Scanned with OKEN Scanner

Foreword

The 2024 edition of the CrowdStrike Global Threat Report arrives at a pivotal moment for our global community of protectors. The speed and ferocity of cyberattacks continue to accelerate as adversaries compress the time between initial entry, lateral movement and breach. At the same time, the rise of generative AI has the potential to lower the barrier of entry for low-skilled adversaries, making it easier to launch attacks that are more sophisticated and state of the art.

These trends are driving a tectonic shift in the security landscape and the world. The "good enough" approach to cybersecurity is simply no longer good enough for modern threats. As organizations increasingly move business to the cloud, adversaries are advancing their capabilities to exploit this, and abuse features unique to the cloud. We continue to see identity-based attacks take center stage, as adversaries focus on social engineering attacks that bypass multifactor authentication. The use of legitimate tools to execute an attack, an increasingly prevalent technique, impedes the ability to differentiate between normal activity and a breach.

We are entering an era of a cyber arms race where AI will amplify the impact for both the security professional and the adversary. Organizations cannot afford to fall behind, and the legacy technology of yesterday is no match for the speed and sophistication of the modern adversary.

With the release of the CrowdStrike 2024 Global Threat Report, our elite Counter Adversary Operations team is delivering the actionable intelligence you need to stay ahead of today's threats and secure your future. This year's report provides critical insight and observations into adversary activity, including:

- The tactics and techniques that adversaries use to exploit gaps in cloud protection
- The continued exploitation of stolen identity credentials and increasingly sophisticated methods adversaries use to gain initial access
- The growing menace of supply chain attacks and exploitation of trusted software to maximize the ROI of attacks
- The potential for adversaries to target global elections in a year that has the potential to transform geopolitics around the world for the near future

Scanned with OKEN Scanner

From Day One, CrowdStrike has said, "You don't have a malware problem, you have an adversary problem." We pioneered the concept of adversary-focused cybersecurity because it's the best way to protect customers and stop breaches. We know the adversary better than anyone, and we use this insight to guide our innovation, protect customers, stop breaches and increase the cost to the adversary.

A secure future requires a strong foundation. This is what we're delivering with the AI-native CrowdStrike Falcon® XDR platform. We're driving the convergence of data, cybersecurity and IT, with generative AI and workflow automation built natively within a single, unified platform to give you and your teams the speed you need to beat the adversary.

I hope you find the CrowdStrike 2024 Global Threat Report informative and inspiring in our shared fight against the adversary. CrowdStrike will remain unrelenting in our mission to deliver the security outcome you need most: stopping the breach.

George Kurtz
CrowdStrike CEO/Co-Founder

Scanned with OKEN Scanner

Table of Contents

Introduction 5

Naming Conventions 8

Threat Landscape Overview 9

2023 Themes 13

Identity-Based and Social Engineering Attacks 13

Adversaries Continue to Develop Cloud-Consciousness 17

Third-Party Relationship Exploitation 20

Vulnerability Landscape: "Under the Radar" Exploitation 24

2023 Israel-Hamas Conflict: Cyber Operations Focus on Disruption and Influence 25

Threats on the 2024 Horizon 32

eCrime Landscape 38

Big Game Hunting 39

eCrime Enablers 45

Targeted eCrime 48

Conclusion 52

Recommendations 54

CrowdStrike Products and Services 56

About CrowdStrike 61

Scanned with OKEN Scanner

Introduction

As we reflect on the 2023 cyber threat landscape, the theme of stealth prevails. Adversaries have faced a hardening attack surface thanks to advancements in threat defense technology and threat awareness, and they have responded by increasingly adopting and relying on techniques that empower them to move faster and evade detection.

These techniques are evident in the consistent prevalence of eCrime, a highly attractive and lucrative business venture for many criminals. Unsurprisingly, eCrime persisted as the most pervasive threat across the 2023 threat landscape as adversaries leveraged techniques to maximize stealth, speed and impact.

While ransomware remains the tool of choice for many big game hunting (BGH) adversaries, data-theft extortion continues to be an attractive — and often easier — monetization route, as evidenced by the 76% increase in the number of victims named on BGH dedicated leak sites (DLSs) between 2022 and 2023. Access brokers continued to profit by providing initial access to eCrime threat actors throughout the year, with the number of advertised accesses increasing by 20% from 2022.

Nation-state adversaries were also active throughout 2023. China-nexus adversaries continued to operate at an unmatched pace across the global landscape, leveraging stealth and scale to collect targeted group surveillance data, strategic intelligence and intellectual property.

In other areas of the world, conflict continued to drive nation-state and hacktivist adversary activity. In 2023, as the Russia-Ukraine war entered its second year, Russia-nexus adversaries and activity clusters maintained high, sustained levels of activity in support of Russian Intelligence Service intelligence collection, disruptive activity, and information operations (IO) targeting Ukraine and NATO countries.

DATA-THEFT EXTORTION CONTINUES TO BE AN ATTRACTIVE – AND OFTEN EASIER – MONETIZATION ROUTE, AS EVIDENCED BY THE 76% INCREASE IN THE NUMBER OF VICTIMS NAMED ON BGH DEDICATED LEAK SITES

Scanned with OKEN Scanner

Iran-nexus adversaries and Middle East hacktivist adversaries were also observed pivoting cyber operations in the latter half of the year in alignment with kinetic operations stemming from the 2023 Israel-Hamas conflict.

North Korean adversaries maintained a consistently high tempo throughout 2023. Their activity continued to focus on financial gain via cryptocurrency theft and intelligence collection from South Korean and Western organizations, specifically in the academic, aerospace, defense, government, manufacturing, media and technology sectors.

Across the rest of the world, stealth played a key role in adversary activity focused on digital surveillance, information collection and control in support of government agendas. The assessed geographic range of this activity, as well as the capabilities and target scope of global threat actors, continued to underscore the extent to which targeted intrusion capabilities have proliferated beyond those demonstrated by commonly reported countries. In some cases, this activity was assisted by private sector offensive actors and openly available adversary emulation frameworks.

One of the greatest threat actor motivations driving stealth in cyber threat operations is CrowdStrike's development of new products and partnerships throughout 2023. These changed the stakes within the operational landscape and left adversaries with no place to hide.

In 2023, CrowdStrike Falcon® Intelligence and CrowdStrike® Falcon OverWatch™ merged to become CrowdStrike Counter Adversary Operations (CAO). Combining the power of threat intelligence with the speed of dedicated hunting teams and trillions of cutting-edge telemetry events from the AI-native CrowdStrike Falcon® platform that detect, disrupt and stop today's sophisticated adversaries, this merger has exponentially raised the business cost of conducting cyberattacks. In 2024, CrowdStrike CAO repackaged CrowdStrike's threat intelligence modules to add managed threat hunting (an industry first), empowering organizations to better pursue adversaries and stop breaches.

Over the course of 2023, CrowdStrike CAO introduced 34 new adversaries — including a newly tracked, Egypt-based adversary, WATCHFUL SPHINX — raising the total number of actors tracked across all motivations to 232. In addition to named adversaries, CrowdStrike CAO tracks more than 130 active malicious activity clusters.

CrowdStrike CAO drives unparalleled, actionable reporting coverage that captures new cyber threat developments in real time and identifies and tracks new adversaries. The CrowdStrike 2024 Global Threat Report sheds light on the standout trends from last year, how adversaries' activities and motivations are evolving and the ways CrowdStrike anticipates the threat landscape will evolve in the coming year.

OVER THE COURSE OF 2023, CROWDSTRIKE CAO INTRODUCED 34 NEW ADVERSARIES – INCLUDING A NEWLY TRACKED, EGYPT-BASED ADVERSARY, WATCHFUL SPHINX – RAISING THE TOTAL NUMBER OF ACTORS TRACKED ACROSS ALL MOTIVATIONS TO 232. IN ADDITION TO NAMED ADVERSARIES, CROWDSTRIKE CAO TRACKS MORE THAN 130 ACTIVE MALICIOUS ACTIVITY CLUSTERS.

Scanned with OKEN Scanner

CrowdStrike CAO Innovations

THE CROWDSTRIKE CAO TEAM PUTS RAPID INSIGHTS INTO THE HANDS OF FRONT-LINE TEAMS SO THEY CAN DISRUPT ADVERSARIES FASTER THAN EVER BEFORE.

IN THE FALL OF 2023, CROWDSTRIKE CAO ROLLED OUT AN IDENTITY THREAT HUNTING CAPABILITY, PAIRING THE LATEST INTELLIGENCE ON ADVERSARY MOTIVES AND TACTICS, TECHNIQUES AND PROCEDURES (TTPS) WITH CROWDSTRIKE FALCON® IDENTITY THREAT PROTECTION AND ELITE CAO THREAT HUNTERS TO QUICKLY IDENTIFY AND REMEDIATE COMPROMISED CREDENTIALS, TRACK LATERAL MOVEMENT AND STAY AHEAD OF ADVERSARIES WITH 24/7 COVERAGE.

AND WHILE THE CAO TEAM HUNTS FOR ADVERSARY ACTIVITY INSIDE CUSTOMER ORGANIZATIONS, THE NEW CAO "EXTERNAL ATTACK SURFACE EXPLORE" CAPABILITY ENABLES CUSTOMERS TO HUNT FOR AND EXAMINE ADVERSARY INFRASTRUCTURE.

CROWDSTRIKE MADE KEY INVESTMENTS IN AUTOMATION IN 2023, HELPING CUSTOMERS IMMEDIATELY TAKE ACTION ON CAO-IDENTIFIED THREATS. VIA FALCON IDENTITY THREAT PROTECTION, CROWDSTRIKE INTRODUCED NEW AUTOMATED WORKFLOWS FOR RESETTING CUSTOMER PASSWORDS EXPOSED ON THE CRIMINAL UNDERGROUND; ONE-CLICK TYPOSQUATTING DOMAIN BLOCKING AND TAKEDOWN; AND NEW CROWDSTRIKE FALCON® FUSION PLAYBOOKS FOR AUTOMATIC INDICATORS OF COMPROMISE (IOCS) RESULTING FROM TYPOSQUATTING THREATS AND THIRD-PARTY SYSTEM INTEGRATION. THESE NEW ENHANCEMENTS ALLOW USERS TO QUICKLY RESPOND TO THREATS THROUGHOUT THEIR SECURITY WORKFLOWS.

THE NEW CROWDSTRIKE CAO MODULES – CROWDSTRIKE FALCON® ADVERSARY OVERWATCH™, CROWDSTRIKE FALCON® ADVERSARY INTELLIGENCE AND CROWDSTRIKE FALCON® ADVERSARY HUNTER – HAVE LINKED THREAT HUNTING EVEN MORE CLOSELY TO THEIR INTELLIGENCE CAPABILITIES, UNIFYING THE USER EXPERIENCE SO CUSTOMERS CAN EASILY LEVERAGE A SINGLE, CONSISTENT USER INTERFACE TO VIEW CRUCIAL INFORMATION ACROSS ALL CAO CAPABILITIES.

CROWDSTRIKE CUSTOMERS ALSO BENEFIT FROM ENHANCED CONTEXT AROUND OBSERVABLES, NEW INDICATOR OF ATTACK (IOA) INTEGRATIONS TO ACCELERATE SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) DETECTION AND RESPONSE, THREAT HUNTING WORKFLOWS THAT WILL MORE EFFECTIVELY IDENTIFY ENVIRONMENTAL THREATS, AND IMPROVEMENTS TO DATA UNIFICATION AND LINKAGE ACROSS THE FALCON PLATFORM AND THIRD-PARTY APPLICATIONS.

Scanned with OKEN Scanner

NAMING CONVENTIONS

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

Scanned with OKEN Scanner

Threat Landscape Overview

year over year = (YoY)

34 new adversaries tracked by CrowdStrike, raising the total to **232**

Cloud-conscious cases increased by **110% YoY**

Cloud environment intrusions increased by **75% YoY**

76% YoY increase in victims named on eCrime dedicated leak sites

84% of adversary-attributed cloud-conscious intrusions were focused on eCrime

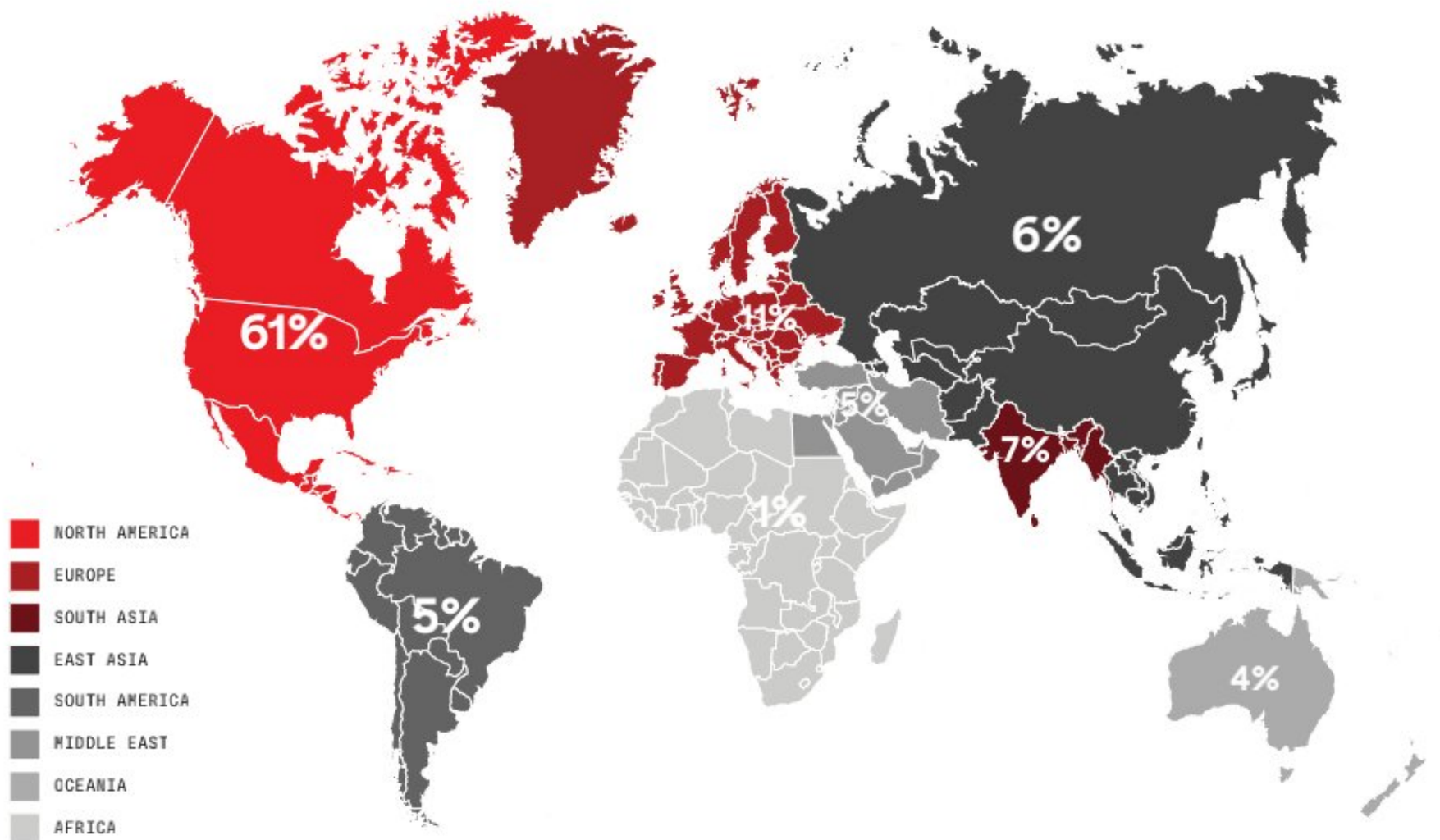
Scanned with OKEN Scanner

Today's cyber threats are particularly alarming due to the widespread use of hands-on or "interactive intrusion" techniques, which involve adversaries actively executing actions on a host to accomplish their objectives. Unlike malware attacks that depend on the deployment of malicious tooling and scripts, interactive intrusions leverage the creativity and problem-solving skills of human adversaries. These individuals can mimic expected user and administrator behavior, making it difficult for defenders to differentiate between legitimate user activity and a cyberattack.

In 2023, CrowdStrike observed a 60% year-over-year increase in the number of interactive intrusion campaigns, with a 73% increase in the second half compared to 2022.

The technology sector was the most frequently targeted industry in which CrowdStrike CAO observed interactive intrusion activity in 2023, a continuing trend from 2022. The charts below reflect the relative frequency of intrusions in the top 10 industry verticals and in geographical regions.

Interactive Intrusions by Region



Interactive Intrusions by Industry

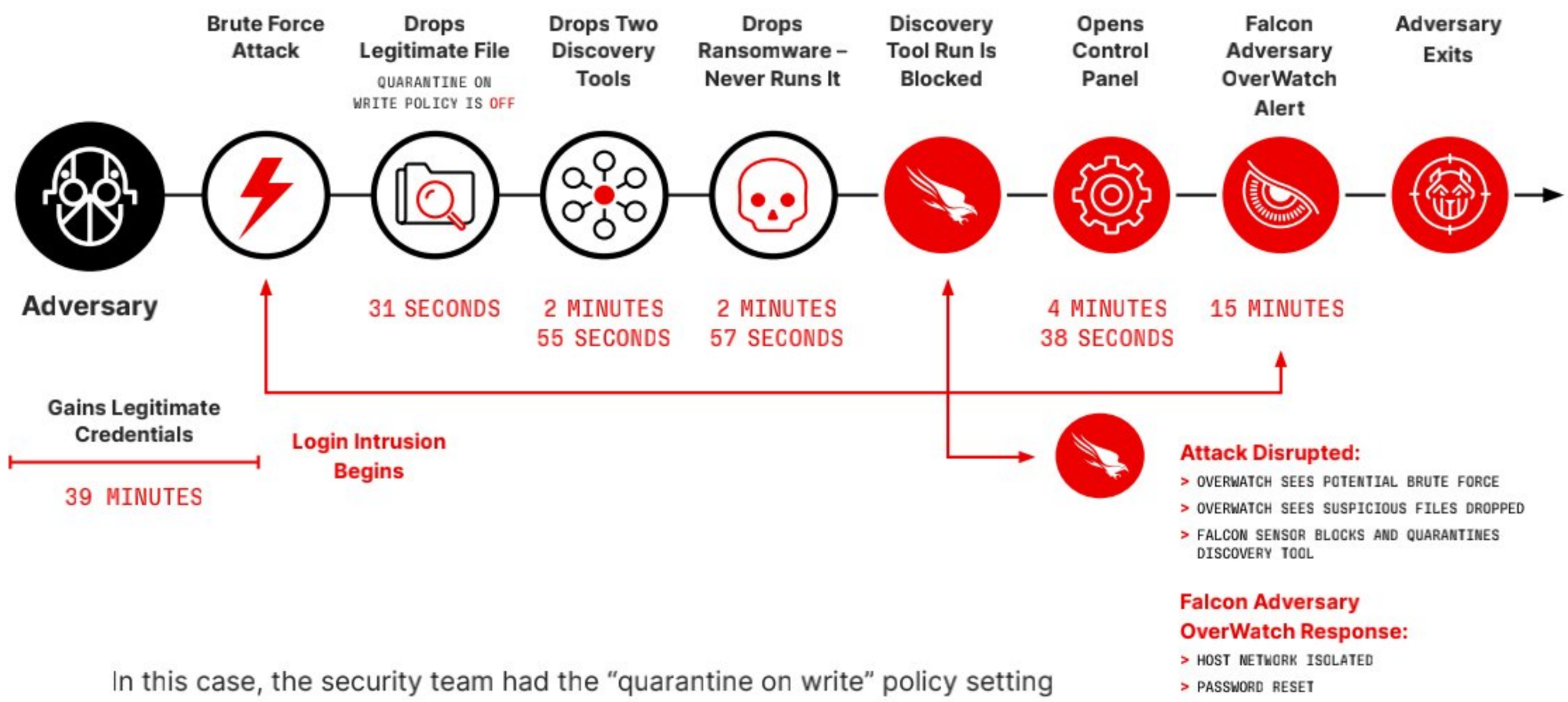
After gaining initial access to a network, adversaries seek to "break out" and move laterally from the compromised host to other hosts within the environment. The time it takes for them to do this — "breakout time" — is crucial because the initially compromised machines are rarely the ones adversaries need to achieve their goals. They must move laterally into the network, conduct reconnaissance, establish persistence and locate their targets. Responding within the breakout time window allows defenders to mitigate costs and other damages associated with intrusions.

