CROWDSTRIKE

2022 Global Threat Report

Foreword

The CrowdStrike 2022 Global Threat Report provides crucial insights into what security teams need to know about to stay ahead of today's threats in an increasingly ominous threat landscape.

For security teams on the front lines and those of us in the business of stopping cyberattacks and breaches, 2021 provided no rest for the weary. In the face of massive disruption brought about by the COVID-driven social, economic and technological shifts of 2020, adversaries refined their tradecraft to become even more sophisticated and brazen. The result was a series of high-profile attacks that rocked many organizations and, on their own, represented watershed moments in cybersecurity.

As organizations scrambled at the start of 2021 to protect supply chains and interconnected systems in the face of the incredibly sophisticated Sunburst attack, adversaries exploited zero-day vulnerabilities and architectural limitations in legacy systems like Microsoft to leave many reeling. At the same time, eCrime syndicates refined and amplified big game hunting (BGH) ransomware attacks that ripped across industries, sowing devastation and sounding the alarm on the frailty of our critical infrastructure.

For security teams already dealing with an ongoing skills shortage, these issues proved challenging enough on their own. But the strain on security teams was amplified even more at the end of the year when the ubiquitous Log4Shell vulnerability threatened a complete security meltdown.

Understanding these events gives visibility into the shifting dynamics of adversary tactics, which is critical for staying ahead of today's threats. This is the context that the CrowdStrike 2022 Global Threat Report delivers. Developed based on the firsthand observations of our elite CrowdStrike Intelligence and Falcon OverWatch™ teams, combined with insights drawn from the vast telemetry of the CrowdStrike Security Cloud, this year's report provides crucial insights into what security teams need to know about an increasingly ominous threat landscape.

Among the details you'll learn in this year's report:

❯ **How state-sponsored adversaries targeted IT and cloud service providers to exploit trusted relationships and supply chain partners**

❯ **How state-sponsored adversaries weaponized vulnerabilities to evade detection and gain access to critical applications and infrastructure**

❯ **How sophisticated adversaries exploited stolen credentials and identities to amplify ransomware BGH attacks and infiltrate cloud environments**

❯ **How malicious actors intensified attacks on critical cloud infrastructure with new, sophisticated approaches**

➜

Enterprise risk is coalescing around three critical areas:
- **Endpoints and cloud workloads**
- **Identity**
- **Data**

Our annual report also paints a picture that shows enterprise risk is coalescing around three critical areas: endpoints and cloud workloads, identity and data. Threat actors continue to exploit vulnerabilities across endpoints and cloud environments, and ramp up innovation on how they use identities and stolen credentials to bypass legacy defenses — all to reach their goal, which is your data. CrowdStrike has observed that *62% of attacks comprise non-malware, hands-on-keyboard activity.* As adversaries advance their tradecraft in this manner to bypass legacy security solutions, autonomous machine learning alone is not good enough to stop dedicated attackers.
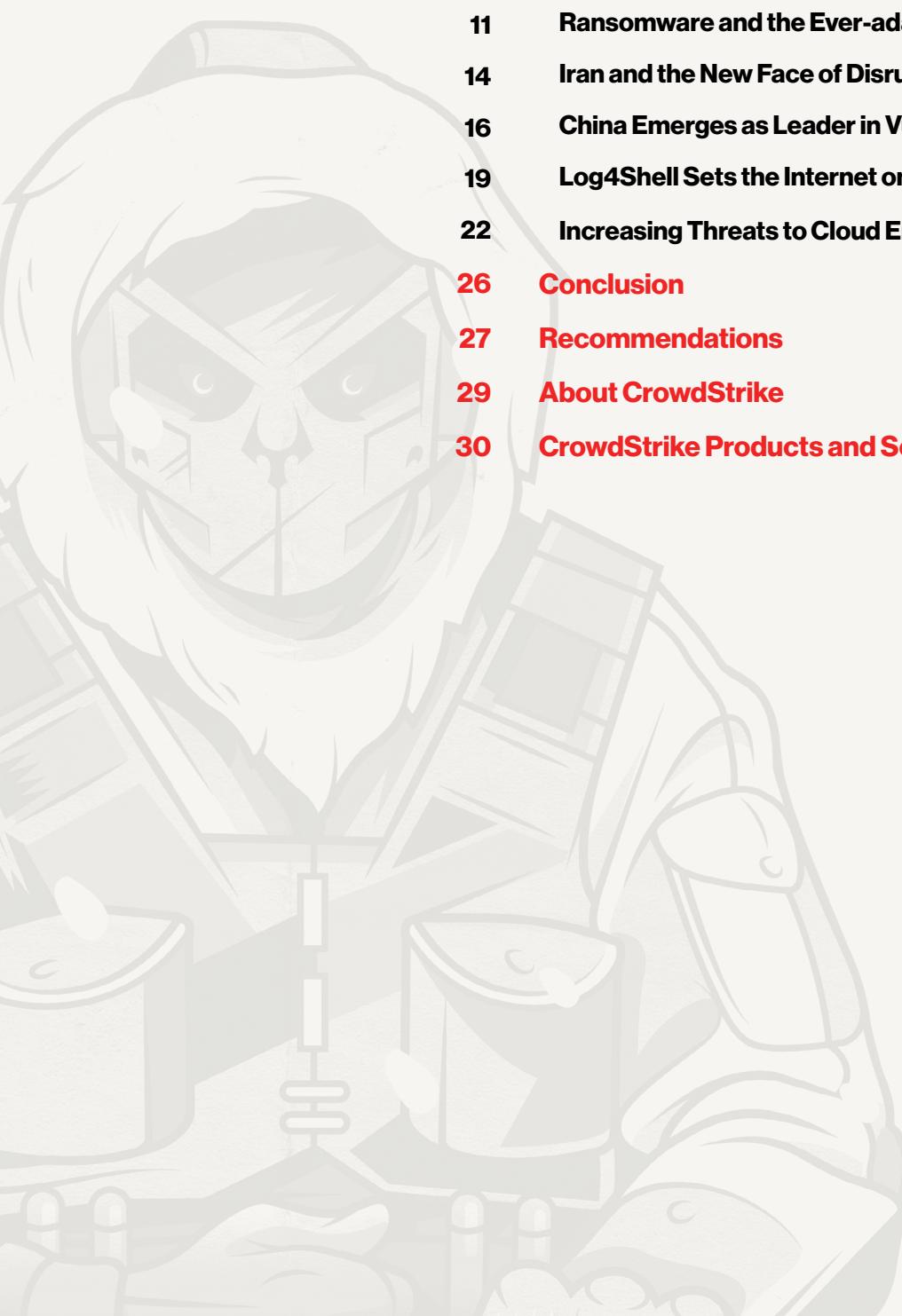
CrowdStrike is relentless in our drive to keep you ahead of adversaries today and into the future. To meet the adversaries head-on, we're unifying a modern approach to security with a platform that connects the machine both to the identity and the data to deliver full Zero Trust protection. As adversaries shift to targeting cloud workloads, we're providing deep visibility and proactive security across the entire cloud-native stack. To alleviate the burden of the constant cycle of patching, we're prioritizing the vulnerabilities that create the most risk. And for the most sophisticated attacks, we've delivered powerful new extended detection and response (XDR) capabilities to help overwhelmed security teams automate response and reduce the time it takes to hunt across domains.

2021 taught us that no matter how much adversity we face, the adversary will not rest. Attacks are growing more destructive, causing mass disruption in all aspects of our daily lives. But this is the challenge we've accepted and a fight that *we will win together*. I hope you find this report informative and that it gives you the same clarity of purpose it gives me: to be unrelenting in our drive to stop adversaries from stopping business and our way of life.

George Kurtz

George Kurtz
CrowdStrike CEO and Co-Founder

Table of Contents

Introduction

➔

In 2021,
targeted intrusion adversaries continued to adapt to the changing operational opportunities and strategic requirements of technology and world events.

As we reflect upon 2021, two overarching themes come to the forefront: adaptability and perseverance. Businesses are finding paths forward with new technologies and solutions, adapting in the face of adversity and persevering in spite of uncertainty as we continue to navigate the challenges of living through a global pandemic. While these issues will ultimately lead to strength and innovation in organizations around the world, they will also create new risks and vulnerabilities that can be exploited.

Cyber adversaries kept pace in 2021 with many adapting to a changing target landscape. This trend was perhaps best exemplified by the shifts observed in the 2021 eCrime ecosystem, which — while remaining vast and interconnected — comprises many criminal enterprises that exist to support big game hunting (BGH) ransomware operations. Notably, adversaries in 2021 were able to circumvent actions that threatened cessation of their operations, and some even resorted to rebranding as a result. Despite new approaches taken by law enforcement, including attempts to seize ransom payments and criminal funds before they reached adversaries' hands, CrowdStrike Intelligence observed an 82% increase in ransomware-related data leaks in 2021, compared to 2020. This increase, coupled with other data leaks, is a stark reminder of the value that adversaries place on victim data.

In 2021, targeted intrusion adversaries continued to adapt to the changing operational opportunities and strategic requirements of technology and world events. Russian, Chinese, Iranian and North Korean adversaries were all observed employing new tradecraft or target-scopes meant to respond to global trends. This included: Russia's targeting of IT and cloud service providers to exploit trusted relationships; China's weaponization of vulnerabilities at scale to facilitate initial access efforts; Iran's use of ransomware to blend disruptive operations with authentic eCrime activity; and Democratic People's Republic of Korea's (DPRK) shift to cryptocurrency-related entities in an effort to maintain illicit revenue generation during economic disruptions caused by the pandemic.

