/>.
- <sup>12</sup> FireEye. "Know Your Enemy: New Financially-Motivated & Spear-Phishing Group." FireEye. August 18, 2016. Accessed July 9, 2019. <https://www2.fireeye.com/WBNR-Know-Your-Enemy-UNC622-Spear-Phishing.html>; root9B. "ShellTea + PoSlurp Malware." R9B. June 19, 2017. Accessed July 9, 2019. <https://www.root9b.com/newsroom/shelltea-poslurp-malware/>.
- <sup>13</sup> root9B. "ShellTea + PoSlurp Malware." R9B. June 19, 2017. Accessed July 9, 2019. <https://www.root9b.com/newsroom/shelltea-poslurp-malware/>.
- <sup>14</sup> root9B. "ShellTea + PoSlurp Malware: Memory-Resident Point-of-Sale Malware Attacks Industry." R9B. June 2017. Accessed July 9, 2019. [https://www.root9b.com/content/uploads/2018/10/PoS-Malware-ShellTea-PoSlurp\\_YARA.pdf](https://www.root9b.com/content/uploads/2018/10/PoS-Malware-ShellTea-PoSlurp_YARA.pdf).
- <sup>15</sup> Kill Chain graphics. Lockheed Martin. Retrieved February 26th, 2019. <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>.