This year, the average breakout time for interactive eCrime intrusion activity decreased from 84 minutes in 2022 to 62 minutes in 2023. The fastest observed breakout time was only 2 minutes and 7 seconds.

Scanned with OKEN Scanner

Anatomy of an eCrime Interactive Intrusion

To gain a better understanding of interactive intrusions, the following timeline illustrates the speed of a real-world hands-on attack:



In this case, the security team had the "quarantine on write" policy setting disabled, enabling the four files to be written to disk. The adversary executed a legitimate tool to obtain system information for reconnaissance and then dropped three more files, including ransomware, onto the system. They attempted to execute a network discovery and reconnaissance tool to map out lateral movement options, which was immediately blocked and quarantined by the Falcon sensor. This caused the adversary to open the control panel to understand which security tool was in use. When they identified the Falcon platform, they never attempted to execute the second discovery tool or the ransomware (which would have been prevented and quarantined) and moved to another victim. Within minutes, CrowdStrike CAO threat hunters notified the customer, took the machine offline and reset the user password.

Once an initial compromise occurs, it only takes seconds for adversaries to drop tools and/or malware on a victim's environment during an interactive intrusion. However, the saying "time is money" holds true for adversaries. More than 88% of the attack time was dedicated to breaking in and gaining initial access. By reducing or eliminating this time, adversaries free up resources to conduct more attacks.

To do this, they have continued to move beyond malware to faster, more effective means such as identity attacks (phishing, social engineering and access brokers) and the exploitation of vulnerabilities and trusted relationships. This trend is apparent over the last five years, as malware-free activity represented 75% of detections in 2023 — up from 71% in 2022.

MALWARE-FREE ACTIVITY

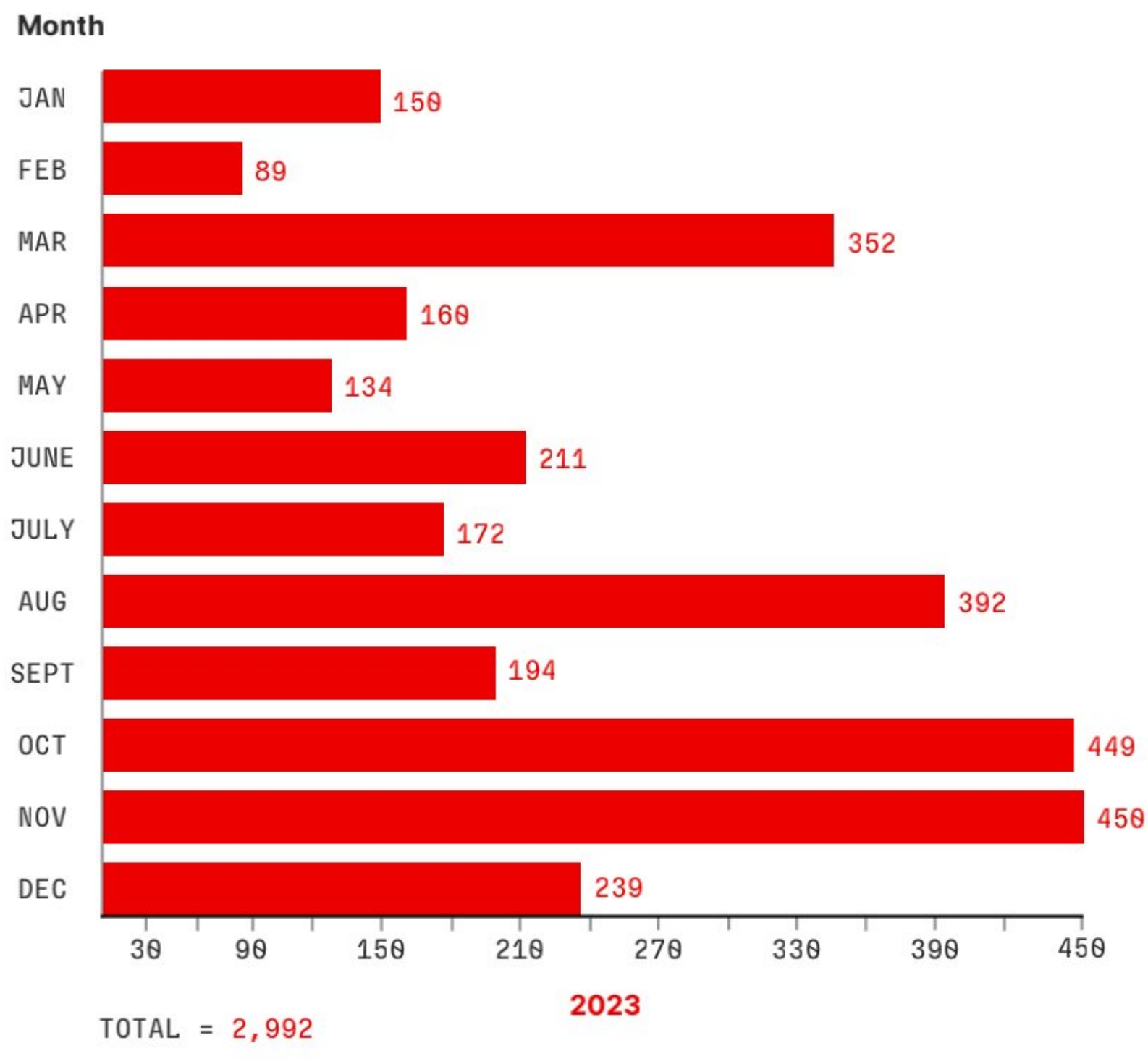
»

75% 2023
71% 2022
62% 2021
51% 2020
40% 2019

Scanned with OKEN Scanner

This trend is partly related to the success of identity attacks, access brokers and the prolific abuse of valid credentials to facilitate access and persistence in victim environments. Access brokers are threat actors who acquire access to organizations and provide or sell this access to other actors, including ransomware operators. These adversaries continued to profit from providing initial access to a variety of eCrime threat actors in 2023, with the number of accesses advertised increasing by almost 20% compared to 2022.

Access Broker Advertisements by Month



Today's sophisticated cyberattacks only take minutes to succeed. Adversaries use techniques such as interactive hands-on-keyboard attacks and legitimate tools to attempt to hide from detection. To further accelerate attack tempo, adversaries can access credentials in multiple ways, including purchasing them from access brokers for a few hundred dollars. Organizations must prioritize protecting identities in 2024.

Scanned with OKEN Scanner

2023 Themes

IDENTITY-BASED AND SOCIAL ENGINEERING ATTACKS

Adversaries spanning multiple motivations and regions continue to use phishing techniques spoofing legitimate users to target valid accounts, as well as other authentication and identifying data, to conduct their attacks. In addition to stealing account credentials, CrowdStrike CAO observed adversaries targeting API keys and secrets, session cookies and tokens, one-time passwords (OTPs) and Kerberos tickets throughout 2023.

Scanned with OKEN Scanner

ACCOUNT CREDENTIALS

Adversaries can authenticate to a system and/or user account using stolen credentials, which can either be obtained by the adversary directly (for example, using information stealers or exploiting unmanaged edge devices) or by purchasing them.

API KEYS AND SECRETS

Access to protected resources using stolen API keys and secrets may allow an adversary to steal sensitive data. Unless the API keys and secrets are changed, the adversary could maintain indefinite access.

SESSION COOKIES AND TOKENS

Adversaries can steal session cookies and tokens to masquerade as the legitimate user and authenticate to an application.

ONE-TIME PASSWORDS (OTPs)

OTP theft allows the adversary to bypass multifactor authentication (MFA) by SIM swapping, SS7 attacks, socially engineering the victim or email compromise.

KERBEROS AND KERBEROS TICKETS

By stealing or forging Kerberos tickets, adversaries can gain access to encrypted credentials, which can then be cracked offline. CrowdStrike CAO recorded a 583% increase in Kerberoasting attacks in 2023.

Figure 1. Identity-based attack vectors

Scanned with OKEN Scanner

BEAR Adversaries Conduct Credential Collection Campaigns

FANCY BEAR conducted regular credential collection campaigns throughout 2023. In March 2023, Microsoft patched a zero-day elevation-of-privilege vulnerability in Microsoft Outlook (CVE-2023-23397), which FANCY BEAR had been exploiting since at least March 2022 to solicit NT LAN Manager authentication sessions from targets using specially crafted spear-phishing emails. The Polish Cyber Command reported that the adversary used this authentication data to connect to Exchange servers and change additional high-value account mailbox permissions through the Exchange Web Services protocol.[1]

FANCY BEAR also conducted credential phishing campaigns and developed a custom toolkit to capture credentials from Yahoo! Mail and ukr.net webmail users. The adversary expanded this toolkit to use the Browser-in-the-Browser technique in April 2023 and added MFA interception capabilities to its toolkit to collect OTPs sent to the MFA contact (e.g., a phone number) linked to the targeted account.

COZY BEAR has conducted credential phishing campaigns using Microsoft Teams messages to solicit MFA tokens for Microsoft 365 accounts since at least late May 2023. If a user accepts its initial message request, COZY BEAR attempts to socially engineer the target by claiming a change was made to their current MFA settings and stating an MFA code is required for verification.

CrowdStrike® Services has observed COZY BEAR connecting to a compromised account using Microsoft Entra ID (previously Azure Active Directory) before registering a new device and enabling a passwordless phone sign-in for the user. The adversary also exported certificates containing private keys and requested a KRBTGT-authentication ticket for a different account using a legitimately issued certificate.

1 https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/detecting-malicious-activity-against-microsoft-exchange-servers/

Scanned with OKEN Scanner

SCATTERED SPIDER Conducts Sophisticated Social Engineering Campaigns

Identity-based techniques are also central to SCATTERED SPIDER tradecraft. Throughout 2023, this adversary conducted sophisticated social engineering campaigns to access victim accounts. SCATTERED SPIDER's tactics included SMS phishing (smishing) and voice phishing (vishing) to harvest credentials and phone calls made to victim organization help desks to persuade support personnel to provide password and/or MFA resets for targeted accounts. In many cases, SCATTERED SPIDER also leveraged earlier intrusions at telecom organizations to SIM swap targeted employee phone numbers, enabling the adversary to then receive SMS messages containing OTP codes.

SCATTERED SPIDER deliberately selects social engineering campaign targets from employees in information security and other IT-related teams. This is likely due to direct employee access to security tools as well as applications and documentation that may support lateral movement and further account compromise. In a minority of incidents, SCATTERED SPIDER targeted accounts belonging to employees who had direct access to company financial resources.

Additionally, SCATTERED SPIDER often configured residential proxies to appear as though they were logging in to victim accounts from the same geographical area as the legitimate account owner. In doing so, the adversary further exhibited its understanding of identity-related security policies in enterprise organizations.

Scanned with OKEN Scanner

ADVERSARIES CONTINUE TO DEVELOP CLOUD-CONSCIOUSNESS

As predicted, cloud environment intrusions increased by 75% from 2022 to 2023 (Figure 2), with cloud-conscious cases increasing by 110% and cloud-agnostic cases increasing by 60%.

Cloud-conscious is a term referring to threat actors who are aware of the ability to compromise cloud workloads and use this knowledge to abuse features unique to the cloud for their own purposes.

eCrime adversaries are especially active in targeting cloud environments: 84% of cloud-conscious intrusions attributed to adversaries were conducted by likely eCrime actors, compared to 16% conducted by targeted intrusion actors. Traditional BGH adversaries, such as INDRIK SPIDER, became more cloud-conscious throughout the year.

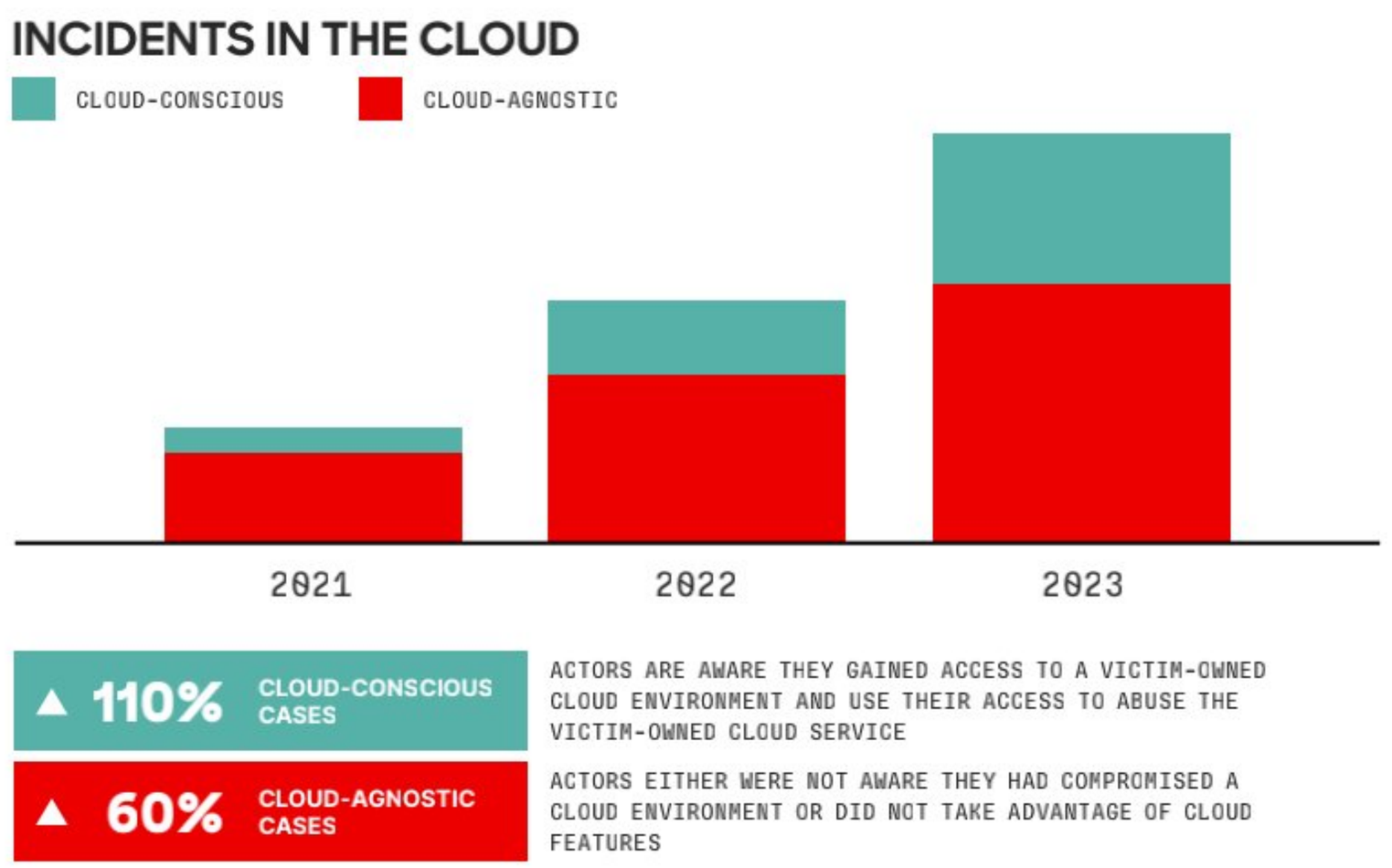


Figure 2. Increases in cloud cases

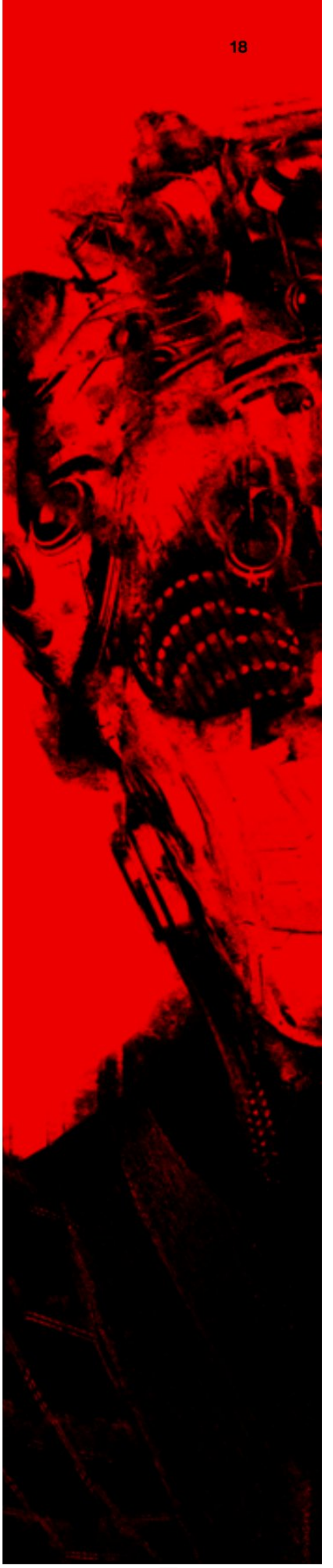
SCATTERED SPIDER predominantly drove cloud-conscious activity increases throughout 2023, accounting for 29% of total cases. Throughout 2023, SCATTERED SPIDER demonstrated progressive and sophisticated tradecraft within targeted cloud environments to maintain persistence, obtain credentials, move laterally and exfiltrate data.