21

Newly named aversaries

45%

Increase in interactive intrusion campaigns

170+

Total adversaries tracked

82%

Increase in ransomware-related data leaks

Governments are also adapting. This year, CrowdStrike Intelligence debuted two new adversary animals — WOLF and OCELOT — to label targeted intrusions emanating from Turkey and Colombia, respectively. The presence of these new adversaries underscores the increase in offensive capabilities outside of governments traditionally associated with cyber operations, and highlights the variety of actor end goals. Private sector offensive actors (PSOAs), such as *NSO Group* and *Candiru*, continued to serve as hackers-for-hire throughout 2021, providing governments with substitute or supplemental capabilities and further enlarging the global actor space.

In the hacktivist landscape, CrowdStrike Intelligence observed the continued development of grassroots operations and a proliferation of established hacktivist groups across the world. The rise of Belarusian group *Cyber Partisans* since late 2020, the expanded role and diversification of the broader Iranian hacktivist ecosystem, and the growing participation of various hacktivists in response to Western political developments all exemplify this trend.

As our adversaries adapt, so do we. CrowdStrike Intelligence offered an unparalleled level of coverage throughout 2021, adding 21 named adversaries and raising the total of tracked actors across all motivations to over 170. CrowdStrike Intelligence continues to expand coverage of threat landscapes beyond targeted intrusion, eCrime and hacktivist mission areas; in 2021, we increased support for vulnerability intelligence and mobile intelligence across all our products.

In 2021, CrowdStrike launched Falcon X Recon+ as a companion service for Falcon X Recon™. Falcon X Recon+ analysts manage monitoring, triaging, assessing and mitigating threats across the criminal underground. They also assess and recommend effective mitigation steps, helping customers act decisively and proactively to prevent and detect future attacks. CrowdStrike's Falcon X Elite service was also expanded in 2021 to provide a single point of contact for onboarding, product integration, intelligence clarification, personalized threat briefing and intelligence research. Falcon X Elite analysts continue to provide proactive notifications of threats to CrowdStrike customer organizations.

The CrowdStrike 2022 Global Threat Report summarizes the entirety of analysis performed by the CrowdStrike Intelligence team throughout 2021, including descriptions of notable themes, trends and significant events in cybersecurity. This analysis, combined with case studies from the Falcon OverWatch™ managed threat hunting team, demonstrates how threat intelligence and proactive hunting can provide a deeper understanding of the motives, objectives and activities of these actors — information that can empower swift proactive countermeasures to better defend your valuable data now and in the future.

Naming Conventions

This report follows the naming conventions instituted by CrowdStrike to categorize adversaries according to their nation-state affiliations or motivations. The following is a guide to these adversary naming conventions.

Adversary	Nation-state or Category
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SPIDER	ECRIME
TIGER	INDIA
WOLF	TURKEY

Threat Landscape Overview

eCrime Breakout Time

1 hour 38 minutes

Today's eCrime adversaries move with speed and purpose in pursuit of their objectives.

The CrowdStrike Falcon OverWatch team measures breakout time — the time an adversary takes to move laterally from an initially compromised host to another host within the victim environment. Our analysis of the breakout time for hands-on eCrime intrusion activity in 2021 — where such a metric could be derived — revealed an average of just 1 hour 38 minutes.

This number is essentially unchanged from what was reported by CrowdStrike's Falcon OverWatch team in the CrowdStrike 2021 Threat Hunting Report, when breakout time for eCrime actors was measured at 1 hour 32 minutes. eCrime adversaries continue to show a high degree of sophistication as evidenced by the speed at which they can move through a victim environment, leaving a very short window for defenders to respond.
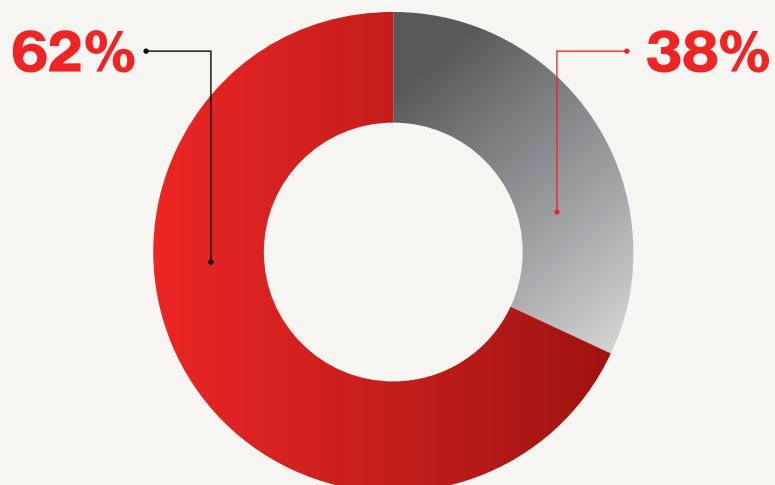
Adversary Tactics

Detections indexed by the CrowdStrike Security Cloud in Q4 2021

■ Malware-Free   ■ Malware

Adversaries continue to show that they have moved beyond malware.
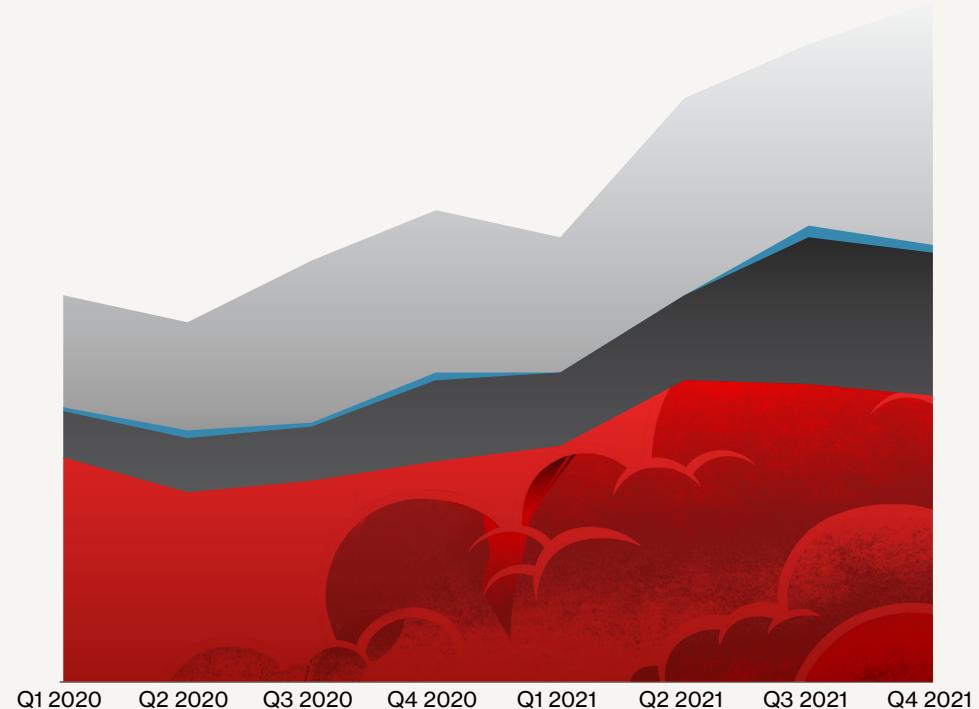
Attackers are increasingly attempting to accomplish their objectives without writing malware to the endpoint. Rather, they have been observed using legitimate credentials and built-in tools — an approach known as "living off the land" (LOTL) — in a deliberate effort to evade detection by legacy antivirus products. Of all detections indexed by the CrowdStrike Security Cloud in the fourth quarter of 2021, 62% were malware-free.

62%   **38%**

In 2021, OverWatch tracked steadily increasing numbers of interactive intrusion campaigns. Compared to 2020, OverWatch observed a near 45% increase in the number of such campaigns, and uncovered more in the fourth quarter than in any other quarter.

Interactive Intrusion Activity Over Time

Figure 1. Quarterly Growth in Interactive Intrusion Campaigns by Threat Type, Q1 2020 to Q4 2021
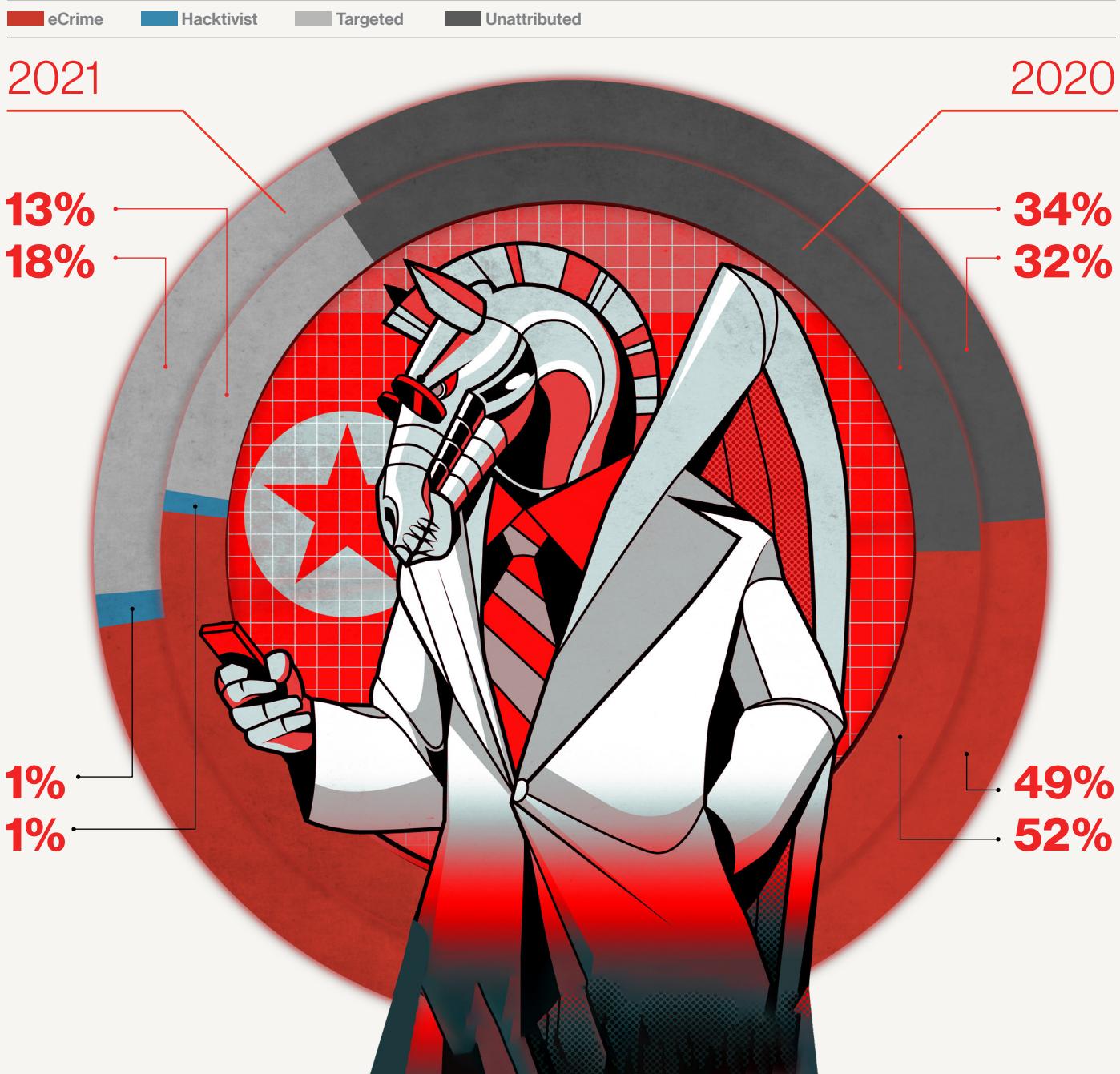
Types of Threat Activity

eCrime	Financially motivated criminal intrusion activity
Targeted	State-sponsored intrusion activity that includes cyber espionage, state-nexus destruction attacks and generating currency to support a regime
Hacktivist	Intrusion activity undertaken to gain momentum, visibility or publicity for a cause or ideology
Unattributed	Insufficient data were available to make a confident attribution

Financially motivated eCrime activity continues to dominate the interactive intrusion attempts tracked by OverWatch. Intrusions attributed to eCrime accounted for nearly half (49%) of the observed activity, while targeted intrusions accounted for 18%, hacktivist activity was responsible for 1% and the remaining 32% of attacks remain unattributed. The distribution of these figures is similar to that of 2020.

Interactive Intrusion Campaigns by Threat Type
2020 vs. 2021

■ eCrime   ■ Hacktivist   ■ Targeted   ■ Unattributed

2021

13%
18%

1%
1%

2020

34%
32%

49%
52%

2021 Themes

Ransomware and the Ever-adaptable Adversary

The growth and impact of BGH in 2021 was a palpable force felt across all sectors and in nearly every region of the world. Although some adversaries and ransomware ceased operations in 2021, the overall number of operating ransomware families increased. CrowdStrike Intelligence observed an 82% increase in ransomware-related data leaks in 2021, with 2,686 attacks as of Dec. 31, 2021, compared to 1,474 in 2020. These figures, coupled with other data leaks, highlight how valuable victim data is to adversaries.
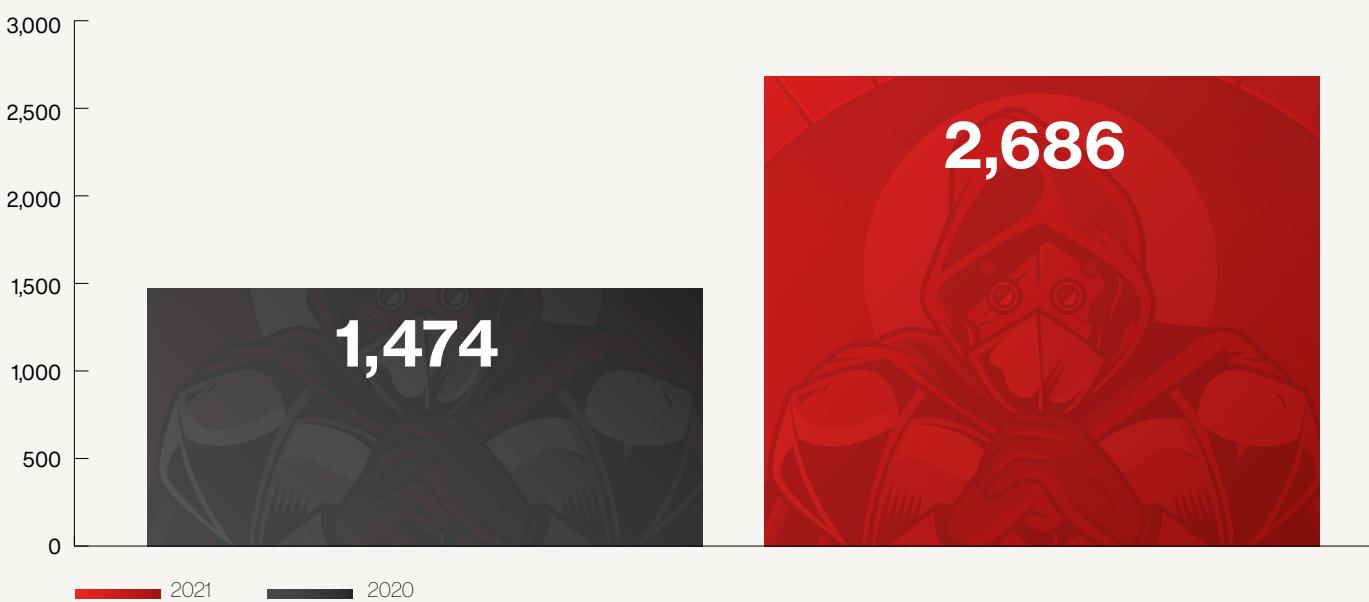
82%
Increase in ransomware-related data leaks in 2021

Number of attacks
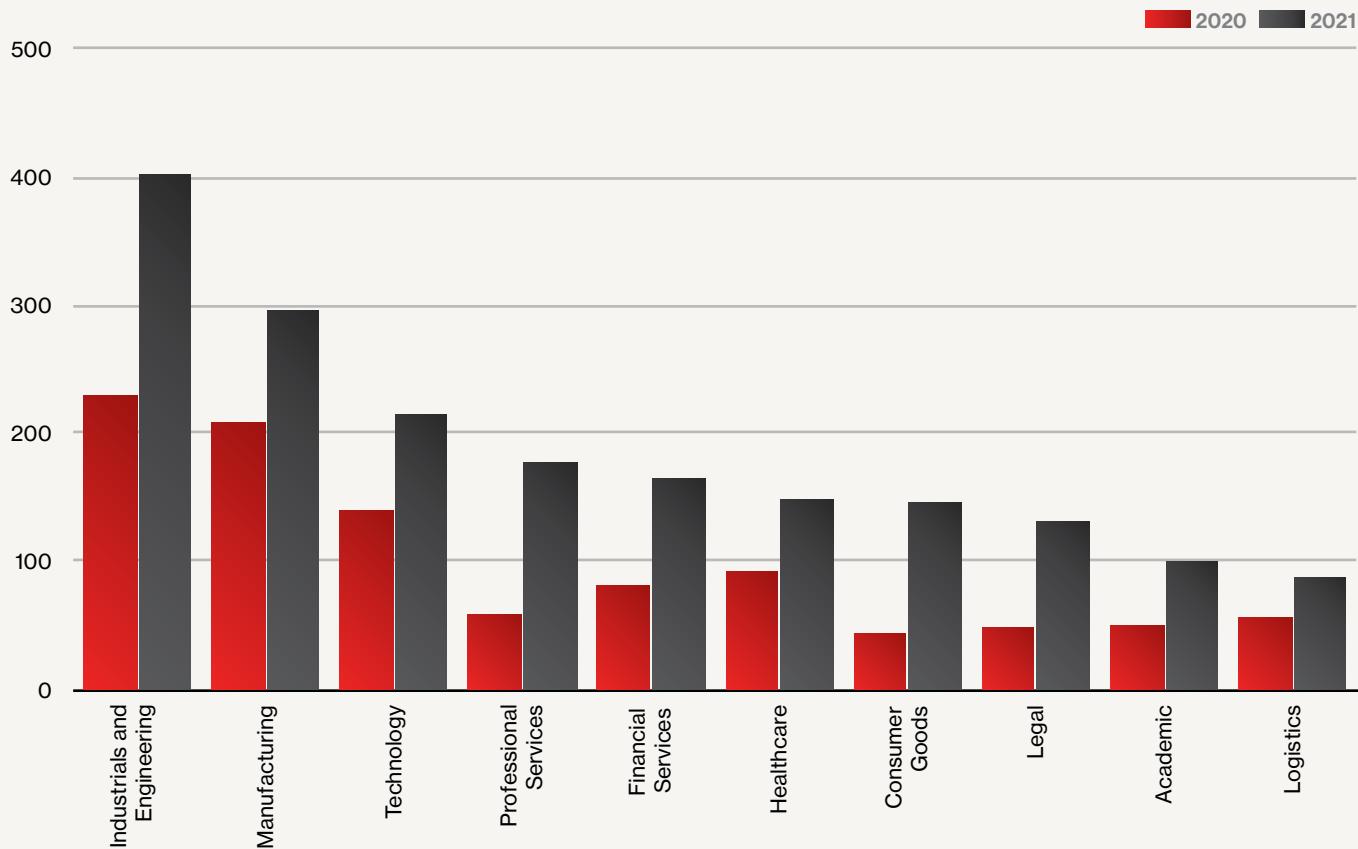
Figure 2. Number of Ransomware-related Attacks Leading to Data Leaks, 2020 vs. 2021

2021 Themes
Ransomware and the Ever-adaptable Adversary

Figure 3. Comparison of Data Leaks by Sector (Top 10), 2020 vs. 2021

At times, the BGH landscape has been unpredictable, and adversaries have not always been able to immediately gauge the success or outcome of their ransomware operations. This change in landscape fluidity was observed following operations that targeted large organizations and resulted in attention and action from the highest levels of U.S. government and law enforcement, causing some adversaries to rebrand or even deactivate their tools.