Adversaries' preference for identity-based techniques is evident in their cloud-focused attacks. Next are several observations of cloud- and identity-focused activities categorized by the MITRE ATT&CK® enterprise tactics of Initial Access, Persistence, Privilege Escalation, Credential Access, Lateral Movement, Exfiltration and Impact.

AS PREDICTED, CLOUD ENVIRONMENT INTRUSIONS INCREASED BY 75% FROM 2022 TO 2023 (FIGURE 2), WITH CLOUD-CONSCIOUS CASES INCREASING BY 110% AND CLOUD-AGNOSTIC CASES INCREASING BY 60%.

↑75%
IN CLOUD INTRUSIONS

Scanned with OKEN Scanner



Initial Access

Adversaries relied on valid credentials to achieve initial access. They obtained these credentials via accidental credential leakage, brute-force attacks, phishing/social engineering, credential stealers, access brokers, insecure self-service password-reset services and insider threats.

IN THE WILD

FANCY BEAR AND SCATTERED SPIDER COMMONLY TARGETED MICROSOFT 365 CREDENTIALS VIA CREDENTIAL-PHISHING ATTACKS.

Persistence

To maintain access to Azure and Microsoft 365, adversaries commonly achieved persistence at the identity level.

IN THE WILD

ACHIEVING PERSISTENCE AT THE IDENTITY LEVEL IS COMMONLY ACHIEVED BY REGISTERING ADDITIONAL AUTHENTICATION FACTORS IN ENTRA ID.

SCATTERED SPIDER USED AN IDENTITY PROVIDER TO ESTABLISH PERSISTENCE WITH A FEDERATED DOMAIN IN ENTRA ID, INITIALLY RELYING ON AADINTERNALS AZURE AD BACKDOOR.[2] THIS PROVIDED THE ADVERSARY WITH PERSISTENT ACCESS TO MULTIPLE ENTRA ID IDENTITIES. LATER, SCATTERED SPIDER TRANSFERRED THE CONCEPT TO OKTA AND ADDED A FEDERATED IDENTITY PROVIDER TO A VICTIM'S OKTA TENANT.

Privilege Escalation

Adversaries escalated privileges by obtaining access to additional identities from stored credentials, social engineering campaigns or insecure password-reset portals. They also escalated privileges by modifying policies or adding identities to privileged groups or roles.

IN THE WILD

DURING AN INTRUSION TARGETING A NORTH AMERICAN SOFTWARE COMPANY, SCATTERED SPIDER ESCALATED PRIVILEGES BY ATTACHING A NEW ADMINISTRATOR ACCESS POLICY TO A PREEXISTING CLOUD USER, TO WHICH THEY ADDED A NEW ACCESS KEY.

2 https://aadinternals.com/post/aadbackdoor/

Scanned with OKEN Scanner

Credential Access

Threat actors harvested credentials from password stores and information repositories.

IN THE WILD

INDRIK SPIDER ACCESSED CREDENTIALS STORED IN AZURE KEY VAULT. IN A SEPARATE ATTACK, SCATTERED SPIDER ACCESSED CREDENTIALS STORED IN A CLOUD SECRETS MANAGER, AN IDENTITY-BASED SECRETS AND ENCRYPTION MANAGEMENT SYSTEM, AND SHAREPOINT.

IN ANOTHER CASE, SCATTERED SPIDER ALSO LOCATED A DOMAIN CONTROLLER INSIDE A VICTIM'S AZURE TENANT, COPIED THE DISKS AND CREATED A NEW ADVERSARY-CONTROLLED VIRTUAL MACHINE (VM) INTO WHICH THEY MOUNTED DOMAIN-CONTROLLER DISK COPIES. FROM THOSE DISK COPIES, THE ADVERSARY DUMPED ACTIVE DIRECTORY (AD) DATABASE *NTDS.DIT*.

Lateral Movement

Threat actors moved back and forth between on-premises and cloud environments.

IN THE WILD

SCATTERED SPIDER OFTEN USED ACCESS TO VICTIMS' MICROSOFT 365 ENVIRONMENTS TO SEARCH SHAREPOINT ONLINE FOR VIRTUAL PRIVATE NETWORK (VPN) SETUP INSTRUCTIONS AND THEN LOGGED ON TO THE VPN AND MOVED LATERALLY TO ON-PREMISES SERVERS.

SCATTERED SPIDER WAS ALSO OBSERVED USING AZURE RUN COMMANDS AND SIMILAR CAPABILITIES TO MOVE LATERALLY FROM THE CLOUD CONTROL PLANE TO COMPUTE INSTANCES.

Exfiltration

Adversaries exfiltrated data by using tooling, by directly downloading data from internet-accessible repositories — such as SharePoint Online or GitHub — or by **uploading data to internet-accessible web services.**

IN THE WILD

SCATTERED SPIDER LEVERAGED THE OPEN-SOURCE S3 BROWSER TO EXFILTRATE DATA TO AN EXTERNAL, ADVERSARY-CONTROLLED CLOUD STORAGE BUCKET.

Scanned with OKEN Scanner

Impact

Some cloud-conscious BGH threat actors targeted cloud storage as part of their operations.

IN THE WILD

CROWDSTRIKE CAO SPECIFICALLY OBSERVED SCATTERED SPIDER ADOPTING BGH TACTICS AND DEPLOYING RANSOMWARE FOR IMPACT.

IN A SEPARATE INCIDENT, AN ALPHA SPIDER AFFILIATE DEPLOYED TOOLING THAT ENABLES *Alphv* TO ENCRYPT AZURE STORAGE FILE SHARES. IN A *LockBit* INCIDENT, INDRIK SPIDER DELETED BACKUPS STORED IN AZURE BACKUPS.

THIRD-PARTY RELATIONSHIP EXPLOITATION

Throughout 2023, targeted intrusion actors consistently attempted to exploit trusted relationships to gain initial access to organizations across multiple verticals and regions. This type of attack takes advantage of vendor-client relationships to deploy malicious tooling via two key techniques: 1) compromising the software supply chain using trusted software to spread malicious tooling and 2) leveraging access to vendors supplying IT services.

Threat actors targeting third-party relationships are motivated by the potential return on investment (ROI): One compromised organization can lead to hundreds or thousands of follow-on targets. These stealthy attacks can also more effectively provide an opportunity for attackers seeking to exploit a hardened end target.

Scanned with OKEN Scanner

Threat Highlight: Trusted-Relationship Compromises by China-Nexus Adversaries

In 2023, China-nexus adversaries increasingly targeted third-party relationships in efforts to deploy malicious implants and gain initial access. Two adversaries — JACKPOT PANDA and CASCADE PANDA — consistently exploited trusted relationships through supply chain compromises and actor-on-the-side or actor-in-the-middle attacks. In each case, the operations focused on Chinese-speaking victims, possibly indicating ongoing domestic surveillance.

Throughout 2023, JACKPOT PANDA continued to use trojanized executables to deploy malicious utilities or second-stage implants. Beginning in May 2023, the adversary used a trojanized installer for CloudChat, a China-based chat application popular with illegal, Chinese-speaking gambling communities in Mainland China. The trojanized installer served from CloudChat's website contained the first stage of a multi-step process that ultimately deployed *XShade* — a novel implant with code that overlaps with JACKPOT PANDA's unique *CplRAT* implant.

Additional JACKPOT PANDA activity was identified in May 2023 using a signed .NET downloader, dubbed *QuestDownloader*, launched by a LiveHelp100 process. LiveHelp100 is associated with Comm100, a software utility targeted by a JACKPOT PANDA supply chain compromise in September 2022. *QuestDownloader* was ultimately used to deploy *Cobalt Strike* and *UltraVNC*.

Beginning in late 2023, CASCADE PANDA routinely used likely actor-in-the-middle or actor-on-the-side attacks to intercept legitimate update traffic from common utilities, as well as Chinese-language tools, to deploy *WinDealer* — a malicious remote access tool (RAT) uniquely associated with this adversary. In all CASCADE PANDA instances from this time period, legitimate software update processes connected to legitimate infrastructure associated with respective products and legitimate Chinese internet service provider infrastructure.

CASCADE PANDA likely distributes *WinDealer* by using domestic infrastructure to redirect legitimate traffic in transit. In one instance, CASCADE PANDA used a legitimate trojanized Chinese-language translation tool executable to deploy *WinDealer*.

FOR MORE INFORMATION ON ANY OF THE ADVERSARIES MENTIONED IN THIS REPORT AND THOSE TARGETING YOUR INDUSTRY OR REGION, CHECK OUT THE CROWDSTRIKE ADVERSARY UNIVERSE.

Scanned with OKEN Scanner

Unattributed targeted intrusion actors using TTPs consistent with China-nexus adversaries also exploited trusted relationships to conduct operations in 2023. Throughout the second half of the year, an unattributed actor compromised an India-based information security software vendor and used the resulting access to distribute trojanized executables via legitimate software update processes.

These attacks target victims from multiple regions and industries, including the construction, financial services, government, technology, telecom and logistics sectors throughout the U.S., India, Brazil, Sri Lanka, the Philippines, Zambia, Mexico and Malaysia. Though this trusted-relationship exploitation activity remains unattributed, the final payload used in this attack shares significant code overlaps with *BackShell* and *StealthPipes*, two tools uniquely attributed to WET PANDA.

A second unattributed actor was observed in late 2023 distributing *ShadowPad* to suspected Chinese-speaking targets as part of a likely supply chain compromise. The actor compromised a China-based virtual conference platform and leveraged the resulting access to deploy a trojanized *ShadowPad* installer masquerading as a legitimate software tool. Though this activity is unattributed, *ShadowPad* is exclusively used by China-nexus adversaries such as AQUATIC PANDA, WICKED PANDA and VAPOR PANDA.

In early 2023, an unattributed actor likely compromised an update server associated with iPhone i4Tools management software to deploy *AvanteGarde*, a malware framework associated with China-nexus activity cluster InnateSpark. Though CrowdStrike CAO was able to confirm at least 250 customers had connected to the compromised update server, only 10% received the malicious update, possibly indicating the actor down-selected high-value targets.

Threat Highlight: North Korea's Supply Chain Compromises

Democratic People's Republic of Korea (DPRK) adversaries also demonstrated an increased interest in exploiting trusted relationships in 2023. In particular, LABYRINTH CHOLLIMA abused a trusted relationship between a technology vendor and a client in three instances last year, highlighting an interest in using supply chain compromises as an intrusion vector.

This exploitation tradecraft was first observed in March 2023, when an adversary compromised software at VoIP provider 3CX. This compromise appears to have started with an upstream supply chain compromise of financial technology firm Trading Technologies. The adversary used trojanized 3CX Electron Windows and macOS desktop application variants to deliver information stealers to victim environments. The threat actors then persisted with a July 2023 campaign that similarly abused access to a technology company in efforts to compromise its product and use legitimate infrastructure to infiltrate the compromised company's clientele.

Scanned with OKEN Scanner

CrowdStrike CAO also observed LABYRINTH CHOLLIMA distributing malware via a trojanized CyberLink media player variant. This campaign stands out among other LABYRINTH CHOLLIMA supply chain compromises, as the adversary used execution guardrails that limited the campaign to a specific geography and temporal window, suggesting the targeting of a particular victim set.

The motivation driving these compromises remains undefined. In one supply chain compromise, CrowdStrike CAO detected trojanized software in the environments of 62 customers; however, subsequent supply chain compromises were more limited in scope. The adversary may be using supply chain compromises to cast a wide net and deliver appropriate follow-on tooling to interesting targets.

LABYRINTH CHOLLIMA is equally likely abusing trusted relationships between suppliers and product users to infiltrate specific high-value targets for currency generation and espionage campaigns. CrowdStrike CAO assesses that additional LABYRINTH CHOLLIMA supply chain compromises are increasingly likely to occur in the near future. The adversary likely considers supply chain compromise a useful tactic with potential to streamline operations. This assessment is made with moderate confidence based on the volume of supply chain compromises observed in 2023.

Outlook:
Third-Party Relationship Exploitation

Trusted-relationship compromises will continue to attract targeted intrusion actors in the immediate future. The high ROI for these attacks, particularly in terms of access to potential downstream compromises relative to the limited effort required to compromise one target, will likely motivate attacks throughout 2024.

Organizations operating in the technology sector are uniquely at risk from third-party relationship exploitation. In 2023, nearly every trusted-relationship compromise originated as part of an intrusion at a technology sector organization that provided commercial software.

Scanned with OKEN Scanner

VULNERABILITY LANDSCAPE: "UNDER THE RADAR" EXPLOITATION

Threat actors have adapted to the enhanced visibility of traditional endpoint detection and response (EDR) sensors by altering their exploitation tactics for initial access and lateral movement. They are now targeting the network periphery, where defender visibility is reduced by the possibility that endpoints may lack EDR sensors or cannot support sensor deployment (Figure 3).

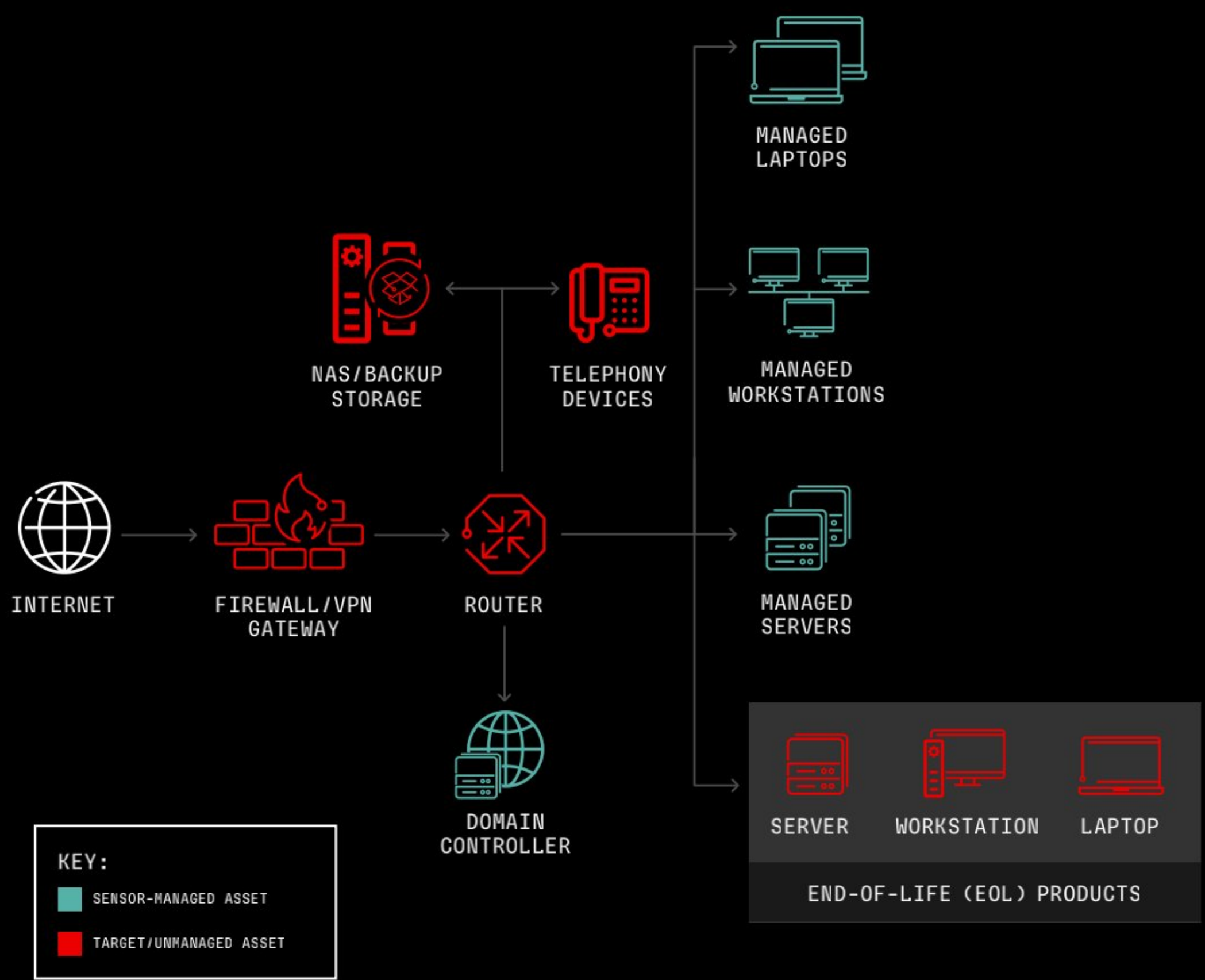


Figure 3. Unmanaged targets on a generic network

Scanned with OKEN Scanner

Unmanaged network appliances — particularly edge gateway devices — remained the most routinely observed initial access vector for exploitation during 2023. These devices are commonly based on obsolete architecture, leading to broadly exploited vulnerabilities in firewall and VPN platforms from Cisco (CVE-2023-20198), Citrix (CVE-2023-3519, CVE-2023-4966) and F5 (CVE-2023-46747).

Exploitation was also observed in various other unmanaged devices throughout 2023. Targeted intrusion actors likely engaged in opportunistic Ivanti mobile device management application targeting via CVE-2023-35078 and CVE-2023-35082. *Akira* ransomware operators leveraged exploits for CVE-2023-27532 — a vulnerability in Veeam Backup & Replication — to pivot into victim backup storage infrastructure. Additionally, eCrime actors developed zero-day exploits for telephony products based on an abandoned open-source project.

UNMANAGED NETWORK APPLIANCES – PARTICULARLY EDGE GATEWAY DEVICES – REMAINED THE MOST ROUTINELY OBSERVED INITIAL ACCESS VECTOR FOR EXPLOITATION DURING 2023.

The latter zero-day exploit relates to another trend observed in 2023: a focus on EOL product exploitation. Threat actors are actively developing exploits for EOL products that cannot be patched and often do not allow for modern sensor deployment. Unsupported operating system (OS) servers and legacy gateway appliances offer easy access — even to otherwise antiquated malware families — leading to lingering infections that distract resources from contemporary security issues.

THREAT ACTORS ARE ACTIVELY DEVELOPING EXPLOITS FOR EOL PRODUCTS THAT CANNOT BE PATCHED AND OFTEN DO NOT ALLOW FOR MODERN SENSOR DEPLOYMENT.