The impact of government and law enforcement action on eCrime operations was also observed in the CrowdStrike eCrime Index (ECX). For example, increased media and law enforcement attention after the Colonial Pipeline and JBS Foods incidents conducted by CARBON SPIDER and PINCHY SPIDER affiliates resulted in a reduction in data leaks and access broker advertisements, which caused the ECX to dip, recover and remain volatile to date. For more detail, read this blog.

New tactics, techniques and procedures (TTPs) used in data theft attacks in 2021 aided adversaries in extorting their victims. For example, adversaries such as BITWISE SPIDER avoided using publicly available exfiltration tools by developing their own. Another major development was increased data theft and extortion without the use of ransomware, leading to the establishment of new marketplaces dedicated to advertising and selling victim data.

However, one key theme highlighted throughout 2021 is that adversaries will continue to react and move operations to new approaches or malware wherever possible, demonstrating that the ever-adaptable adversary remains the key threat within the eCrime landscape.

Falcon OverWatch
Case Study

WIZARD SPIDER Accesses Multiple Servers During Targeted BGH Operation

WIZARD SPIDER was a prolific figure on the ransomware scene in 2021. With a wealth of custom tooling at their disposal and proficiency at using native utilities to progress their intrusions, WIZARD SPIDER identified and developed a successful business model. OverWatch uncovered this threat actor in an intrusion against an organization in the engineering vertical. The TTPs observed throughout this intrusion were consistent with targeted BGH activity seen from WIZARD SPIDER in the past. The intrusion spanned four domain controllers and two valid accounts.

Domain Controller Count: 1

Defense Evasion and Discovery

WIZARD SPIDER utilized RDP to authenticate into a Windows Domain Controller via a valid domain account. The Falcon sensor raised the first of multiple detections when malware was injected into the legitimate MSTSC process by a custom shellcode loader, *ShellStarter*. Falcon OverWatch uncovered the adversary leveraging two native utilities, BITSadmin and Rundll32, to download and execute their custom tooling. OverWatch hunters quickly zeroed in on uncovering the activity's context, armed with CrowdStrike Falcon® sensor telemetry providing insights into the associated process trees. A notification was then pushed to the victim organization.

Persistence

The threat actor created a scheduled task to execute *ShellStarter* at a later date, potentially with the intent to reinfect the victim.

Domain Controller Count: 2

Credential Access

Minutes later, WIZARD SPIDER moved laterally using RDP to access a second domain controller using the same valid credentials. Here they used the built-in Ntdsutil utility to harvest credentials by copying the NTDS database.

Command and Control (C2)

The actor pushed a rogue DLL file to another server before executing the DLL using the Microsoft signed binary Rundll32. In this instance, the WIZARD SPIDER tool, *AnchorDNS*, was used to perform C2 connections over the DNS protocol. Multiple encoded DNS requests were sent outbound to the C2 nameserver.

Domain Controller Count: 3

Lateral Movement

WIZARD SPIDER moved laterally to a third domain controller through a Windows administrative share and set *AnchorDNS* to run as a service using native tooling.

Domain Controller Count: 4

Persistence

Acting on CrowdStrike's notifications, the victim organization's incident response took over at this point and began eliminating the actor within the environment. During remediation, OverWatch identified WIZARD SPIDER returning to a fourth domain controller using a new administrator account. OverWatch rapidly notified the victim, and the actor was once again removed from the environment.

2021 Themes

Iran and the New Face of Disruptive Operations

➜

CrowdStrike Intelligence is currently tracking several adversaries and activity clusters that are engaged in lock-and-leak operations.

Since late 2020, multiple Iran-nexus adversaries and activity clusters have adopted the use of ransomware as well as "lock-and-leak" disruptive information operations (IO) to target multiple organizations within the U.S., Israel and the greater Middle East and North Africa (MENA) region. Lock-and-leak operations are characterized by criminal or hacktivist fronts using ransomware to encrypt target networks and subsequently leak victim information via actor-controlled personas or entities. Since they inauthentically operate as a criminal or hacktivist entity, these types of operations conduct activity beneath a veneer of deniability. Through the use of dedicated leak sites, social media and chat platforms, these actors are able to amplify data leaks and conduct IO against target countries.

At present, CrowdStrike Intelligence is tracking several adversaries and activity clusters that are engaged in lock-and-leak operations. Based on available data, PIONEER KITTEN was the first adversary to switch from conducting likely traditional targeted intrusion operations to lock-and-leak activities in 2021. Following that, SPECTRAL KITTEN (aka *BlackShadow*), the ChaoticOrchestra activity cluster (aka *Deus*) and the SplinteredEnvoy activity cluster (aka *Moses Staff*) were observed primarily targeting Israeli entities with lock-and-leak operations throughout 2021 using multiple ransomware families.

In contrast to the publicity-seeking operations and lock-and-leak campaigns observed throughout 2021, disruptive activity associated with the NEMESIS KITTEN adversary lacked a distinct messaging component and largely operated discreetly. NEMESIS KITTEN conducted wide-ranging scanning and exploitation operations to establish footholds in various networks, and in select instances, conducted ransomware operations using *BitLocker*, a likely unique ransomware variant called *SunDawn*, and, in one case, a custom wiper.

The use of high-profile lock-and-leak operations, as well as the more subdued but pervasive NEMESIS KITTEN activity, provides Iran with an effective capability to disruptively target its rivals in the region and abroad. Given the success of these operations, Iran will likely continue to use disruptive ransomware into 2022.

Falcon OverWatch
Case Study

NEMESIS KITTEN Thwarted at Every Turn

In late 2021, OverWatch uncovered a hands-on intrusion against a South American technology entity. The observed TTPs, along with the use of specific tooling including the *Fatedier* Reverse Proxy tool, were consistent with activity previously attributed to the threat actor tracked by CrowdStrike Intelligence as NEMESIS KITTEN. The actor's efforts were largely unsuccessful because they were blocked at every turn by the Falcon sensor.

Defense Evasion

The actor was observed making numerous attempts to disable Windows Defender, including modifying the Windows registry to disable Windows Defender real-time monitoring and using PowerShell to create a scheduled task configured to use the `Set-MpPreference` cmdlet to impair Windows Defender protections. This was the first of multiple attempted attack techniques blocked by the Falcon sensor.

Persistence and C2

The actor attempted to create a scheduled task to download and execute the *Fatedier* Reverse Proxy tool configured to communicate with known NEMESIS KITTEN C2 infrastructure. This attempt was prevented by the Falcon sensor. In an attempt to establish persistence, the actor created a new local user account, then added the account to the Administrators and Remote Desktop Users local groups. The adversary then set the account password to never expire. Additionally, the actor unsuccessfully attempted to modify the registry to enable inbound RDP connections.

Discovery

After the failed attempts to establish persistence and C2, NEMESIS KITTEN undertook host and user reconnaissance, which included efforts to locate Domain Controller-related information.

Credential Access

Finally, the actor attempted to perform credential harvesting by modifying the registry to enable WDigest and allow for the storage of credentials in plain text. The actor then attempted to use PowerShell, along with Rundll32, to launch `comsvcs.dll` with minidump and extract contents of Local Security Authority Subsystem Service (LSASS). This attempt proved unsuccessful as well, thanks to the advanced capabilities of the Falcon sensor.
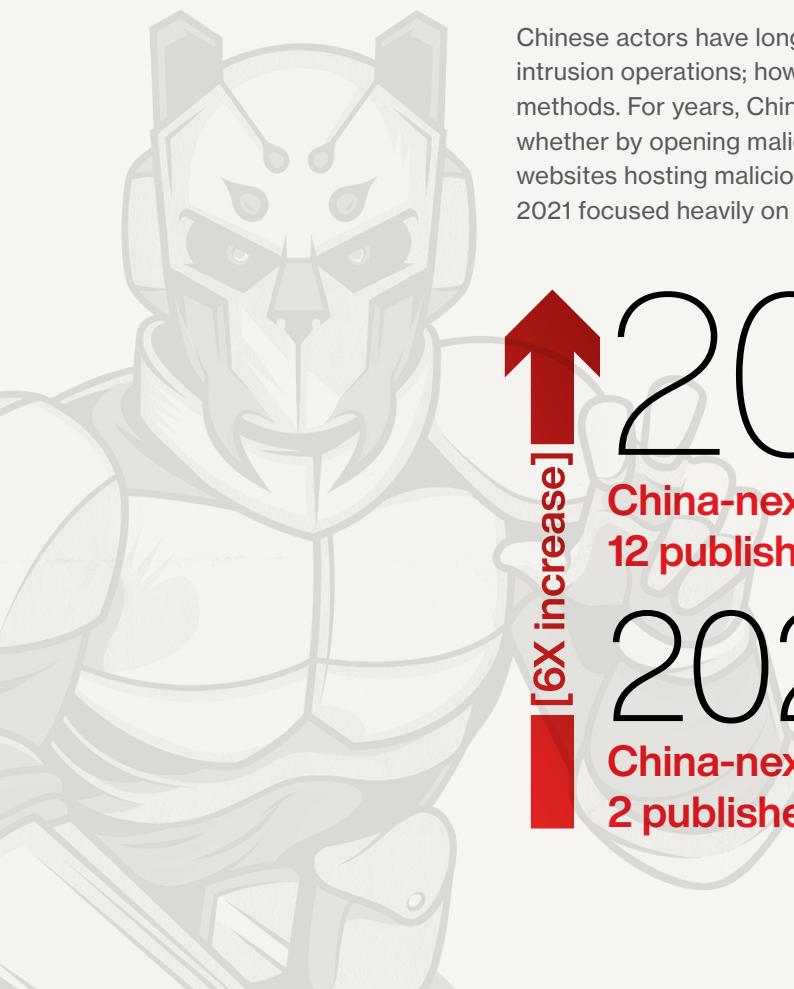
2021 Themes

China Emerges as Leader in Vulnerability Exploitation

CrowdStrike Intelligence observed China-nexus actors deploying exploits for new vulnerabilities at a significantly elevated rate in 2021, when compared to 2020.

In 2020, CrowdStrike Intelligence confirmed the exploitation by China-nexus actors — including WICKED PANDA — of two vulnerabilities published in 2020: CVE-2020-14882 (Oracle WebLogic) and CVE-2020-10189 (Zoho ManageEngine). In 2021, CrowdStrike Intelligence confirmed China-nexus actor exploitation of 12 vulnerabilities published in 2021, affecting nine different products. Ten named adversaries or activity clusters were linked to the exploitation of these vulnerabilities and a number of other incidents were identified in which activity was likely linked to unnamed Chinese actors.

Chinese actors have long developed and deployed exploits to facilitate targeted intrusion operations; however, 2021 highlighted a shift in their preferred exploitation methods. For years, Chinese actors relied on exploits that required user interaction, whether by opening malicious documents or other files attached to emails or visiting websites hosting malicious code. In contrast, exploits deployed by these actors in 2021 focused heavily on vulnerabilities in internet-facing devices or services.

[6X increase]

2021
China-nexus actors exploited 12 published vulnerabilities

2020
China-nexus actors exploited 2 published vulnerabilities
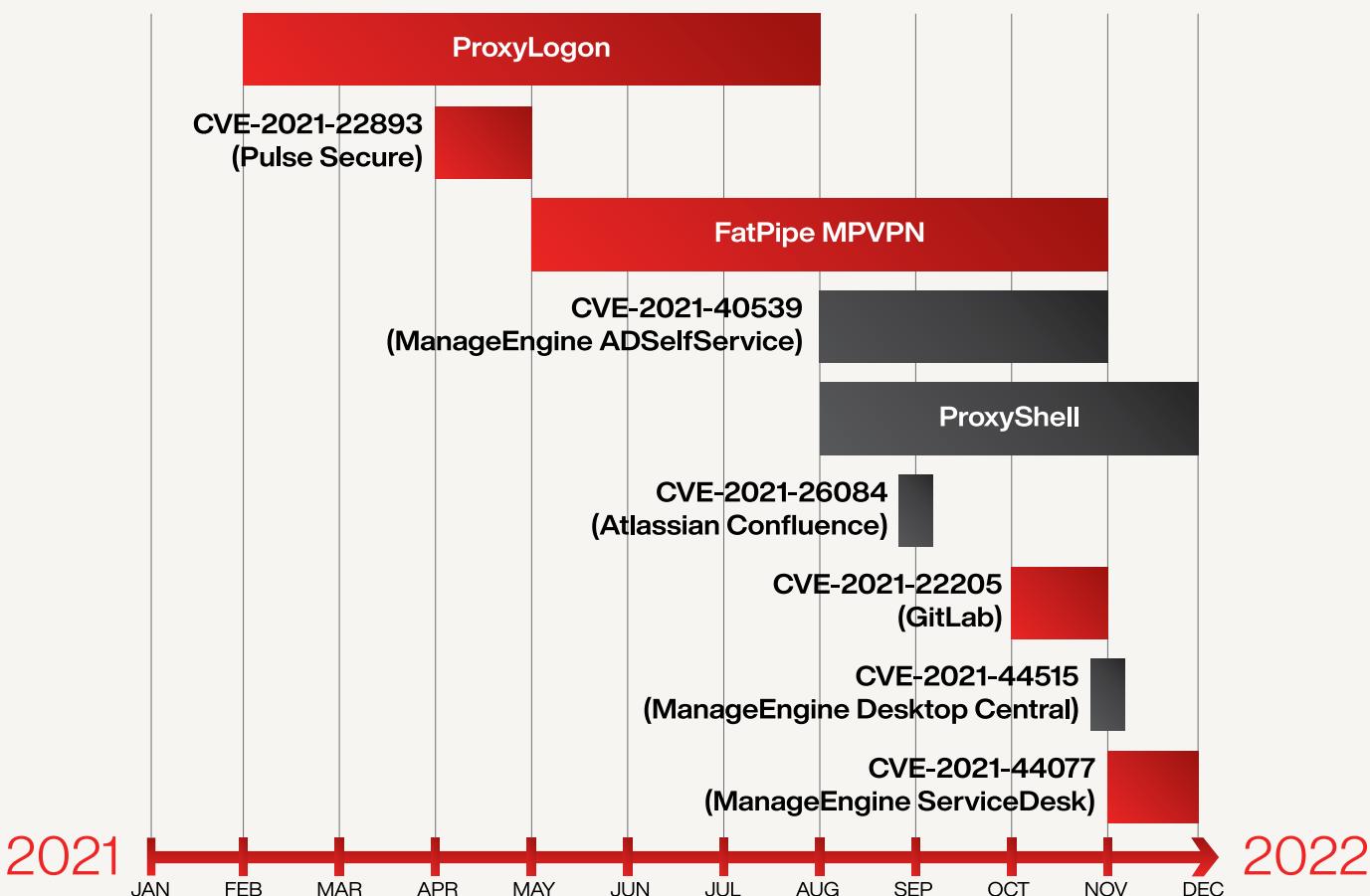
2021 Themes
China Emerges as Leader in Vulnerability Exploitation

In 2021, Chinese actors focused significant attention on a series of vulnerabilities in Microsoft Exchange — now collectively known as ProxyLogon and ProxyShell — and used them to launch intrusions against numerous organizations worldwide. Chinese adversaries also continued to exploit internet-routing products such as VPNs and routers for both infrastructure acquisition and initial access purposes. Enterprise software products hosted on internet-facing servers were also popular targets. CrowdStrike Intelligence observed Chinese actors exploit products for initial access in a range of intrusions such as Zoho ManageEngine, Atlassian Confluence and GitLab.[1]

Activity from China-nexus actors in 2021 highlighted their range of exploit-acquisition capabilities. Chinese targeted intrusion actors likely independently developed a number of the observed exploits or acquired them from in-country security researchers. In particular, the Tianfu Cup hacking competition demonstrates the significant exploitation development talent within China's hacker community. Exploits submitted at the Tianfu Cup have later been acquired by Chinese targeted intrusion actors for use in their operations. In several 2021 incidents, Chinese actors demonstrated an ability to rapidly operationalize public proof-of-concept (POC) exploit code for newly acknowledged vulnerabilities.


Figure 4. Timeline of Zero-day Exploits Deployed by China-nexus Actors in 2021

[1] Relevant zero-day vulnerabilities exploited in connection to this activity affected Zoho ManageEngine (CVE-2021-40539, CVE-2021-44515 and CVE-2021-440077), Atlassian Confluence (CVE-2021-26084) and GitLab (CVE-2021-22205)

Falcon OverWatch
Case Study

Suspected PANDA Exploits Microsoft Exchange Server Vulnerabilities Against Think Tank

Falcon OverWatch uncovered a targeted threat actor conducting a hands-on intrusion against a Europe-based think tank. The activity, which spanned multiple Windows-based hosts, began after the successful exploitation of a known Microsoft Exchange vulnerability. The adversary employed several notable TTPs in an effort to secure a persistent foothold in the victim environment. The adversary also showed a particular interest in gathering credential information, using four distinct credential dumping and harvesting techniques.

Initial Access

The adversary gained initial access to the primary host following the successful compromise of the Microsoft Exchange application pool `MSExchangeOWAAppPool`. OverWatch hunters promptly discovered this malicious access after seeing the Microsoft IIS worker process `w3wp.exe` writing an unknown executable on the host, with malicious scripts being written to a web directory. This activity included command execution indicative of China Chopper web shell usage, triggering an initial Falcon detection.

Discovery

Initial access was immediately followed by attempts at broad host- and user-based reconnaissance operations.

Execution

Operating as the SYSTEM user, the adversary deployed multiple instances of the China Chopper web shell and attempted to execute them via PowerShell beneath the IIS worker process `w3wp.exe`, but they were immediately detected by the Falcon sensor. The adversary was largely unsuccessful in their efforts to bypass existing controls by deploying several renamed versions of the Microsoft Windows command shell to execute further malicious tasking.

Persistence and Lateral Movement

In a likely attempt to preserve access in case the web shells were made unavailable, the adversary also deployed implants across several hosts and attempted execution using trusted utilities including the Microsoft .NET ClickOne Launch Utility and Rundll32. The adversary was able to use Rundll32 to successfully load their implant `WmiAd.dll`, which was configured to beacon to an adversary-controlled IP. The adversary also configured a scheduled task to persist the implant execution by setting it to launch on host startup. The adversary then moved laterally, using compromised credentials to authenticate to three hosts of interest. They then copied their working implant file to the hosts and created a scheduled task to preserve access.