Increasing defender visibility to such exploit vectors is key in mitigating the risk posed by these tactics. CrowdStrike® Falcon Surface℠ can be leveraged to monitor and reduce internet-exposed services and maintain an application inventory across an organization's attack surface. Defenders should prioritize patching exposed products, particularly open-source platforms, when the products are subject to known remote code execution (RCE) vulnerabilities. Finally, CrowdStrike Falcon® Spotlight can determine whether sensor-deployed assets are subject to known vulnerabilities and when these endpoints have reached EOL.

2023 ISRAEL-HAMAS CONFLICT: CYBER OPERATIONS FOCUS ON DISRUPTION AND INFLUENCE

On October 7, 2023, Hamas military wing Izz al-Din al-Qassam Brigades (IDQB) and several other Gaza-based militant groups launched a massive kinetic attack against Israel, killing hundreds of Israelis and taking hostages. In the ensuing months, CrowdStrike CAO tracked ongoing cyber operations from targeted intrusion and hacktivist actors. Activity and claims from both groups primarily focus on targeting operational technology or other critical systems — likely to psychologically influence target populations — and deploying destructive wipers against Israeli or Israel-linked entities.

Most conflict-driven cyber operations observed include hacktivist activity and operations by suspected faketivists. Within the context of the Israel-Hamas conflict, the dividing line between these two threat actor types has blurred, as genuine hacktivist groups often amplify the claims of, or provide support to, likely state-nexus inauthentic personas.

Scanned with OKEN Scanner

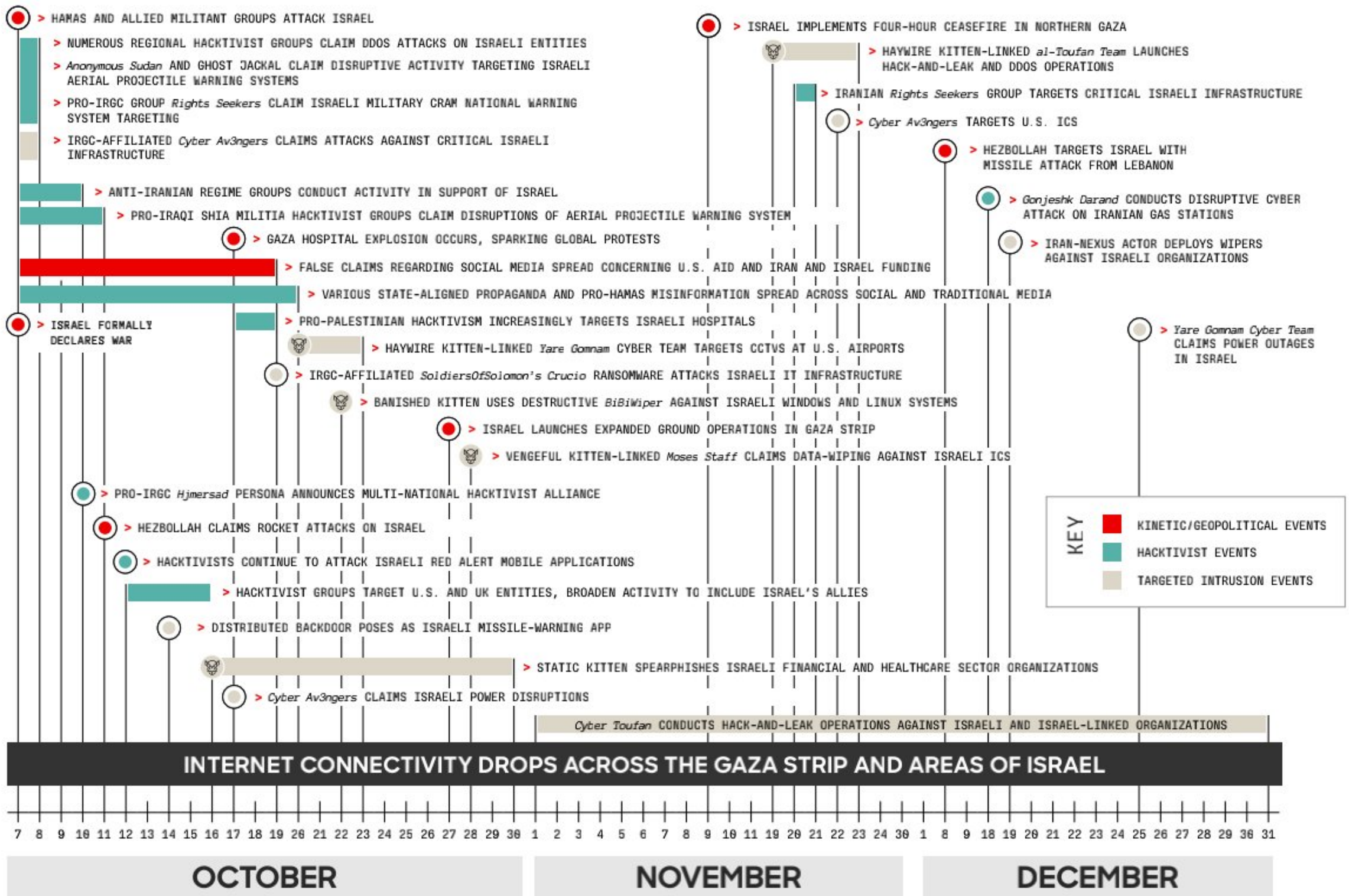


Figure 4. Significant cyber and kinetic conflict-related events

Faketivists associated with Iranian state-nexus adversaries and hacktivists branding themselves as "pro-Palestinian" focused on targeting critical infrastructure, Israeli aerial projectile warning systems and activity intended for information operation purposes in 2023.

Though CrowdStrike CAO tracks multiple adversaries associated with the Hamas militant group, activity attributed to these adversaries has not been observed in connection with the Israel-Hamas conflict to date. This is likely due to unavailable resources or the degradation of internet and electricity-distribution infrastructure in the conflict zone.

Faketivism

INTRODUCED IN THE CROWDSTRIKE 2016 GLOBAL THREAT REPORT, FAKETIVISM REFERS TO ACTIVITY BY ENTITIES THAT CHARACTERIZE THEMSELVES AS HACKTIVIST GROUPS BUT MORE LIKELY REPRESENT A FRONT FOR A GOVERNMENT OR OTHERWISE PROFESSIONAL ENTITY.

IN AN EFFORT TO APPEAR GENUINE, FAKETIVISTS – AKA INAUTHENTIC PERSONAS – OFTEN ADOPT THE EXISTING IMAGERY, RHETORIC, TTPS AND SOMETIMES NAMES OF ESTABLISHED HACKTIVISTS. THEY OFTEN SURFACE IN DIRECT RESPONSE TO GEOPOLITICAL EVENTS, OFTEN HAVE LITTLE OR NO ESTABLISHED ACTIVITY HISTORY, AND ALMOST ALWAYS OPERATE IN DIRECT ALIGNMENT WITH STATE GOVERNMENT INTERESTS. THESE PERSONAS PROVIDE STATE BACKERS WITH A LAYER OF DENIABILITY BUT CAN ALSO SERVE INFORMATION OPERATIONS GOALS.

Scanned with OKEN Scanner

Hamas-Nexus Adversaries Noticeably Absent from Conflict-Related Activity

CrowdStrike CAO-assessed, likely Gaza-based adversaries EXTREME JACKAL and RENEGADE JACKAL demonstrate support for strategic Hamas interests. Additionally, evidence suggests the CruelAlchemy activity cluster represents a Hamas-linked cyber operations unit physically present in Turkey.

RENEGADE JACKAL was the most active Hamas-nexus adversary throughout 2023. The group primarily targeted Middle East-based government entities with its custom *Micropsia* Windows malware and Android implants. In mid-October 2023, CrowdStrike CAO linked RENEGADE JACKAL to the *Jerusalem Electronic Army*, an ostensible hacktivist group Hamas officials previously indicated was in support of the IDQB Cyberwarfare Unit.

Open-source reporting identified activity, allegedly attributable to Hamas, targeting Israeli Defense Forces (IDF) personnel. However, CrowdStrike CAO has no further evidence to suggest the aforementioned adversaries are currently targeting Israeli entities in connection with recent events in Israel and Gaza.[3] Since the onset of the conflict, internet connectivity in the Gaza Strip has been significantly degraded almost certainly due to a combination of kinetic activity, power outages and distributed denial-of-service (DDoS) attacks.

Power and internet disruptions have likely hindered Gaza-based adversary operations. Though no CruelAlchemy activity has been observed in direct association with the Israel-Hamas conflict, identified command-and-control (C2) infrastructure indicates the actor remained active following the onset of the conflict, possibly supporting prior reporting that suggests CruelAlchemy operates from outside of Gaza.

Widespread Hacktivist Operations Span Motivational Spectrum, Demonstrate Concerted Interest in Critical Systems

Though the October 7, 2023, launch of the Israel-Hamas conflict ignited a flurry of pro-Palestine and pro-Israel hacktivist activity, the former far outpaced the latter. Known and previously unobserved hacktivists within the conflict region and from around the world claimed the activity, a significant portion of which revolved around attempted or alleged aerial projectile warning system and critical infrastructure disruption targeting Israel. A smaller number of hacktivists also extended their operations beyond the conflict region to target countries or entities deemed supportive of Israel.

3 https://www.timesofisrael.com/liveblog_entry/idf-exposes-catfishing-network-seeking-to-extract-info-from-troops-on-hamass-behalf/

Scanned with OKEN Scanner

Aerial Projectile Warning Systems and Critical Infrastructure Targeting

Multiple hacktivist entities have targeted aerial projectile warning systems in Israel and claimed to have disrupted IDF counter-rocket, artillery and mortar systems to prevent notification delivery and/or send false imminent attack notifications to Israeli citizens. Observed targeting of these services decreased after mid-October 2023; however, a surge of kinetic activity in the region could ignite a renewed interest in further disruption or false notifications.

Throughout the duration of the conflict, pro-Palestine hacktivists have consistently targeted critical infrastructure in Israel, including disruptive activity against energy-distribution infrastructure and water pumps, DDoS attacks against utility companies, and hack-and-leak operations against water treatment and energy plants. This activity is likely an attempt to inflict physical and psychological damage on Israeli citizens and will likely continue throughout the duration of the Israel-Hamas conflict. This assessment is made with high confidence based on consistent targeting to date and similar activity observed in other recent conflicts, such as the Russia-Ukraine war.

Operations Beyond the Immediate Conflict Region

Limited hacktivist activity extended beyond the immediate conflict area in retaliation against real or perceived support of Israel. On October 12, 2023, Yemeni group *Team R70* claimed a DDoS attack against a U.S.-based airport, alleging the airport receives the most Israeli air traffic.

On October 14, 2023, prominent South Asian hacktivist group *Team Insane Pakistan* claimed a DDoS attack against a British military website. This activity was accompanied by references to U.K. support for Israel.

On October 16, 2023, a likely Indonesian hacktivist group calling itself *INFINITE INSIGHT* shared leaked data, claiming to have breached the personally identifiable information (PII) of nearly 790,000 doctors in the United States. The alleged leak was reportedly in retaliation against U.S. support for Israel as well as to show support for Palestinians.

Hacktivists will likely continue limited targeting of countries and entities beyond the conflict region that they perceive as supporting Israel. This assessment is made with high confidence based on consistent activity observed to date and in similar conflicts, such as the Russia-Ukraine war, as well as observed communications within hacktivist channels.

Scanned with OKEN Scanner

Iranian Adversaries Operate Inauthentic Personas for Disruption and IO

CrowdStrike CAO has not observed Iranian state-nexus adversaries providing direct operational support to Hamas' cyber units or IDQB's kinetic operations. Iranian adversaries associated with the country's Ministry of Intelligence and Security (MOIS) and Islamic Revolutionary Guard Corps (IRGC) have an established record of using disruptive and destructive attacks, hack-and-leak operations, inauthentic personas and hacktivist groups to target Israeli entities.

This cyber-enabled activity is likely intended to influence Israeli audiences during the ongoing crisis. Though Iranian cyber operations have historically focused on Israel, the number of faketivist personas leveraged against Israeli targets has increased since the onset of the Israel-Hamas conflict. These personas' claims focus on campaign impacts on operational technology and are almost certainly intended to influence the target populations' perception of Iranian adversaries' ability to disrupt critical services.

Figure 5. Iran-nexus cyber activity during the conflict

Scanned with OKEN Scanner

Adversary	Date in 2023	Activity
SPECTRAL KITTEN	OCTOBER 9	*MALEKTEAM* PERSONA LEAKED PII, CCTV FOOTAGE AND OTHER DATA ALLEGEDLY SOURCED FROM INTRUSIONS TARGETING ISRAELI ENTITIES
HAYWIRE KITTEN	OCTOBER-NOVEMBER	HAYWIRE KITTEN, ASSOCIATED WITH IRGC CONTRACTOR EMENNET PASARGAD, OPERATED PERSONAS *YARE GOMNAM CYBER TEAM* AND *AL-TOUFAN TEAM* TO CLAIM CCTV SYSTEM TARGETING AT U.S. AIRPORTS, THREATEN CYBER-ENABLED KINETIC ATTACKS AGAINST ISRAEL, AND CARRY OUT HACK-AND-LEAK AND DDOS OPERATIONS
BANISHED KITTEN	OCTOBER	MOIS-LINKED BANISHED KITTEN DEPLOYED THE *BIBIWIPER* MALWARE FAMILY AGAINST COMPANIES IN ISRAEL; A *KARMA POWER* ANTI-ISRAELI MESSAGING CAMPAIGN OCCURRED ALONGSIDE THE REPORTED WIPER OPERATIONS
VENGEFUL KITTEN	OCTOBER 26-28	*MOSES STAFF* CLAIMED DATA-WIPING ACTIVITY AGAINST MORE THAN 20 COMPANIES' INDUSTRIAL CONTROL SYSTEMS (ICS) IN ISRAEL AND INDICATED INTEREST IN SMS, BASE-TRANSCEIVER STATIONS AND PUBLIC ALERT SYSTEMS
UNATTRIBUTED IRGC-NEXUS PERSONAS	OCTOBER-NOVEMBER	IRGC-LINKED *SOLDIERSOFSOLOMON* USED DESTRUCTIVE RANSOMWARE VARIANT *CRUCIO* AGAINST INTERNET OF THINGS (IoT) DEVICES IN ISRAEL; IRGC-AFFILIATED *CYBER AV3NGERS* COMPROMISED AND DEFACED PROGRAMMABLE LOGIC CONTROLLERS (PLCs) IN ISRAEL AND THE U.S. AT CRITICAL INFRASTRUCTURE ENTITIES SUCH AS WATER TREATMENT FACILITIES[4]
UNKNOWN IRAN-NEXUS ACTOR	DECEMBER 19	UNKNOWN IRAN-NEXUS ACTOR DEPLOYED WIPERS AGAINST ISRAELI ORGANIZATIONS
HAYWIRE KITTEN	DECEMBER 25	*YARE GOMNAM CYBER TEAM* CLAIMED RESPONSIBILITY FOR POWER OUTAGES IN ISRAEL

4 https://www.cisa.gov/news-events/alerts/2023/12/01/cisa-and-partners-release-joint-advisory-irgc-affiliated-cyber-actors-exploiting-plcs

Scanned with OKEN Scanner

Outlook:
Cyber Operations in the Conflict

Unlike in the Russia-Ukraine war, where known cyber operations have directly contributed to the conflict, those involved in the Israel-Hamas conflict have not directly contributed to Hamas' military operations against Israel. The full breadth and effects of activity targeting Israel, particularly by Iranian state-nexus adversaries and allied proxies, are almost certainly not fully known. However, identified incidents have largely been misaligned with early concerns that Iranian cyberattacks could cause significant disruptions across critical sectors in Israel and broaden in scope to allied countries. This misalignment may point to Iranian forces' incapability or lack of preparedness and their desire to avoid an unintended escalation that could draw Iran more directly into the conflict.

CrowdStrike CAO tracks activity clusters SpoiledMocha and Moonshuttle. These are reportedly aligned with Iran's regional proxies — the Houthi movement in Yemen and Hezbollah in Lebanon, respectively — even though these entities have not yet been observed within the Israel-Hamas conflict context.

Pro-Iraqi Shia militia hacktivist groups have demonstrated consistent involvement in targeting Israeli entities since the onset of the conflict. An escalation in kinetic hostilities could lead to related activity from these groups.

Hacktivist activity will almost certainly continue apace with fluctuations in related geopolitical developments. This assessment is made with high confidence based on the activity patterns exhibited to date as well as consistent patterns observed across other similar conflicts.

Scanned with OKEN Scanner

THREATS ON THE 2024 HORIZON

As organizations plan for potential threats emerging in 2024, two potential disruption drivers come to the forefront: generative AI and 2024 global government elections.

Generative AI Use Within the Threat Landscape

Mainstream accessible generative AI technology exploded in late 2022, opening up a new realm of possibilities for efficient content creation and drawing the attention of adversaries seeking ways to exploit this new technology for their own purposes.

Generative AI has massively democratized computing to improve adversary operations. It can also potentially lower the entry barrier to the threat landscape for less sophisticated threat actors.

Two primary generative AI opportunity areas within the threat landscape include:

- Developing and/or executing malicious computer network operations (CNO), including tool and resource development such as scripts or code that could be functionally malicious if used correctly
- Supporting the efficiency and effectiveness of social engineering and information operations campaigns

>> GENERATIVE AI HAS MASSIVELY DEMOCRATIZED COMPUTING TO IMPROVE ADVERSARY OPERATIONS. IT CAN ALSO POTENTIALLY LOWER THE ENTRY BARRIER TO THE THREAT LANDSCAPE FOR LESS SOPHISTICATED THREAT ACTORS.