Credential Access

The adversary attempted multiple LOTL techniques to extract the contents of the LSASS memory space and seek credential information stored in files.

The second attempt involved the use of the Microsoft Sysinternals tool ProcDump. The third attempt saw the adversary leverage their own tooling, executing a loader that was then used to launch a probable credential dumping binary. Finally, the adversary used the `findstr` command to search for credential-related information contained in `.xml` files on a remote share.
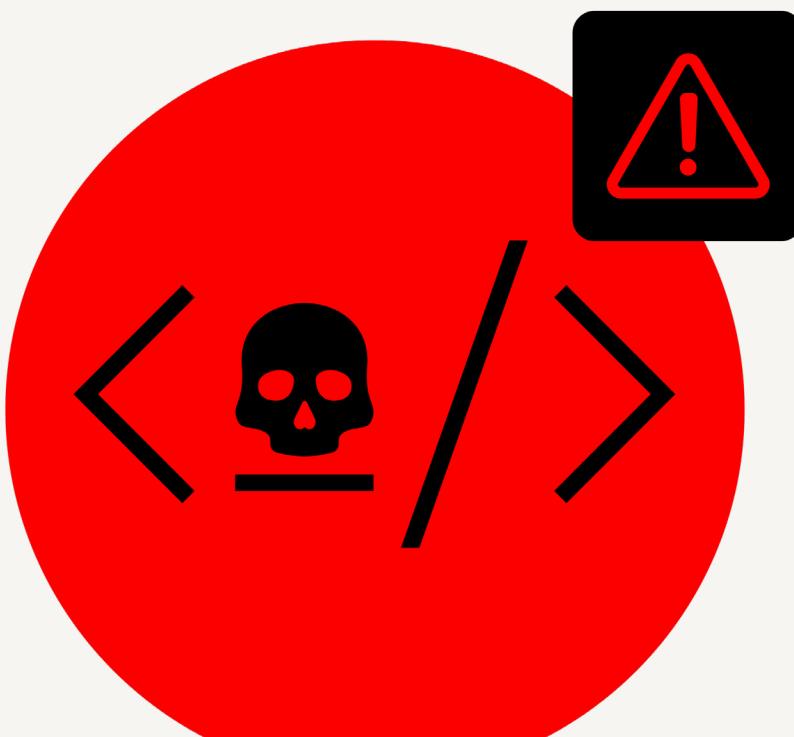
2021 Themes

Log4Shell Sets the Internet on Fire

Routine discovery, disclosure and subsequent exploitation of a series of high-profile vulnerabilities occurred throughout 2021. Due to the number of potentially affected endpoints, Log4Shell received more attention than any other vulnerability.
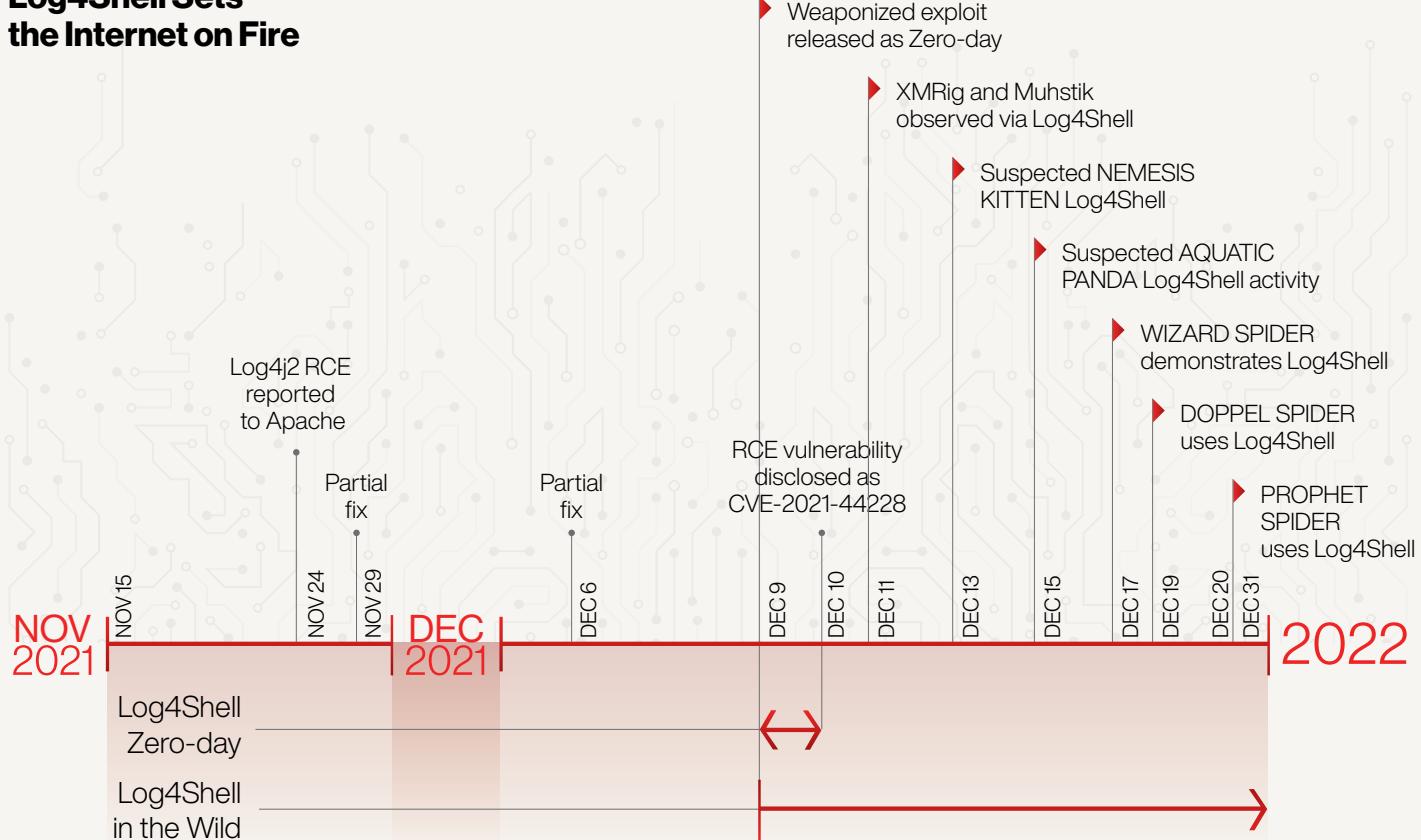
Apache's Log4j2 is an ubiquitous logging library used by many web applications. A vulnerability reported in November 2021 and tracked as CVE-2021-44228 and "Log4Shell" can be exploited by remote attackers to inject arbitrary Java code into affected services. Specially crafted requests may result in access to the system, delivery of malware or acquisition of sensitive data such as user credentials.

Between Dec. 9-31, 2021, a variety of groups incorporated Log4Shell exploitation into their arsenal (Figure 5). Opportunistic eCrime actors aggressively engaged in widespread Log4Shell exploitation most commonly affiliated with commodity botnet malware (e.g., *Muhstik*). However, other eCrime-focused actors — including affiliates of DOPPEL SPIDER and WIZARD SPIDER — adopted Log4Shell as an access vector to enable ransomware operations. Additionally, state-nexus actors, including NEMESIS KITTEN and AQUATIC PANDA, were also affiliated with probable Log4Shell exploitation before the end of 2021.

2021 Themes
## Log4Shell Sets the Internet on Fire

Figure 5. Timeline of Log4Shell Events and Affiliated Actors

The initial wave of opportunistic Log4Shell attacks was very simple, and each exploit was structured nearly identically. However, achieving reliable remote code execution (RCE) via CVE-2021-44228 on various impacted platforms potentially requires the actor to tailor the Log4Shell exploit for a specific target. While this adds effort, this tailoring has not prevented actors such as AQUATIC PANDA from leveraging more specific versions of CVE-2021-44228 exploits. In particular, CrowdStrike Intelligence and industry sources linked Log4Shell exploitation to the compromise of VMware products.

Due to the widespread nature of the Log4j2 logging library, it is difficult to assess which products are vulnerable and ensure they are protected against exploitation. Targeting of CVE-2021-44228 by criminal threat groups is increasing and will continue into 2022.

Many state-operated actors are likely to integrate Log4Shell exploits into their toolchain, since this logging library provides a method through which actors can gain access to target environments via vulnerable entry point systems or move laterally by exploiting internal servers on already compromised networks. This assessment is based on the vulnerability's massive prevalence. However, all impacted products cannot be exploited with the same technique, and tailoring of exploits for specific targets may be required.

CrowdStrike Intelligence assesses that actors will continue to integrate increasingly effective exploit chains to rapidly achieve RCE. This assessment is made with moderate confidence based on the substantial number of incidents facilitated by multistage exploit chains — such as ProxyShell and ProxyLogon — that proved commonplace during 2021.

→

STAY UP-TO-DATE ON LOG4SHELL
Visit the CrowdStrike Log4j/"Log4Shell" Vulnerability Learning Center.

Falcon OverWatch
Case Study

PROPHET SPIDER Leverages Log4j Exploit for Attempted Credential Harvesting from a Cloud Workspace Service

PROPHET SPIDER is a prolific access broker with a track record of successfully leveraging known vulnerabilities to gain access to web servers and cloud services in order to harvest credentials. OverWatch recently uncovered a hands-on intrusion against a U.S.-based financial services entity following the successful compromise of a VMware Horizon web component. Observed TTPs were consistent with those previously seen from PROPHET SPIDER and included the retrieval of tooling from an actor-controlled IP, along with host and domain reconnaissance.