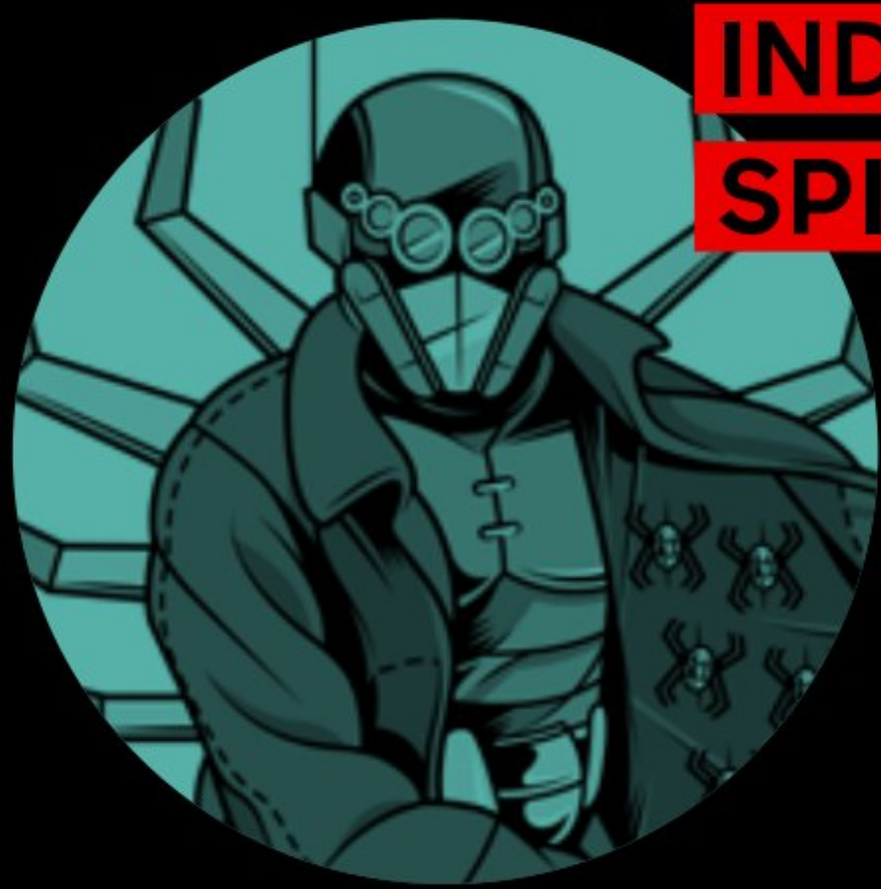
Generative AI in Malicious Computer Network Operations

It's difficult to confidently gauge the probability of adversaries using newer technologies such as generative AI in their operations, particularly in relation to how these technologies will support malicious CNO. Only rare concrete observations included likely adversary use of generative AI during some operational phases.

CrowdStrike's visibility into the use of such tools is likely incomplete. This is either a result of limited observations, the fact that the AI-generated material did not intrinsically leave significant indicators of its true nature or adversaries taking steps to avoid revealing evidence that generative AI was in use.

Throughout 2023, generative AI was rarely observed supporting malicious CNO development and/or execution.

Scanned with OKEN Scanner



INDRIK SPIDER

In February 2023, CrowdStrike Services responded to an INDRIK SPIDER incident involving BITWISE SPIDER's *LockBit RED* ransomware. During this incident, INDRIK SPIDER exfiltrated credentials from cloud-based credential manager Azure Key Vault. Logs show that INDRIK SPIDER also visited ChatGPT while interacting with the Azure Portal.

In addition to visiting ChatGPT while browsing the Azure Portal — presumably to understand how to navigate in Azure — browsing activity analysis indicates INDRIK SPIDER used search engines such as Google and Bing and searched on GitHub during the operations to understand how to exfiltrate Azure Key Vault credentials.

Using search engines and visiting ChatGPT indicate that though INDRIK SPIDER is likely new to the cloud and not yet sophisticated in this domain, it is using generative AI to fill these knowledge gaps.

SCATTERED SPIDER

In the second half of 2023, SCATTERED SPIDER used the Azure AD PowerShell module to download all Entra ID user immutable IDs at a North American financial services victim. Using its Entra ID backdoor, the adversary could log in as any of the downloaded users. The PowerShell used to download the users' immutable IDs resembled large language model (LLM) outputs such as those from ChatGPT. In particular, the pattern of one comment, the actual command and then a new line for each command matches the Llama 2 70B model output.

Based on the similar code style, SCATTERED SPIDER likely relied on an LLM to generate the PowerShell script in this activity.

Scanned with OKEN Scanner

Generative AI in Social Engineering and Information Operations

In recent years, certain language models have been able to compose fictional stories[5] and generate digital artwork.[6] Since at least mid-2021, CrowdStrike has frequently reported on alleged research interest in highly deceptive AI-fabricated images, audio and video (aka "deepfakes") by Russia, China and Iran. Researchers and academics have further speculated that threat actors will almost certainly use generative AI tools in information and influence operations in the near future.[7]

These speculations began actualizing in 2023: A Chinese information operations campaign, likely reliant on images produced by generative AI (specifically diffusion-model-generated images), gained authentic engagement across several prominent social media platforms throughout September. Beyond state-nexus actors, CrowdStrike also observed a hacktivist group attempting to create a spam tool using generative AI as part of its efforts to disseminate pro-Azerbaijan messaging.

Outlook

Generative AI has potential for use in numerous fields not likely identified or popularized in mainstream public discourse. AI's continuous development will undoubtedly increase the potency of its potential misuse — particularly within the scope of information operations and especially for less digitally literate audiences. The degree to which popular generative AI tools can be used maliciously will likely adapt over time as companies, tool owners and governments respond to new developments and perceived misuse.

CrowdStrike CAO assesses that generative AI will likely be used for cyber activities in 2024 as the technology continues to gain popularity. The team will track exactly how threat actors use this technology, and how this use differs from mainstream applications, throughout 2024. This type of research includes examinations of both:

- The potential that adversaries will use publicly available or open-source LLMs, which will likely require continual adversary navigation around safeguards against malicious or illegal activity (e.g., jailbreaking).
- Adversaries' attempts to develop their own models or generative AI tools that require less prompt engineering. Notably, the cost of training LLMs can significantly deter their independent, illicit development. Threat actors' attempts to craft and use such models in 2023 frequently amounted to scams that created relatively poor outputs and, in many cases, quickly became defunct.

---

5 https://apnews.com/article/7f49bd9aa9d1427d8400e40beb9f5ba4
6 https://apnews.com/article/artificial-intelligence-images-rights-1c6d9e0e260e2d135a3e3bf98d5493df
7 https://cdn.openai.com/papers/forecasting-misuse.pdf

Scanned with OKEN Scanner

2024 Elections

In 2024, individuals from 55 countries representing more than 42% of the global population will participate in presidential, parliamentary and/or general elections. This includes seven of the 10 most populous countries in the world: India, the U.S., Indonesia, Pakistan, Bangladesh, Russia and Mexico. High-profile, national-level elections will also occur in countries or groups involved in, or proximal to, major geopolitical conflicts. These include Taiwan, Azerbaijan, India, Pakistan, Iran, Belarus, Russia, Finland, Lithuania and the European Union.

2024's potential to transform geopolitics around the globe for the near future will likely give adversaries numerous opportunities, and a considerable strategic impetus, to target entities involved in electoral processes throughout the coming year.

Election Targeting

Cyber activity targeting elections can range from direct attempts to disrupt electoral processes to more indirect efforts to sway voter opinion toward outcomes preferred by the adversary.[8] The most direct, but least frequent, targeting involves intrusions against the software and hardware used to record, tally, count and transmit votes in voting systems. This form of election interference can range from using computer network attacks to intentionally disrupt, degrade or destroy voting systems to using privileged access or vulnerabilities to attempt to alter vote counts without detection.

Less direct forms of targeted intrusion can involve attempts to compromise, disrupt access to or leak data from government systems that provide logistical information to voters, store voter registration data or otherwise support transparent and democratic election conduct. These targeted intrusion efforts include using DDoS attacks or website defacements against local, municipal, provincial and state government systems, a tactic historically favored by hacktivists seeking to espouse their viewpoints during tense political moments. Other parties involved in elections — such as political candidates, parties, donors and advocacy groups — can also be targeted in a variety of ways, including via the use of hack-and-leak operations often designed to publicly discredit the target.

The least direct type of election targeting — but almost certainly the most common and typically the most difficult to prevent — involves distributing mis- or disinformation to electorates before, during and after voting processes in an effort to influence popular opinion.

These information operations can take many forms. One common theme involves attempts to generate disruptive narratives — for example, they may undermine public confidence in election outcomes, enhance perceptions that specific political parties or individuals are corrupt, impugn candidates' personal character or disseminate inflammatory and polarizing social rhetoric. Other operations may aim to reinforce perspectives that portray the threat actor responsible in a more positive light; for example, as an advocate for specific policy positions beneficial to that entity or representative of cooperation or coexistence rhetoric.

8 Though this section details the actions of external malicious actors targeting elections, it is worth noting that ostensibly democratic governments sometimes also use their own domestic security authorities to legally restrict the free flow of information during election cycles (e.g., internet shutdowns and censorship).

IN 2024, INDIVIDUALS FROM 55 COUNTRIES REPRESENTING MORE THAN 42% OF THE GLOBAL POPULATION WILL PARTICIPATE IN PRESIDENTIAL, PARLIAMENTARY AND/OR GENERAL ELECTIONS. THIS INCLUDES SEVEN OF THE 10 MOST POPULOUS COUNTRIES IN THE WORLD

Scanned with OKEN Scanner

Threat Highlight:
Iranian Targeting of U.S. Elections in 2020

In late October 2020, a few weeks before the last U.S. presidential election cycle, Iranian threat actors conducted varied targeted IO against U.S. entities. They sent threatening emails to voters, alleging to represent a far-right U.S. political group and directing recipients to vote for a specific candidate. Iranian threat actors also disseminated a video falsely alleging to depict overseas actors fabricating ballots, implying one particular political party would seek to exploit security vulnerabilities and compromise voting systems.

Outlook

The most common malicious activities targeting elections have historically involved information operations likely conducted by state-nexus entities against citizens of countries that hold specific geopolitical interest to the threat actor and simple, short-lived hacktivism — including DDoS attacks and website defacements — against state and local government entities. This trend is highly likely to continue in 2024.

Scanned with OKEN Scanner

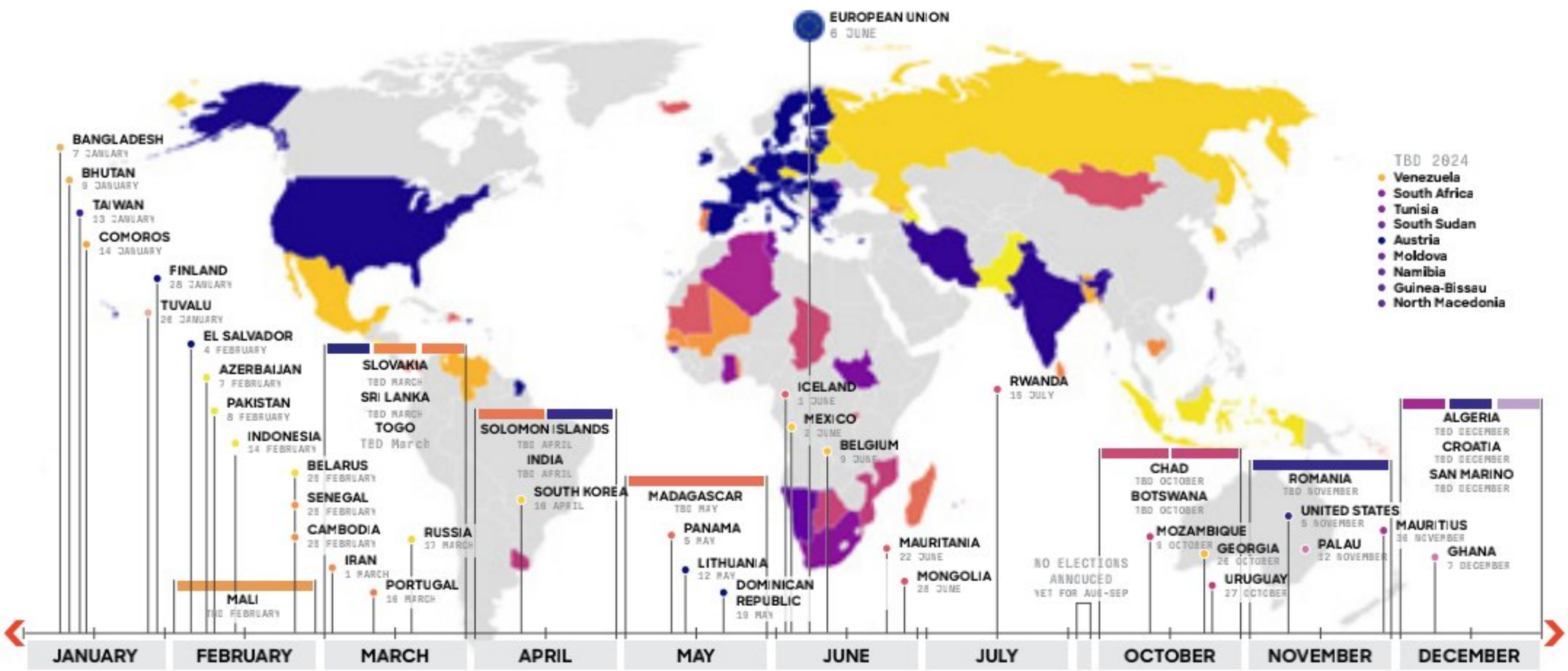


Figure 6. Countries holding presidential, parliamentary or general elections in 2024

In 2024, countries of interest involved in election cycles will likely be at risk of significant and lengthy IO campaigns from major global powers. Russia and Iran will likely leverage IO against the U.S. and the EU, which they consider major geopolitical opponents.

China will also likely conduct IO against elections held in its perceived regional sphere of influence, such as those in Indonesia, South Korea and Taiwan. Russia will almost certainly behave similarly in elections occurring in Belarus, Lithuania, Finland and Georgia. India and Pakistan are highly likely to conduct significant IO campaigns against one another during their respective elections in April and February 2024, particularly given the current political upheaval and polarization in both countries.[9]

Given the ease with which AI tools can generate deceptive but convincing narratives, adversaries will highly likely use such tools to conduct IO against elections in 2024. Politically active partisans within those countries holding elections will also likely use generative AI to create disinformation to disseminate within their own circles.

These issues were already observed within the first few weeks of 2024, as Chinese actors used AI-generated content in social media influence campaigns to disseminate content critical of Taiwan presidential election candidates.

The overall polarization of the political spectrum in many countries amid continuing economic and social issues will likely increase the susceptibility of those countries' citizenries to IO — particularly IO campaigns targeted at reinforcing those individuals' negative opinions of political opponents.[10]

Additionally, changes to or staff reductions affecting the enforceability of content moderation policies at major social media companies will likely provide opportunities for adversary exploitation using these platforms to disseminate IO narratives.[11]

With such political environments currently existing in most of the large and geopolitically significant countries, 2024 will almost certainly present a challenging global test for democracies.

RUSSIA AND IRAN WILL LIKELY LEVERAGE IO AGAINST THE U.S. AND THE EU, WHICH THEY CONSIDER MAJOR GEOPOLITICAL OPPONENTS.

9 https://www.eastasiaforum.org/2024/01/06/military-influence-and-political-peril-in-pakistan/
https://foreignpolicy.com/2024/01/02/india-elections-modi-bjp-congress-nda-lok-sabha-brics/

10 https://www.cambridge.org/core/journals/american-political-science-review/article/abs/partisan-polarization-is-the-primary-psychological-motivation-behind-political-fake-news-sharing-on-twitter/3F7D2098CD87AE5501F7AD4A7FA83602

11 https://www.theguardian.com/media/2023/dec/07/2024-elections-social-media-content-safety-policies-moderation

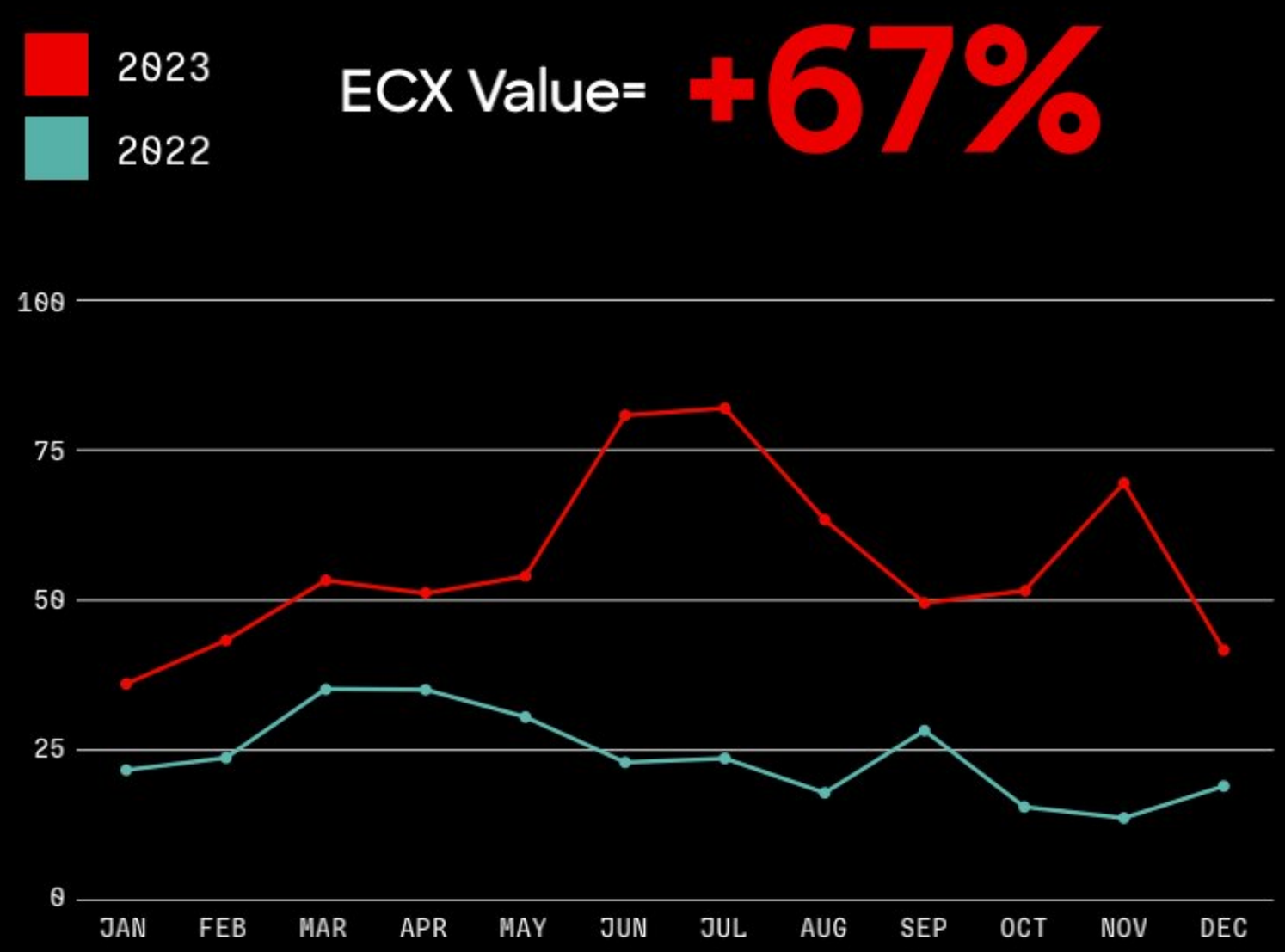
Scanned with OKEN Scanner

eCrime Landscape

The CrowdStrike eCrime Index® (ECX) tracks activity — including the number of observed spam emails and the average cost of buying access to a corporate network — across multiple eCrime ecosystem segments and calculates the total number of observed ransomware victims.