C2 and Persistence

Upon initial access to the host, PROPHET SPIDER immediately leveraged obfuscated PowerShell to download a wget binary, which they then used to download a custom proxy tool. The suspicious PowerShell activity triggered an initial Falcon sensor detection, and OverWatch hunters created additional notifications on the actor's activity.

Discovery

PROPHET SPIDER performed host and active directory reconnaissance, including the enumeration of domain trust information along with active directory topology and replication status.

Execution and Discovery

PROPHET SPIDER used the Windows Command shell to launch their custom proxy tool, `winntaa.exe`. Once executed, they leveraged it to conduct more discovery operations, including gathering information on domain trusts and running processes.
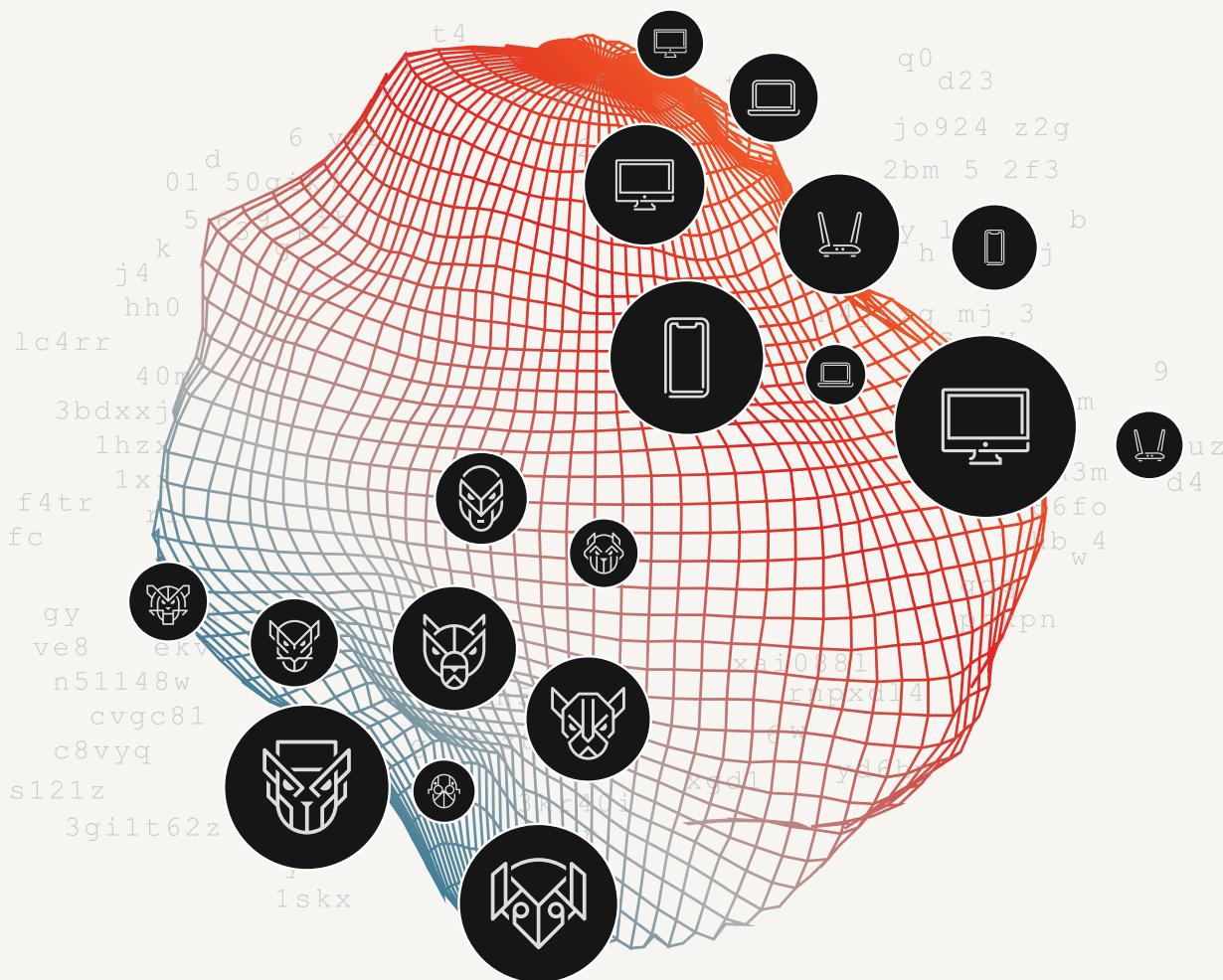
Defense Evasion

PROPHET SPIDER proceeded to delete their tooling from the host in an effort to prevent artifact recovery operations.

2021 Themes

Increasing Threats to Cloud Environments

Cloud-based services now form crucial elements of many business processes, easing file sharing and collaboration. However, these same services are increasingly abused by malicious actors in the course of computer network operations (CNO), a trend that is likely to continue in the foreseeable future as more businesses seek hybrid work environments. Common cloud attack vectors used by eCrime and targeted intrusion adversaries include cloud vulnerability exploitation, credential theft, cloud service provider abuse, use of cloud services for malware hosting and C2, and the exploitation of misconfigured image containers.

Cloud Vulnerability Exploitation

Malicious actors tend to opportunistically exploit known RCE vulnerabilities in server software, typically scanning for vulnerable servers without focusing on particular sectors or regions. After initial access, actors may deploy a variety of tools. Wider criminal exploitation of cloud services for initial access includes the exploitation of Accellion FTA vulnerabilities. Since January 2021, multiple companies have self-disclosed breaches related to the exploitation of such vulnerabilities.

VMware has also been targeted by threat actors, including CVE-2021-21972 — a critical vulnerability impacting VMware ESXi, vCenter Server and Cloud foundation products. Targeting this vulnerability provides a simple and reliable method for exploitation that threat actors can use across multiple host-operating systems, attack vectors and intrusion stages. Multiple adversaries, particularly BGH actors, have likely leveraged this vulnerability.

Credential Theft

Credential-based intrusions against cloud environments are among the more prevalent exploitation vectors used by eCrime and targeted intrusion adversaries. Criminal actors routinely host fake authentication pages to harvest legitimate authentication credentials for cloud services such as Microsoft Office 365 (O365), Okta or online webmail accounts. Actors then use these credentials to attempt to access victim accounts.
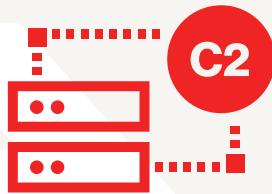
Access to cloud-hosted email or file-hosting services can also facilitate espionage and theft of information. In April 2021, CrowdStrike observed COSMIC WOLF targeting victim data stored within the Amazon Web Services (AWS) cloud environment. The adversary compromised the AWS environment via a stolen credential that allowed the operator to interact with AWS using the command line. Employing this technique, the adversary altered security group settings to allow direct SSH access from malicious infrastructure.

Cloud Service Provider Abuse

Adversaries have leveraged cloud service providers to abuse provider trust relationships and gain access to additional targets through lateral movement from enterprise authentication assets hosted on cloud infrastructure. If an adversary can elevate their privileges to global administrator levels, they may be able to pivot between related cloud tenants to further their access.

This issue is particularly significant if the initially targeted organization is a managed service provider (MSP). In this case, global administrator access can be used to take over support accounts used by the MSP to make changes to their customer networks, thereby creating multiple opportunities for vertical propagation to many more networks. This technique was used by COZY BEAR throughout 2020, with evidence of continued intrusion in MSP networks continuing into 2021.

Malware Hosting and Command and Control

Both eCrime and targeted intrusion adversaries extensively leverage legitimate cloud services to deliver malware; targeted actors also use these services for command and control. This tactic has the advantage of being able to evade signature-based detections, because top-level domains of cloud hosting services are typically trusted by many network scanning services. Using legitimate cloud services, including chat applications, can enable adversaries to evade some security controls by blending into normal network traffic. Moreover, using cloud-hosting providers for C2 allows the adversary to switch or remove payloads from an affiliated C2 URL with ease.

Exploitation of Misconfigured Image Containers

Criminal actors have periodically exploited improperly configured Docker containers. Docker images are templates used for creating containers. These images can be used either on a standalone basis, for users to directly interact with a tool or service, or as the parent to another application. Because of this hierarchical mode, if an image has been modified to contain malicious tooling, any container derived from it will also be infected.

In 2021, CrowdStrike Intelligence reported on the malware family *Doki*, which uses containers as both an initial infection vector and as a means for parallel track tasking. Once malicious actors gain access, they can abuse these escalated privileges to accomplish lateral movement and then proliferate throughout the network.

CrowdStrike Intelligence has also continued to track adversary operations involving the access and modification of constituent parts of Kubernetes clusters. Kubernetes is an open-source container-orchestration system that automates the deployment, scaling and management of applications and their associated shared resources. Falcon OverWatch has observed increasing adversary interest in Kubernetes clusters operating within corporate environments. The Kubernetes framework is a complex system comprising a number of constituent parts allowing ample opportunity for misconfiguration that could provide an adversary with initial access to one component and subsequent lateral propagation opportunities that provide access to desired resources.

Threat Highlight:
Russian Adversaries Look to the Cloud

FANCY BEAR

The FANCY BEAR adversary is associated with the 85th Main Center of the Special Services (aka Military Unit 26165) of Russia's Main Intelligence Directorate (GRU). Earlier in its operational lifespan, when conducting victim exploitation and credential collection, the adversary extensively used spear-phishing emails containing malicious documents or links that redirected to malicious infrastructure. However, after multiple exposures of its operations — particularly by the U.S. Department of Justice (DOJ) in 2018 — FANCY BEAR appears to have reevaluated their operational tradecraft and decreased their use of malware while shifting toward increased use of credential-harvesting tactics including both large-scale scanning techniques and victim-tailored phishing websites.

Credential harvesting plays a significant role in FANCY BEAR's acquisition of intelligence and primary access into target organizations or individuals. Adapting to the trend of public and private entities increasingly hosting parts of their internal infrastructure (e.g., email, internal chat, or identity and device-management services) via cloud services, the adversary has targeted numerous cloud-based email providers with a variety of collection methodologies throughout 2021. Examples of targeted email providers include enterprise services such as Microsoft 365 or GSuite, as well as webmail services more likely used by individuals. The adversary's credential-collection operations have technically matured over the years while maintaining a consistently high volume and tempo.

COZY BEAR

Throughout 2021, COZY BEAR also repeatedly demonstrated a high level of post-exploitation proficiency, particularly involving the enumeration of, and lateral movement within, cloud environments. During a CrowdStrike Services investigation, COZY BEAR operators were identified using authentication cookie theft to bypass multifactor authentication (MFA) restrictions implemented on target networks. This technique leverages existing local network access and has been used to access user accounts in possession of enterprise cloud service privileges. This technique highlights the adversary's ability to use a range of post-compromise activities to expand their access and maximize intelligence collection.

Future operations consistent with this cluster of COZY BEAR-associated activity are highly likely to continue mirroring this behavior, particularly through the successive identification and compromise of user accounts that are assigned administrative or special privileges on cloud services and tenants. This assessment is made with moderate confidence based on the increasing application of MFA restrictions on cloud service access and the consistency of COZY BEAR-related operations identified to date.

Conclusion

➡

CrowdStrike Intelligence
continues to provide
industry-leading actor
profiles, malware analysis
and campaign tracking
through its suite of
intelligence reporting
products and coverage of
threat landscapes.

In 2021, CrowdStrike Intelligence observed adversaries continue to adapt to security environments impacted by the ongoing COVID pandemic. These adversaries are likely to look at novel ways in which they can bypass security measures to conduct successful initial infections, impede analysis by researchers and continue tried-and-tested techniques into 2022.

BGH operations will continue to dominate the eCrime landscape in 2022, likely significantly increasing their use of ransomware from ransomware-as-a-service (RaaS) operations in an effort to allow for a wider array of adversarial skill sets. The access broker market will also continue as an avenue for ransomware operators to gain victims, removing the initial access step and allowing swifter deployment of malware.

Targeted intrusion adversaries are expected to continue to capitalize on trends in technology and the broader threat landscape throughout 2022 in attempts to maximize impacts while minimizing effort. (In 2021, this behavior was reflected in Iran's shift to disruptive ransomware, China's emphasis on vulnerability exploitation — often at scale — to achieve initial access to victims, and Russia's targeting of cloud service providers and environments.) Cloud-related threats are particularly likely to become more prevalent and to evolve, given that targeted intrusion adversaries are expected to continue prioritizing targets that provide direct access to large consolidated stores of high-value data.

As today's world continues to increasingly rely on mobile devices, some adversaries will continue to diversify their tool arsenal to include mobile malware — either to make money and/or collect sensitive information. Similarly, adversaries will continue to seek weaknesses in platforms used by their targets in 2022; opportunities to exploit vulnerabilities will be capitalized upon once they are discovered. Through the coming year, adversaries are expected to continue to react to vulnerability identification and seek to gain access to their targets through exploitive means as quickly as possible.

In response to these evolving threats, CrowdStrike Intelligence continues to provide industry-leading actor profiles, malware analysis and campaign tracking through its suite of reporting products and coverage of threat landscapes spanning targeted intrusion, eCrime, hacktivist, vulnerability and mobile threat intelligence.

Recommendations

01

Protect All Workloads

An organization is only secure if every asset is protected. You must secure all critical areas of enterprise risk: endpoints and cloud workloads, identity and data. Look for solutions that deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Establish strong IT hygiene with an asset inventory and consistent vulnerability management. Remember, it's impossible to defend systems you don't know are there.

02

Know Your Adversary

There is a human behind every cyberattack. If you know the adversaries that target the industry or the geolocation your organization resides in, you can prepare yourself to better defend against the tools and tactics they employ. CrowdStrike Falcon X intelligence identifies today's bad actors and exposes their playbook to enable security teams to proactively optimize preventions, strengthen defenses and accelerate incident response.

03

Be Ready When Every Second Counts

Speed often dictates success or failure. It's especially true in cybersecurity where stealthy breaches can occur in a matter of hours with devastating consequences. Security teams of all sizes must invest in speed and agility for their daily and tactical decision making by automating preventive, detection, investigative and response workflows with integrated cyber threat intelligence directly observed from the front lines.

04

Stop Modern Attacks

Nearly 80% of cyberattacks leverage identity-based attacks to compromise legitimate credentials and use techniques like lateral movement to quickly evade detection. CrowdStrike Falcon Identity Threat Protection enables hyper-accurate threat detection and real-time prevention of identity-based attacks, combining the power of advanced AI, behavioral analytics and a flexible policy engine to enforce risk-based conditional access.

05 Adopt Zero Trust

As adversaries want to monetize their activity, they target their victim's data seeking payoffs through ransom and extortion, and will even auction data to the highest bidder. Because today's global economy requires data to be accessible from anywhere at any time, it is critical to adopt a Zero Trust model. The CrowdStrike Zero Trust solution connects the machine to the identity and the data to deliver full Zero Trust protection.

06 Monitor the Criminal Underground

Adversaries congregate to collaborate using a variety of hidden messaging platforms and dark web forums. In addition to monitoring your own environment, security teams must be vigilant and monitor activity within the criminal underground. Leverage digital risk monitoring tools like Falcon X Recon to monitor imminent threats to your brand, identities or data. Get advance warnings of active threats and use this visibility to prevent data leak incidents and costly ransomware attacks.

07 Eliminate Misconfigurations

The most common causes of cloud intrusions continue to be human errors such as omissions introduced during common administrative activities. It's important to set up new infrastructure with default patterns that make secure operations easy to adopt. This strategy ensures that new accounts are set up in a predictable manner, eliminating common sources of human error. Also, make sure to set up roles and network security groups that keep developers and operators from needing to build their own security profiles and accidentally doing it poorly.

08 Invest in Elite Threat Hunting

CrowdStrike has observed that 62% of attacks comprise non-malware, hands-on-keyboard activity. As adversaries advance their tradecraft in this manner to bypass legacy security solutions, autonomous machine learning alone is not good enough to stop dedicated attackers. The combination of technology with expert threat hunters is absolutely mandatory to see and stop the most sophisticated threats. Top-quality managed services such as Falcon Complete and Falcon OverWatch can help you close the growing cyber skills gap with the expertise, resources and coverage needed to augment your team.

09 Build a Cybersecurity Culture

While technology is clearly critical in the fight to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs table top exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

About CrowdStrike

CrowdStrike Holdings, Inc. (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/

CrowdStrike
Products
and Services

➜ Endpoint Security

FALCON XDR™ | EXTENDED DETECTION AND RESPONSE (XDR)
Supercharges detection and response across your entire security stack by synthesizing multi-domain telemetry in one unified, threat-centric command console

FALCON INSIGHT™ | ENDPOINT DETECTION AND RESPONSE (EDR)
Delivers continuous, comprehensive endpoint visibility and automatically detects and intelligently prioritizes malicious activity to ensure nothing is missed and potential breaches are stopped

FALCON PREVENT™ | NEXT-GENERATION ANTIVIRUS
Protects against all types of threats, from malware and ransomware to sophisticated attacks, and deploys in minutes, immediately protecting your endpoints

FALCON FIREWALL MANAGEMENT™ | HOST FIREWALL
Delivers simple, centralized host firewall management, making it easy to manage and control host firewall policies

FALCON DEVICE CONTROL™ | USB DEVICE VISIBILITY AND CONTROL
Provides the visibility and precise control required to enable safe usage of USB devices across your organization

→ Threat Intelligence

FALCON X™ | AUTOMATED INTELLIGENCE

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

FALCON X 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

FALCON X RECON™ | DIGITAL RISK MONITORING

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

FALCON SANDBOX™ | MALWARE ANALYSIS

Uncovers the full malware attack lifecycle with in-depth insight into all file, network, memory and process activity, and provides easy-to-understand reports, actionable IOCs and seamless integration

→ Managed Services

FALCON OVERWATCH™ | MANAGED THREAT HUNTING

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

FALCON COMPLETE™ | MANAGED DETECTION AND RESPONSE (MDR)

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

Cloud Security

FALCON CLOUD WORKLOAD PROTECTION™

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

FALCON HORIZON™ | CLOUD SECURITY POSTURE MANAGEMENT

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

→ Security and IT Operations

FALCON DISCOVER™ | IT HYGIENE

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

FALCON SPOTLIGHT™ | VULNERABILITY MANAGEMENT

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

FALCON FILEVANTAGE™ | FILE INTEGRITY MONITORING

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

FALCON FORENSICS™ | FORENSIC CYBERSECURITY

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

→ Identity Protection

FALCON IDENTITY THREAT DETECTION

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

FALCON IDENTITY THREAT PROTECTION

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

→ Log Management

HUMIO | OBSERVABILITY AND LOG MANAGEMENT

Humio offers an advanced, purpose-built log management platform that lets organizations log everything to answer anything in real time. Humio enables complete observability for all streaming logs and event data, and helps better prepare for the unknown by making it easy to explore and find the root cause of any incident.

→ Services

CROWDSTRIKE SERVICES | IR AND PROACTIVE

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