Until May 2023, the ECX exhibited trends similar to those observed in 2022. However, from June 2023 onward, the ECX grew significantly, with major spikes between June and August. The most impactful contributors to these spikes included high BGH incident frequency and a sudden increase in observed DDoS attacks.

The ECX spiked again in November 2023, reflecting increases in spam email numbers and the rising average price for loaders and stealers.



New Vulnerabilities with 9/10 CVSS3 Score
+6%

BGH Incidents Involving Data Leaks
+76%

Average Loader Cost
+169%

Average Crypter Cost
+250%

Average Stealer Cost
+286%

Average Ransom Demand
-27%

Identified Spam Emails
-15%

Figure 7. eCrime index value, 2022 vs. 2023, and key observable changes, 2023

Scanned with OKEN Scanner

The 2023 ECX tracked the most annual activity to date, representing the index's year-over-year growth. Spam emails likely decreased in 2023 as adversaries searched for other means of initial access and after a multinational operation shut down MALLARD SPIDER's *QakBot*.

Though the average ransom demand was lower in 2023 than in 2022, this highly likely represents an outlier in the dataset and not an accurate view of the threat landscape. Ransom demands have likely remained consistently high throughout this period, but the ability to track these values is becoming challenging due to threat actors and victims implementing stricter privacy measures around ransom price demands and payments.

BIG GAME HUNTING

2023 BGH DLS Statistics

The number of victims named on BGH dedicated leak sites increased significantly in 2023, with 4,615 victim posts made to DLSs — a 76% increase over 2022. Several factors contributed to this growth, including newly emerged BGH adversaries, growth of existing adversary operations and select high-volume campaigns such as multiple GRACEFUL SPIDER zero-day exploitations.

THE NUMBER OF VICTIMS NAMED ON BGH DEDICATED LEAK SITES INCREASED SIGNIFICANTLY IN 2023, WITH 4,615 VICTIM POSTS MADE TO DLSs – A 76% INCREASE OVER 2022.

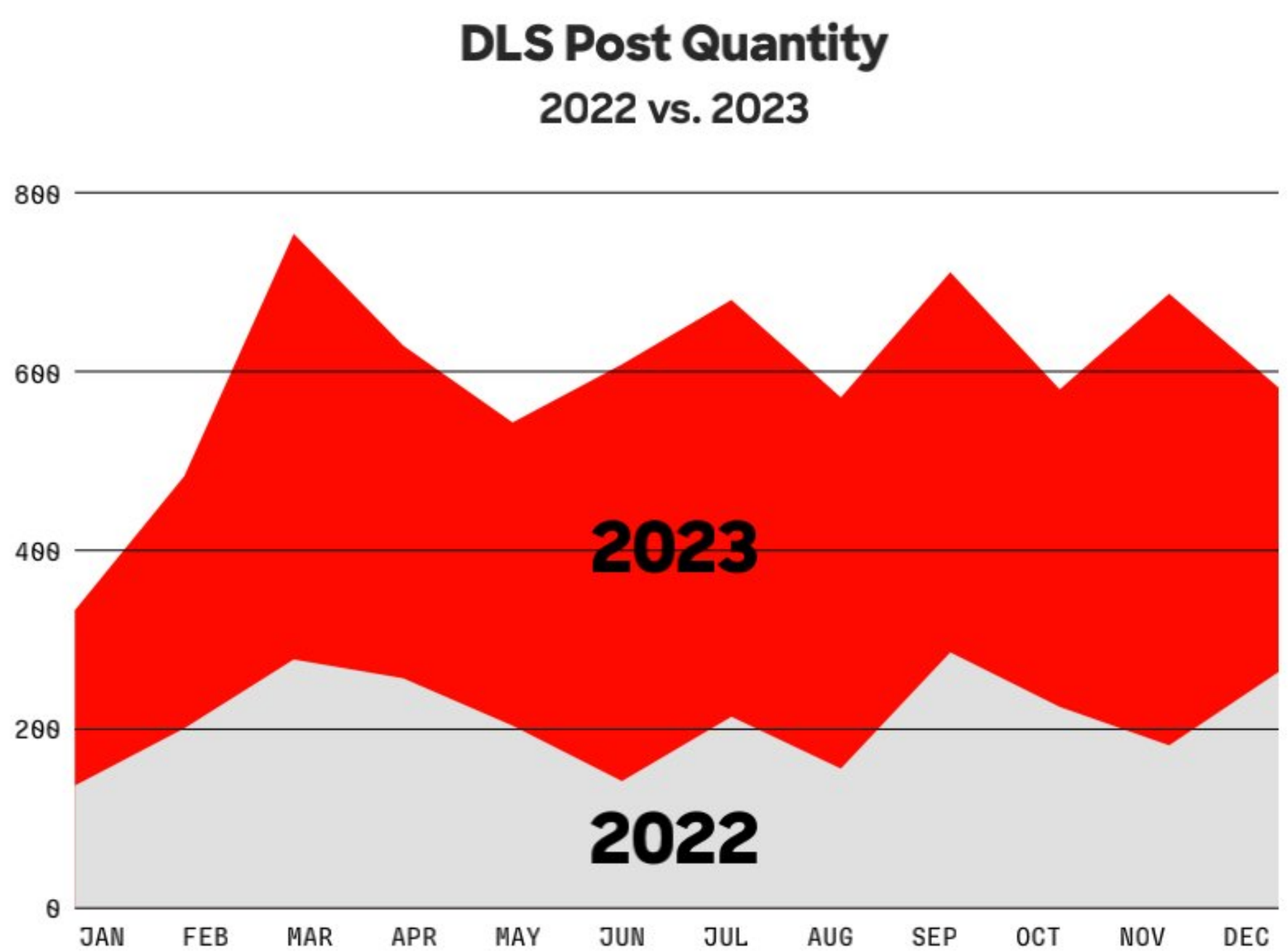


Figure 8. DLS post quantity, 2022 vs. 2023

Collectively, BITWISE SPIDER, ALPHA SPIDER, GRACEFUL SPIDER, RECESS SPIDER and BRAIN SPIDER accounted for 77% of posts across all tracked adversary DLSs. BITWISE SPIDER and ALPHA SPIDER have historically posted numerous new DLS posts and were ranked in first and second place, respectively, for the highest number of DLS posts in 2022 and 2023.

Scanned with OKEN Scanner

RECESS SPIDER and BRAIN SPIDER started their own ransomware operations in mid-2022 and January 2023, respectively. They have since grown in prominence to account for the fourth (RECESS SPIDER) and fifth-highest (BRAIN SPIDER) number of DLS posts in 2023.

GRACEFUL SPIDER — which has operated since 2016 and has typically conducted low-volume campaigns — exploited three zero-day vulnerabilities in 2023 to exfiltrate data from hundreds of victims across the globe. This adversary ultimately published the third-highest number of DLS posts in 2023.

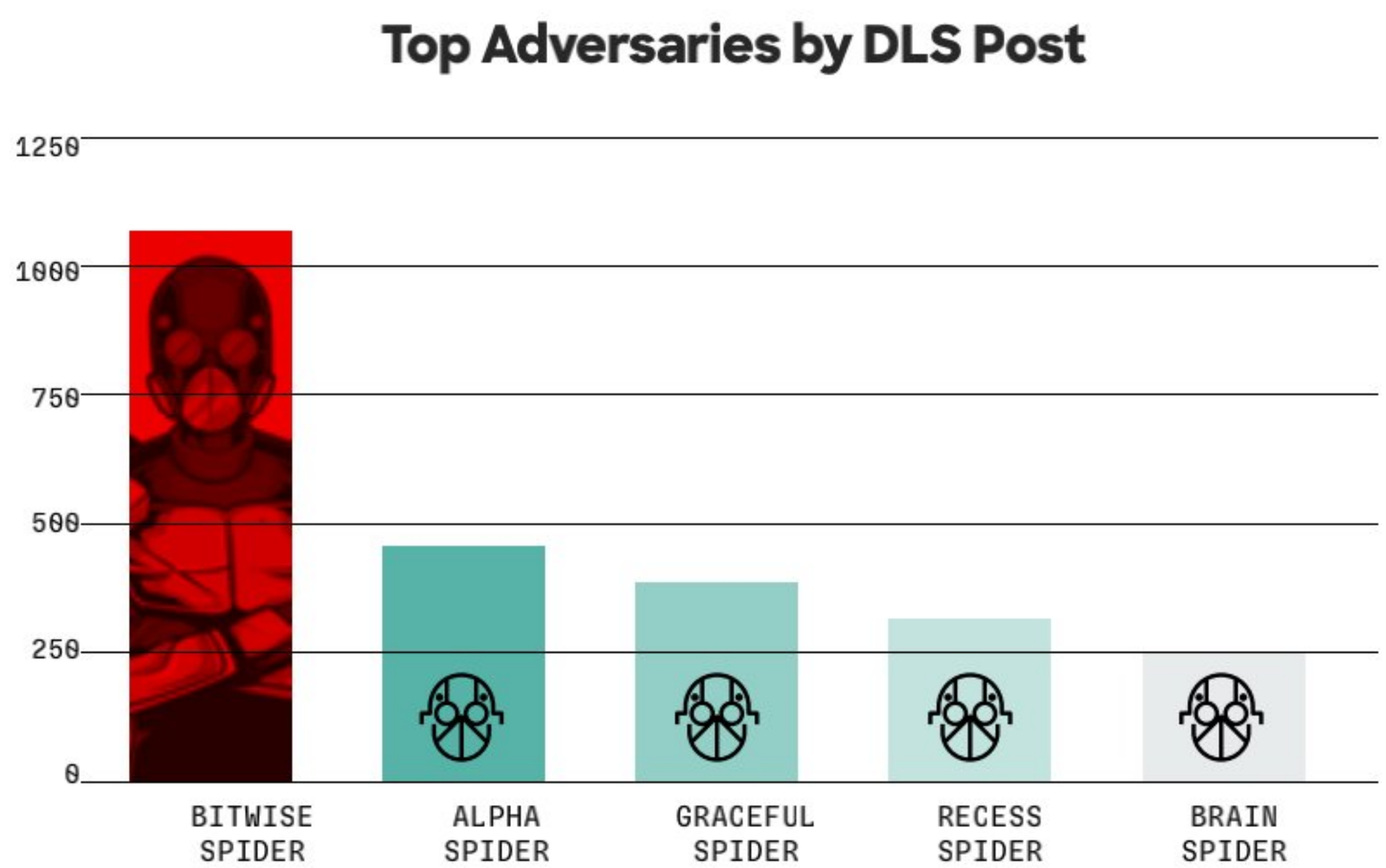


Figure 9. Top five adversaries by DLS posts, 2023

SCATTERED SPIDER Adopts Ransomware as Primary Monetization Method

SCATTERED SPIDER began using ALPHA SPIDER's *Alphv* ransomware in April 2023. The adversary had previously monetized intrusions by selling victim data and SIM swaps as well as stealing cryptocurrency. Adopting ransomware as its primary means of extortion has shifted the scope of the adversary's target profile: Most SCATTERED SPIDER victims in 2023 can be categorized as either reconnaissance targets or monetization targets. Reconnaissance targets are typically organizations in the business process outsourcing, customer relationship management, customer experience, technology and telecom sectors. SCATTERED SPIDER uses intrusions into these entities' networks to identify data that may prove useful in downstream, third-party monetization targeting.

The adversary's monetization target profile is considerably broader. Most directly observed targets include high-revenue — often Fortune 500 — U.S.-based private sector entities. A notable uptick in North American financial services victims occurred in the second half of 2023.

Scanned with OKEN Scanner

Law Enforcement Activity Targets BGH Adversaries

In 2023, various law enforcement agencies targeted BGH adversary operations and their supporting campaigns. Their actions ranged from arresting suspected adversary personnel to technically disrupting adversary infrastructure.

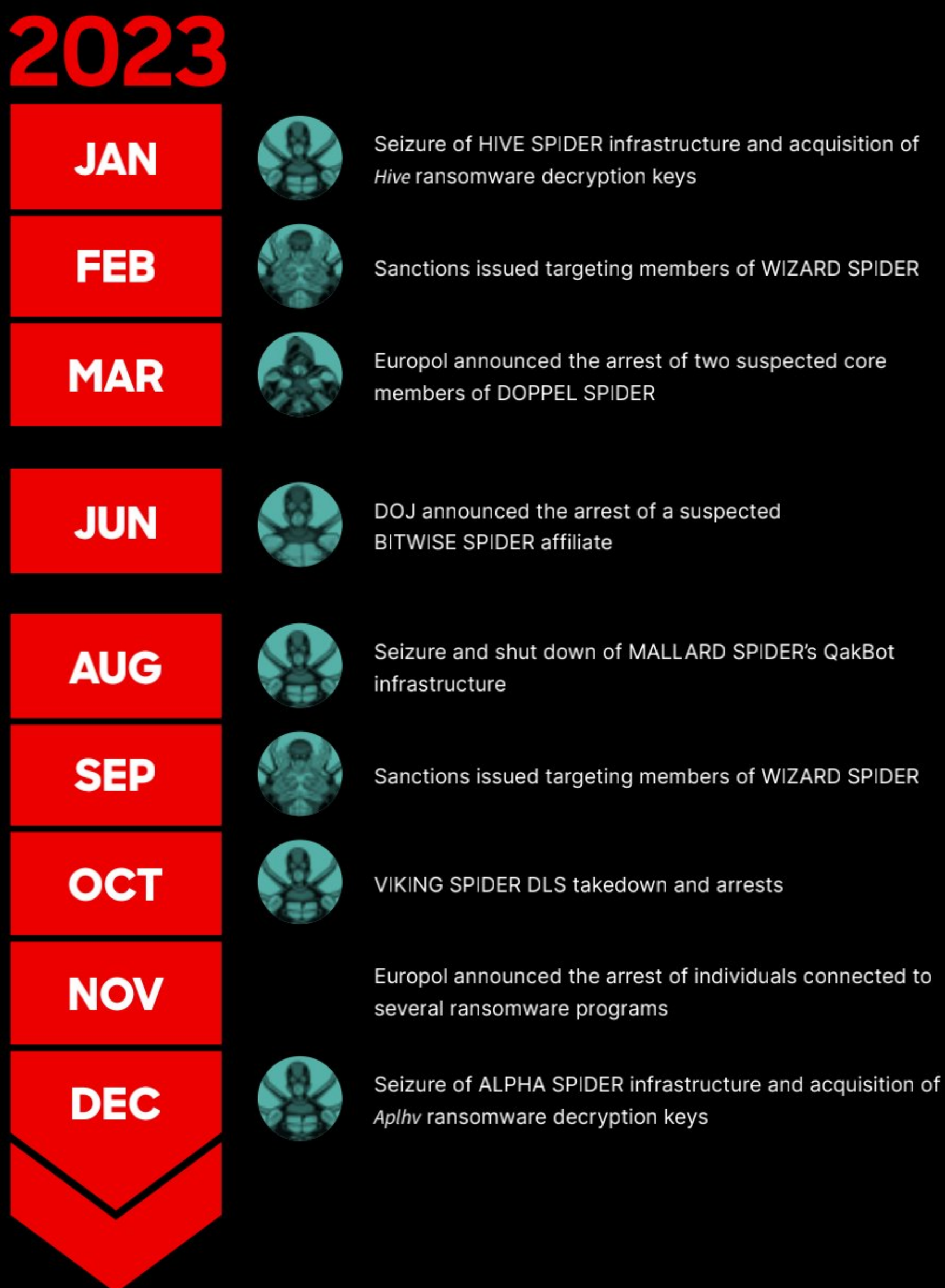


Figure 10. Law enforcement activity against BGH and supporting operations, 2023

Scanned with OKEN Scanner

In January 2023, a coordinated international law enforcement operation resulted in the seizure of HIVE SPIDER infrastructure and acquisition of the *Hive* ransomware decryption key. The U.S. Department of Justice (DOJ) has reportedly maintained access to HIVE SPIDER's internal infrastructure since July 2022 and has since provided decryption keys to more than 300 worldwide victims, preventing ransom payments totaling 130 million USD. No HIVE SPIDER activity has been observed since January 2023; however, *Hive* affiliates have since migrated to other ransomware as a service (RaaS) operations.

In February and September 2023, law enforcement issued sanctions against WIZARD SPIDER members aiming to restrict the named individuals' finances, travel, and assets and disrupt the adversary's operations as it worked to circumvent the restrictions.

In March 2023, Europol announced the arrest of two suspected core DOPPEL SPIDER members. In June 2023, the DOJ announced the arrest of a suspected BITWISE SPIDER affiliate. In August 2023, the FBI announced a multinational operation — using a custom payload to send a shutdown command — that removed MALLARD SPIDER's *QakBot* malware from more than 700,000 hosts and seized a significant amount of cryptocurrency. WANDERING SPIDER also used MALLARD SPIDER's *QakBot*.

In October 2023, law enforcement agencies announced they had taken down VIKING SPIDER's *Ragnar Locker* DLS and arrested a suspected *Ragnar Locker* developer. In November 2023, Europol also announced it had arrested personnel connected to an unnamed ransomware actor. Finally, in December 2023, the FBI seized ALPHA SPIDER's infrastructure, including the *Alphv* DLS — ransomware SCATTERED SPIDER used throughout most of 2023.

The FBI offered an *Alphv* decryption tool to more than 500 ALPHA SPIDER victims, prompting ALPHA SPIDER to migrate its DLS and affiliate panel to new Tor sites while it attempted to regain control of its compromised infrastructure. ALPHA SPIDER then removed targeting restrictions from affiliates, excepting prohibition against targeting entities within the Commonwealth of Independent States.

Scanned with OKEN Scanner

Data Theft and Extortion Optimization

Since 2019, BGH adversaries have threatened to publish stolen data on DLSs as a secondary extortion means in concert with deploying ransomware.[12] In 2023, adversaries continued to invent exploitation methods to steal victim data and increase pressure on victims, with many — including GRACEFUL SPIDER and MASKED SPIDER — adopting data theft as their sole means of extortion.

GRACEFUL SPIDER was the most prolific data theft and extortion actor in 2023. The adversary exploited zero-day vulnerabilities in file-transfer applications GoAnywhere Managed File Transfer and MOVEit Transfer as well as IT management software SysAid On-Premise. GRACEFUL SPIDER's *Clop* ransomware deployment within the scope of these campaigns was not observed, although the adversary exfiltrated and published data to its DLS that belonged to more than 380 victim organizations. To allow broader audience access to leaks, GRACEFUL SPIDER also published victim data on clearweb domains, a technique first used by an ALPHA SPIDER affiliate in 2022.

BGH adversaries have historically and indiscriminately exfiltrated and published stolen victim data. In 2023, these threat actors demonstrated greater focus on stolen data in efforts to maximize pressure on victims, as shown by the following:

- Publishing victim Domain Admin credentials and system IP addresses on the *Black Basta* RaaS DLS. This data could be leveraged by distinct threat actors to target victim organizations.
- Creating separate victim posts for third-party organizations whose data was identified in the victim network but were not subjected to compromises.
- Multiple RaaS affiliates compromised mental and physical healthcare entities and highlighted their access to — and provided previews of — sensitive data and records, including patient photos, in DLS posts.
- VICE SPIDER continued to use a PS script to automate data exfiltration but customized the script to search for directory and filenames containing strings such as `*violence*`, `*abuse*`, `*Theft*`, `*Stealing*`, `*humiliation*`, `*harassment*` and `*death*`, likely to identify data that posed a high potential for embarrassing victim organizations.

Many adversaries, including GRACEFUL SPIDER and MASKED SPIDER, have struggled with cryptographic flaws in their ransomware that enable trivial decryption under specific conditions. In contrast, data theft and extortion offer BGH actors an easier route to monetization, and many simply steal data from a single host or public-facing application. CrowdStrike CAO assesses that BGH adversaries will likely continue to become more targeted in their pursuit of data with a high potential for embarrassing victims.

12 https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1

Scanned with OKEN Scanner

Outlook

The record number of victims named on DLSs throughout 2023 demonstrates BGH's status as the current most significant eCrime threat to organizations across all geographical regions and industries. This increase is driven by various factors, including GRACEFUL SPIDER's zero-day exploitation campaigns, BGH adversaries' continued targeting of unmanaged devices — such as edge gateway devices for initial access and targeting VMware ESXi for encryption — and an increasing number of adversaries naming victims following data theft incidents that did not include ransomware deployment.

Though CrowdStrike CAO assesses that ransomware will highly likely remain the primary extortion method through 2024, BGH adversaries will increasingly emphasize stolen-data exploitation as a means to pressure victims into payment. This is particularly true as U.S. Securities and Exchange Commission (SEC) rules impact major cybersecurity incident disclosures.[13]

SCATTERED SPIDER's *Alphv* ransomware underscored the effectiveness of extortion as a tactic throughout 2023. Though SCATTERED SPIDER previously monetized campaigns through cryptocurrency theft and SIM swaps, ransomware is a more opportunistic tactic, enabling the adversary to broaden its target scope. Barring any successful law enforcement activity targeting the adversary, SCATTERED SPIDER will highly likely remain a critical threat to high-revenue private sector entities in 2024, particularly those based in Europe and North America.

Coordinated international law enforcement operations targeted BGH actors in 2023. These included adversary personnel arrests, technical action against various capabilities, cryptocurrency seizure and sanctioning of named individuals. The disruption of HIVE SPIDER's *Hive* RaaS and MALLARD SPIDER's enabling *QakBot* malware left voids that were quickly filled by competing RaaS and malware as a service (MaaS) actors, demonstrating the eCrime ecosystem's resilience against takedowns that do not arrest the individuals behind the operations.

THE RECORD NUMBER OF VICTIMS NAMED ON DLSs THROUGHOUT 2023 DEMONSTRATES BGH'S STATUS AS THE CURRENT MOST SIGNIFICANT ECRIME THREAT TO ORGANIZATIONS ACROSS ALL GEOGRAPHICAL REGIONS AND INDUSTRIES.

13 https://www.sec.gov/news/press-release/2023-139

Scanned with OKEN Scanner

eCRIME ENABLERS

Malware Delivery Trends Following Mark-of-the-Web Patch on ISO Files

Adversaries in 2023 experimented with malware delivery methods that do not rely on macros or ISO files, following a sharp increase in ISO files being used for malware delivery and a subsequent patch by Microsoft for a Mark-of-the-Web bypass vulnerability in container files in 2022.

The number of malware campaigns using malicious OneNote files for initial access rose significantly[14] between late December 2022 and March 2023, with the technique's earliest adopters including criminals distributing information stealers and commodity malware. By mid-January 2023, large-scale malware distributors such as LUNAR SPIDER, HONEY SPIDER and MALLARD SPIDER began using OneNote files as a primary malware distribution method. In March 2023, Microsoft announced a change that would prevent file types commonly abused by adversaries from being embedded in OneNote files.[15] Following the announcement, the popularity of OneNote files within adversary campaigns rapidly declined.

Though no one technique has emerged as a front-runner to replace OneNote files, adversaries continue to experiment with malware delivery methods. Adversaries such as LUNAR SPIDER, APOTHECARY SPIDER and HERMIT SPIDER have consistently used malvertising and search engine optimization (SEO) poisoning.

Adversaries reliant on spam campaigns use multiple techniques and file types to deliver malware. Several adversaries have used PDF files containing links to files hosted on external URLs as well as HTML smuggling. More novel techniques have included using WebDAV files to distribute payloads. Toward the end of 2023, multiple malware families were distributed in new lures containing fake browser updates.

Malvertising and SEO Poisoning

Malvertising is a technique in which threat actors create malicious advertisements to facilitate criminal activity. Adversaries use SEO poisoning to falsely promote malicious websites to higher ranks in search engine results. Similar to malvertising, SEO poisoning relies on users believing the results closest to the top of a search result are the most credible.

Throughout 2023, adversaries such as LUNAR SPIDER regularly abused Google advertisements to ensure their malicious ads appeared at the top of search result pages. Threat actors such as SolarMarker operators regularly used SEO poisoning throughout 2023.

---

14 https://www.crowdstrike.com/blog/qakbot-ecrime-campaign-leverages-microsoft-onenote-for-distribution/
15 https://learn.microsoft.com/en-us/deployoffice/security/onenote-extension-block

Scanned with OKEN Scanner

Increasing macOS Malware Use

Throughout 2023, multiple macOS malware variants — including *MacOS Stealer, Private MacOS Stealer, ShadowVault* and COOKIE SPIDER's *Atomic macOS Stealer (AMOS)* — emerged on underground marketplaces. All observed macOS malware families are information stealers capable of harvesting stored passwords, cookies and cryptocurrency wallets.

AMOS customers have distributed these tools via SEO poisoning as well as fake play-to-earn games and illegitimate job advertisements. *MacOS Stealer* customers, including BITWISE SPIDER, ROYAL SPIDER and ALPHA SPIDER ransomware affiliates, have praised the stealer. Although COOKIE SPIDER stated that a portion of its current 50 to 100 customers include BITWISE SPIDER and ALPHA SPIDER affiliates, CrowdStrike CAO cannot presently verify this claim.

macOS stealers gained traction in the eCrime ecosystem throughout 2023 due to their ability to enable opportunistic actors and ransomware affiliates during criminal operations. Since the majority of information stealers typically target Windows-based OSs, the increasing number of macOS stealers in the eCrime ecosystem has expanded eCrime profit opportunities.

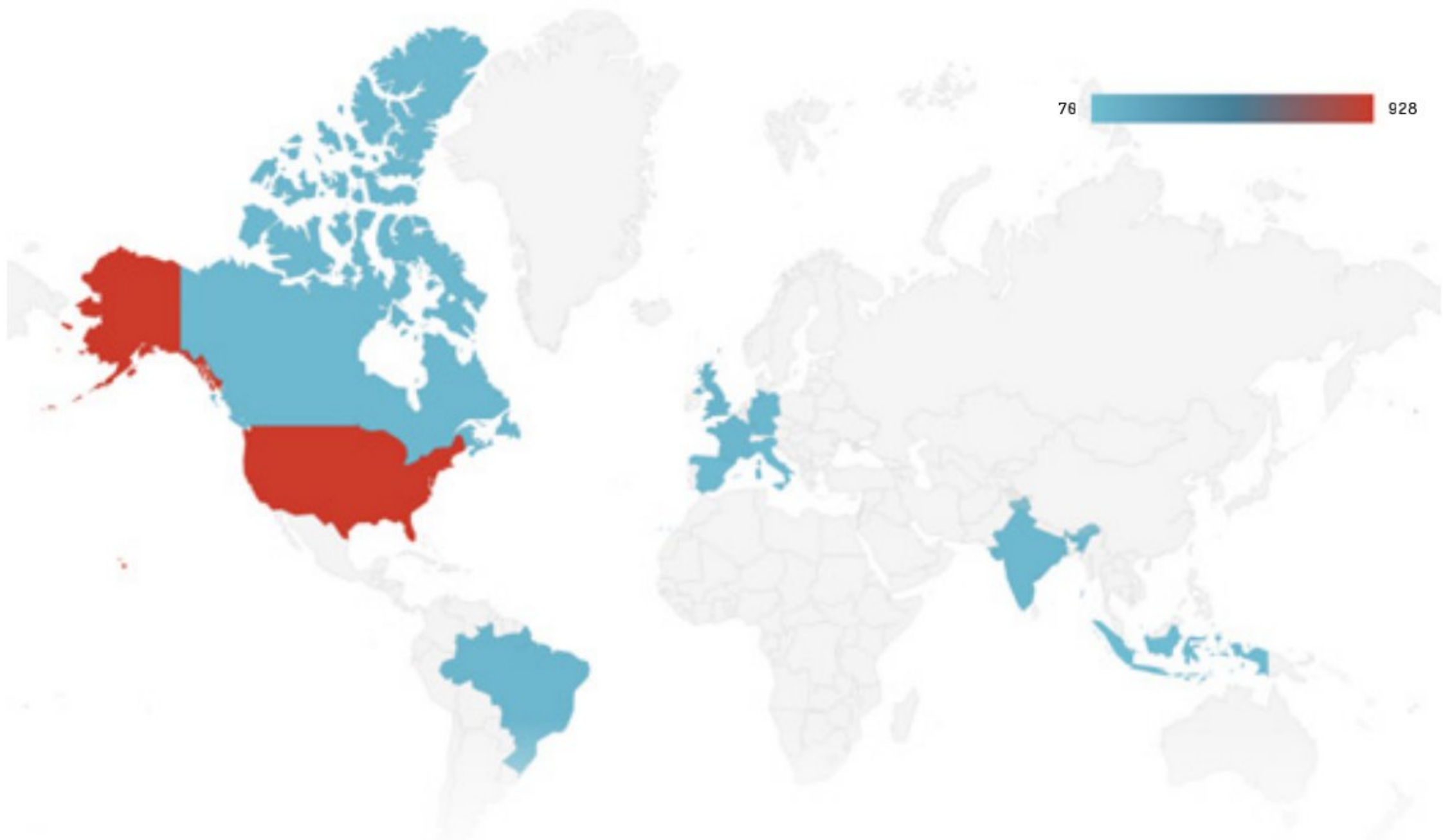
Access Brokers Persistently Provide Access Opportunities

Access brokers continued to profit from providing initial access to a variety of eCrime threat actors in 2023, with the number of accesses advertised increasing by 20% compared to 2022. The academic sector was the most frequently advertised, and advertisements for U.S.-based entities far surpassed all other regions. Initial access TTPs observed in 2023 were relatively consistent with those used in 2022 and regularly targeted and abused compromised credentials.

ACCESS BROKERS CONTINUED TO PROFIT FROM PROVIDING INITIAL ACCESS TO A VARIETY OF eCRIME THREAT ACTORS IN 2023, WITH THE NUMBER OF ACCESSES ADVERTISED INCREASING BY 20% COMPARED TO 2022.

Scanned with OKEN Scanner

TOP ACCESS BROKER ADVERTISEMENTS BY COUNTRY
2023



TOP SECTORS ADVERTISED BY ACCESS BROKERS | 2023

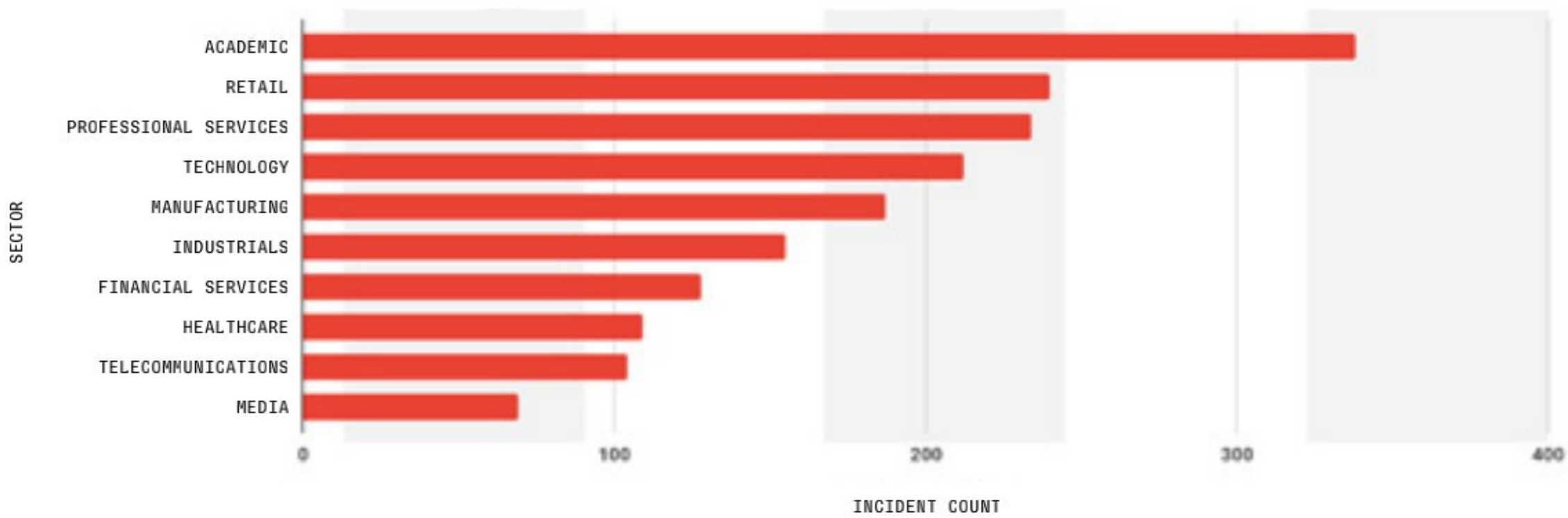


Figure 11. Top 10 countries and sectors advertised by access brokers, 2023

Scanned with OKEN Scanner

Outlook

The rise of macOS malware and the evolution of malware delivery techniques demonstrate the eCrime ecosystem's innovative nature. Furthermore, eCrime enablers regularly copy successful tactics used by other criminal actors, as made evident by the increase of OneNote files for malware delivery.

eCrime enablers will highly likely continue to innovate and offer new products on criminal marketplaces in 2024. This assessment is made with high confidence based on historical trends in the eCrime ecosystem. Malware delivery trends will likely continue to fluctuate, with SEO poisoning and malvertising remaining popular and spam-reliant adversaries proceeding to regularly experiment with different methods. This assessment is made with high confidence based on malware delivery trends observed since the end of 2022.

The access broker threat shows no immediate sign of abating. These threat actors will almost certainly facilitate intrusions into various organizations worldwide throughout 2024 using a mixture of established TTPs alongside commodity and custom tooling.

TARGETED eCRIME

Adversaries Continue Legitimate RMM Tool Use

Throughout 2023, multiple targeted eCrime adversaries — particularly CHEF SPIDER, DISTANT SPIDER and SOLAR SPIDER — heavily used legitimate remote monitoring and management (RMM) tools.

Starting in March 2023, CHEF SPIDER adopted sophisticated social engineering tactics to direct victims to download Inno Setup and ClickOnce installers for RMM tool ConnectWise ScreenConnect. Though CHEF SPIDER has historically targeted point-of-sale systems in the hospitality sector by compromising internet-facing servers, the adversary gradually shifted to targeting U.S.-based hospitality sector service providers, financial service providers and digital marketing firms throughout 2023.

In 2023, DISTANT SPIDER — which universally relies on ConnectWise ScreenConnect — continued deploying MSI installers (aka Windows Installers) for this legitimate RMM tool after exploiting vulnerable internet-facing servers within victim environments. In September 2023, an earlier DISTANT SPIDER ConnectWise ScreenConnect intrusion likely enabled an ALPHA SPIDER affiliate to exfiltrate data and demand a ransom from a victim.

In June 2023, SOLAR SPIDER likely used phishing emails to direct victims to download a ZIP archive hosted on GitHub. This archive contained a loader that abuses DLL search-order hijacking to run the legitimate RMM Remote Management System tool. SOLAR SPIDER has used the legitimate RMM tool NetSupport Manager since at least October 2022.

Scanned with OKEN Scanner

Historical CARBON SPIDER Malware Distributed in Low-Volume Campaigns

Throughout 2023, eCrime actors used numerous malware families previously exclusive to CARBON SPIDER (Figure 12). Since the now-inactive MaaS vendor *Goodsoft* distributed these families in 2022 and 2023, none of these campaigns can be attributed to now-inactive CARBON SPIDER; however, the campaigns demonstrate the tools' enduring popularity. In contrast to typical MaaS operators, the low volume of campaigns using *Goodsoft* tooling likely indicates only a handful of customers were given access.

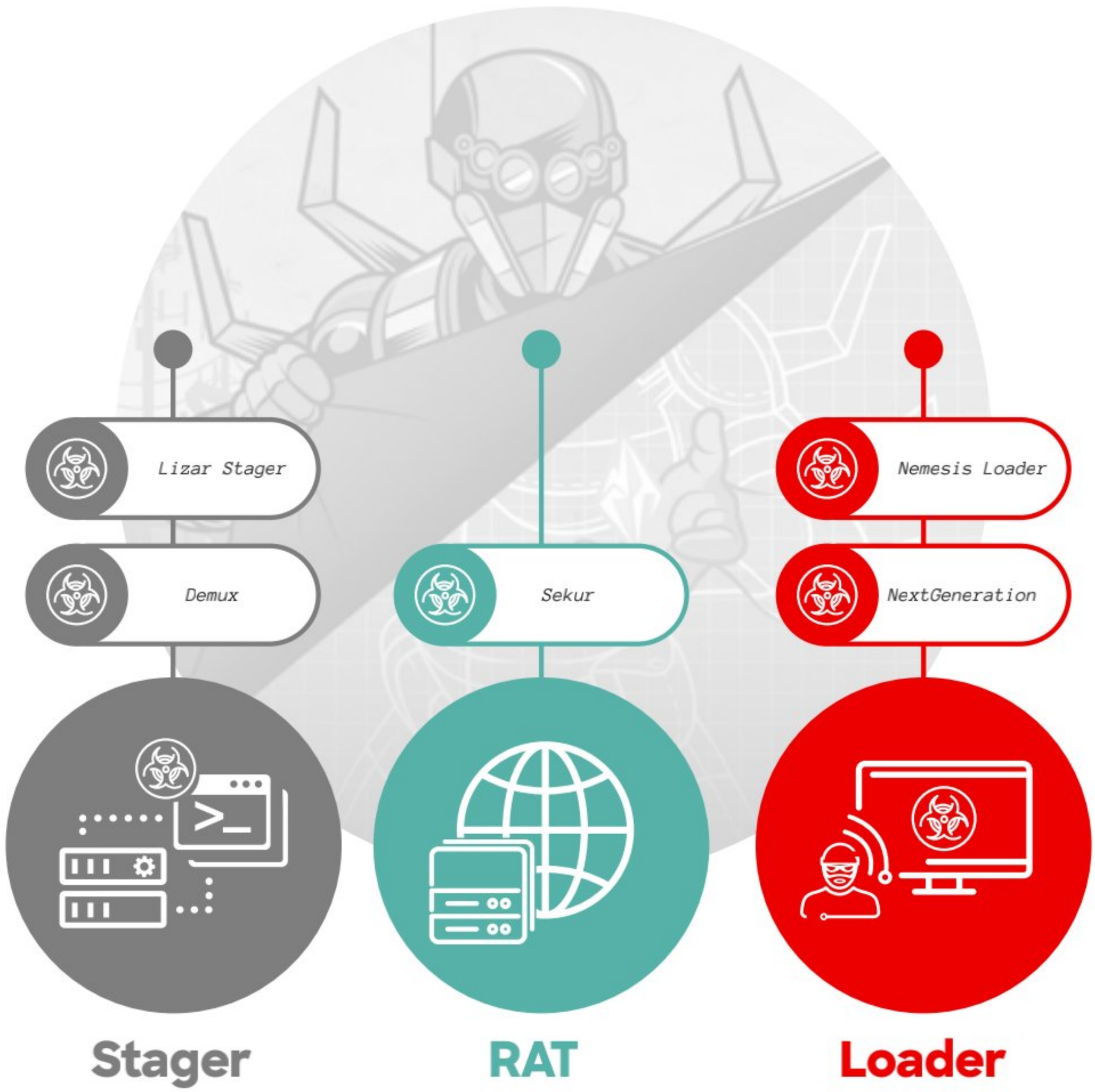


Figure 12. Legacy CARBON SPIDER tooling used in 2023

Scanned with OKEN Scanner

Additional LATAM-Focused Adversaries Identified

In 2023, CrowdStrike CAO named three new SPIDER adversaries focused primarily — but not exclusively — on Latin America (LATAM): ODYSSEY SPIDER, ROBOT SPIDER and SQUAB SPIDER (Figure 13). Including previously identified BLIND SPIDER, four SPIDER adversaries now focus on LATAM targeting.

Figure 13. LATAM-focused SPIDER adversaries

Scanned with OKEN Scanner

AVIATOR SPIDER, BLIND SPIDER and ODYSSEY SPIDER all used ROBOT SPIDER's *Fsociety* crypter service during 2023. *Fsociety* tools typically consist of a set of scripts that download and execute an intermediate .NET payload that subsequently loads a final RAT payload in memory. Throughout 2023, ROBOT SPIDER continued to update the *Fsociety* crypter to improve obfuscation and add capabilities. Generally, infection chains leveraging *Fsociety* culminated in commodity RATs such as *njRAT Lime*.

ODYSSEY SPIDER, which is likely based in Brazil, uses ROBOT SPIDER's *Fsociety* crypter service along with other commodity crypters and RATs. ODYSSEY SPIDER predominantly focuses on the travel and hospitality sectors in LATAM and Southeastern Europe, specifically aiming to monetize payment card details entered during travel-related booking processes. However, in Q3 2023, the adversary began targeting numerous other sectors and regions, likely while leveraging local tax return periods.

SQUAB SPIDER primarily targets financial institutions, particularly but not exclusively those based in Mexico. The adversary achieves initial access by exploiting web servers to deploy a wide set of webshells. From there, threat actors rely on passive BLUEAGAVE bind shells or simple listeners to enable lateral movement through a network and to generally avoid conventional C2 traffic. SQUAB SPIDER likely attempts to steal transaction-related data from victims.

Outlook

Though opportunistic BGH campaigns remain the primary eCrime threat across all sectors, a smaller eCrime actor subset will likely continue targeted eCrime campaigns seeking to steal payment card- or transaction-related data from victims. As with the BGH ecosystem, legitimate RMM tools will likely remain popular among targeted eCrime operations due to their widespread use within normal business processes. The endurance of LATAM-focused adversaries BLIND SPIDER, ODYSSEY SPIDER, ROBOT SPIDER and SQUAB SPIDER highlights how the LATAM-targeted eCrime ecosystem will likely persist in the mid-term.

Scanned with OKEN Scanner

Conclusion

Over the course of 2023, CrowdStrike CAO observed adversaries across the targeted intrusion, eCrime and hacktivist landscapes operating with unprecedented stealth. The ability to operate undetected remains paramount for malicious actors, and today's sophisticated cybercriminals continue to discover new methods to increase effectiveness, enhance operations and achieve objectives.

eCrime remained a 2023 threat landscape cornerstone, with BGH adversaries SCATTERED SPIDER and GRACEFUL SPIDER accounting for most activity. CrowdStrike CAO assesses BGH will continue to pose the dominant threat within the eCrime landscape in 2024. This assessment is made with high confidence based on the continued success of these operations, as observed in the 76% growth in DLS posts in 2023. Trends likely to be observed in 2024 in support of BGH operations include ransomware-free data leak operations and an increase in cloud-conscious operations.

The number of cloud-conscious threat actors continued to grow in 2023 — as in 2022 — and will highly likely continue to grow in 2024. Adversaries are highly motivated to invest in and use cloud and other new technologies, such as generative AI, to increase the efficiency and success of their operations. Cloud-aware adversaries will look to detect, enumerate and navigate cloud environments to harvest valuable proprietary information from Microsoft 365, SharePoint and code repositories. They will use this information in ongoing operations and ransom negotiations or simply sell it to other eCrime adversaries.

Financially motivated adversaries also increasingly realized the benefits of dedicated relationships in 2023 and were likely able to increase resulting operational success rates. Access brokers and RaaS actors will likely continue to forge dedicated relationships in 2024. The coming year will also likely include enhancements in social engineering effectiveness, MFA bypass and third-party provider targeting in efforts to leverage a single larger point of access.

Scanned with OKEN Scanner

High-profile geopolitical conflicts — namely the Russia-Ukraine and Israel-Hamas conflicts — generated significant targeted intrusion and hacktivist cyber activity in 2023, particularly for Iran-nexus and Russia-nexus adversaries. In 2024, these and other high-profile conflicts will remain as significant hacktivism drivers.

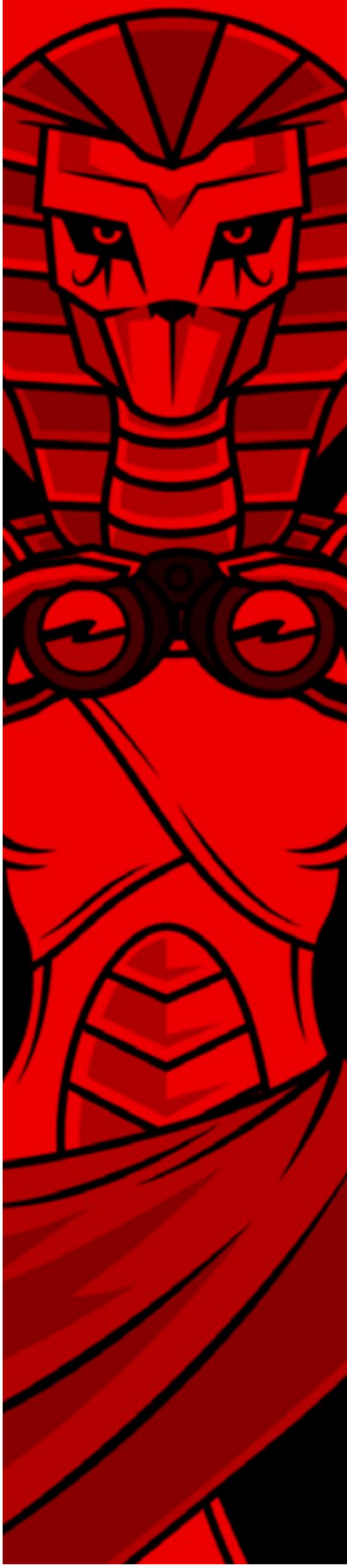
Beyond cyber activity related to the Israel-Hamas conflict, Iran-nexus adversaries remained consistent in targeting telecom organizations, a trend likely to continue in 2024. Russia-nexus adversaries also persisted in their targeting of Ukraine, NATO members and partner countries. They will almost certainly continue to conduct intelligence collection operations and IO in these geographies in 2024.

CrowdStrike CAO graduated several activity clusters to named adversaries in 2023, including the first-ever Egypt-nexus adversary, WATCHFUL SPHINX. Consistent with previous assessments, CrowdStrike CAO expects the majority of established adversaries and activity clusters to continue to expand or update their capabilities in 2024. Fewer adversaries and activity clusters around the world are likely to expand their assessed target scope; rather, they will likely continue to focus on historical and predominantly regional target sets.

Within the vulnerability threat landscape, CrowdStrike CAO assesses that several 2023 trends — namely, edge device and EOL product targeting — will persist in 2024. eCrime threat actors remained the primary threat to most mobile users in 2023 and will likely continue as such in 2024. Targeted intrusion actors will also almost certainly continue to target mobile devices, with increases in platform and device security causing less sophisticated adversaries to struggle to operate successfully in that space.

With the creation of Counter Adversary Operations, CrowdStrike remains steadfast in its mission to stop breaches. Combining best-in-class threat intelligence with a professional, managed threat hunting service unlike anything else offered in the industry, CrowdStrike ensures its customers can access industry-leading information to drive their individual operational success.

CrowdStrike CAO remained focused on disrupting the adversary in 2023 and will continue to deliver unparalleled threat intelligence in 2024 and beyond.



Scanned with OKEN Scanner

Recommendations

1 Make identity protection a must-have

Due to high success rates, identity-based and social engineering attacks surged in 2023. Stolen credentials grant adversaries swift access and control — an instant gateway to a breach. To counter these threats, it is essential to implement phishing-resistant multifactor authentication and extend it to legacy systems and protocols, educate teams on social engineering and implement technology that can detect and correlate threats across identity, endpoint and cloud environments. Cross-domain visibility and enforcement enables security teams to detect lateral movement, get full attack path visibility and hunt for malicious use of legitimate tools. Addressing sophisticated access methods such as SIM swapping, MFA bypass and the theft of API keys, session cookies and Kerberos tickets requires proactive and continuous hunting for malicious behavior.

2 Prioritize cloud-native application protection platforms (CNAPPs)

Cloud adoption is exploding as companies realize the potential for innovation and business agility that the cloud offers. Due to this growth, the cloud is rapidly becoming a major battleground for cyberattacks. Businesses need full cloud visibility, including into applications and APIs, to eliminate misconfigurations, vulnerabilities and other security threats. CNAPPs are critical: Cloud security tools shouldn't exist in isolation, and CNAPPs provide a unified platform that simplifies monitoring, detecting and acting on potential cloud security threats and vulnerabilities. Select a CNAPP that includes pre-runtime protection, runtime protection and agentless technology to help you discover and map your apps and APIs running in production, showing you all attack surfaces, threats and critical business risks.

3 Gain visibility across the most critical areas of enterprise risk

Adversaries often use valid credentials to access cloud-facing victim environments and then use legitimate tools to execute their attack, making it difficult for defenders to differentiate between normal user activity and a breach. To identify this type of attack, you need to understand the relationship between identity, cloud, endpoint and data protection telemetry, which may be in separate systems. In fact, the average enterprise uses 45+ security tools, creating data silos and gaps in visibility. By consolidating into a unified security platform with AI capabilities, organizations have complete visibility in one place and can easily control their operations. With a consolidated security platform, organizations save time and money and can quickly and confidently discover, identify and stop breaches.

Scanned with OKEN Scanner

4 Drive efficiency: Adversaries are getting faster — are you?

It takes adversaries an average of 62 minutes — and the fastest only 2 minutes — to move laterally from an initially compromised host to another host within the environment. Can you keep up? Let's face it — legacy SIEM solutions have failed the SOC. They are too slow, complex and costly, and they were designed for an age when data volumes — and adversary speed and sophistication — were a fraction of what they are today. You need a tool that's faster, easier to deploy and more cost-effective than legacy SIEM solutions. Investigate better approaches, such as CrowdStrike Falcon® Next-Gen SIEM, which unifies all threat detection, investigation and response in one cloud-delivered, AI-native platform for unrivaled efficiency and speed. Or, if you don't have an internal SOC team, consider 24/7 managed detection and response (MDR).

5 Build a cybersecurity culture

Though 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 tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

Scanned with OKEN Scanner

CrowdStrike Products and Services

Endpoint Security

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 INSIGHT XDR | DETECTION AND RESPONSE FOR ENDPOINT AND BEYOND

Offers industry-leading, unified EDR and extended detection and response (XDR) with enterprise-wide visibility to automatically detect adversary activity and respond across endpoints and all key attack surfaces

FALCON COMPLETE | MANAGED DETECTION AND RESPONSE

Stops and eradicates threats in minutes with 24/7 expert management, monitoring and surgical remediation, proactive threat hunting, and integrated threat intelligence — all backed by the industry's strongest Breach Prevention Warranty

FALCON COMPLETE XDR | MANAGED EXTENDED DETECTION AND RESPONSE (MXDR)

Expands Falcon Complete's industry-leading MDR service with cross-domain XDR protection run by CrowdStrike's elite 24/7 expertise, proactive threat hunting and native threat intelligence

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 SECURITY

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

FALCON FOR MOBILE | ENDPOINT DETECTION AND RESPONSE

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

Scanned with OKEN Scanner

Counter Adversary Operations

FALCON ADVERSARY OVERWATCH™ | UNIFIED THREAT HUNTING

Provides around-the-clock protection across endpoint, identity and cloud workloads delivered by AI-powered threat hunting experts, and includes built-in threat intelligence to expose adversary tradecraft, vulnerabilities and stolen credentials

FALCON ADVERSARY INTELLIGENCE | SOC AUTOMATION

Cuts response time from days to minutes across the entire security stack with end-to-end intelligence automation, and enables you to instantly submit potential threats to an automated sandbox, extract indicators of compromise and deploy countermeasures — all while continuously monitoring for fraud and safeguarding your brand, employees and sensitive data

FALCON ADVERSARY HUNTER | INTEL-LED THREAT HUNTING

Provides world-class intelligence reporting, technical analysis, and threat hunting and detection libraries, and cuts the time and cost required to understand and defend against sophisticated nation-state, eCrime and hacktivist adversaries

FALCON COUNTER ADVERSARY OPERATIONS ELITE

ON-DEMAND ANALYST

Provides an assigned analyst who uses advanced investigative and threat hunting tools powered by deep adversary intelligence to identify and disrupt adversaries across your IT environment and beyond

Cloud Security

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)

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

FALCON CLOUD SECURITY FOR MANAGED CONTAINERS

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

Scanned with OKEN Scanner

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 GCP

FALCON COMPLETE CLOUD SECURITY

MDR FOR CLOUD WORKLOADS

Provides a fully managed cloud workload protection service, delivering 24/7 expert security management, threat hunting, monitoring and response for cloud workloads, backed by CrowdStrike's industry-leading Breach Prevention Warranty

Identity Protection

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

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

FALCON COMPLETE IDENTITY THREAT PROTECTION

MANAGED 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 24/7 by CrowdStrike's team of experts

Security and IT Operations

FALCON DISCOVER | IT HYGIENE

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

FALCON SPOTLIGHT | VULNERABILITY MANAGEMENT

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

Scanned with OKEN Scanner

FALCON EXPOSURE MANAGEMENT | EXPOSURE MANAGEMENT

Allows security teams to prioritize exposures making the biggest impact and proactively reduce an adversary's opportunity for compromise and lateral movement

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

FALCON DATA PROTECTION | UNIFIED DATA PROTECTION

Provides deep real-time visibility into what is happening with sensitive data and stops data theft with policy enforcement that automatically follows content, not files

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

FALCON FOR IT | AUTOMATED WORKFLOWS

Extends the Falcon platform to automate IT and security workflows with an end-to-end, visibility-to-action life cycle

Next-Gen SIEM

FALCON NEXT-GEN SIEM | SIEM AND LOG MANAGEMENT

Empowers you to swiftly shut down adversaries and slash SOC costs by unifying industry-leading detection, world-class intelligence, blazing-fast search and AI-led investigations in one cloud-delivered platform

CrowdStrike Services

INCIDENT RESPONSE

Stop active breaches and restore order with the most informed and capable IR team available

- Incident Response
- Compromise Assessment
- Endpoint Recovery
- Network Detection Services
- Services Retainer

Scanned with OKEN Scanner

STRATEGIC ADVISORY SERVICES

Develop and mature the security program to improve defenses

- Tabletop Exercise
- Maturity Assessment
- Ransomware Defense Assessment
- SOC Assessment
- SEC Readiness
- Board and CXO Briefings

RED TEAM SERVICES

Stress-test and validate defenses through simulated attacks

- Penetration Testing
- Red Team/Blue Team Exercise
- Adversary Emulation Exercise

CLOUD AND IDENTITY SERVICES

Proactively secure the new perimeter

- Identity Security Assessment
- Cloud Security Assessment
- Red Team/Blue Team Exercise for Cloud
- Cloud Compromise Assessment

TECHNICAL ADVISORY SERVICES

Audit and address security gaps to tangibly reduce risk

- Technical Risk Assessment
- Cyber Threat Risk Evaluation

TRAINING AND SECURITY UPSKILLING

Become security experts under CrowdStrike tutelage

Scanned with OKEN Scanner

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 | X | LinkedIn | Facebook | Instagram

Start a free trial today: www.crowdstrike.com/free-trial-guide

© 2024 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.

Scanned with OKEN Scanner