MANDIANT
NOW PART OF Google Cloud

ISSUE 2

The Defender's Advantage Cyber Snapshot

The Defender's Advantage Cyber Snapshot was developed with one overarching goal: to provide insights into cyber defense topics of growing importance based on Mandiant frontline observations and real-world experiences. This issue covers a wide range of topics, from threat analysis to cyber defense best practices.

How Information Operations Lead to Disinformation and Misinformation

Information operations (IO) refers to the use of coordinated, inauthentic online assets and/or deceptive tactics to influence target audiences. As a tactic, IO has been growing in scale, frequency and scope during the past few years, as nation-states and other groups around the world seek new ways to influence or manipulate target audiences.

Mandiant tracks a range of activity across the online influence spectrum to generate intelligence that contributes to the exposure and mitigation of threats that result from IO. For years, Mandiant has identified and reported on IO campaigns judged to be operating in support of, or on behalf of nation-state actors, including Belarusian, Russian, Chinese and Iranian campaigns as well as information operations conducted by actors unaffiliated with any nation-state. Our primary focus is to identify, analyze and expose efforts to manipulate target information environments using deceptive tactics.

A look across DRAGONBRIDGE

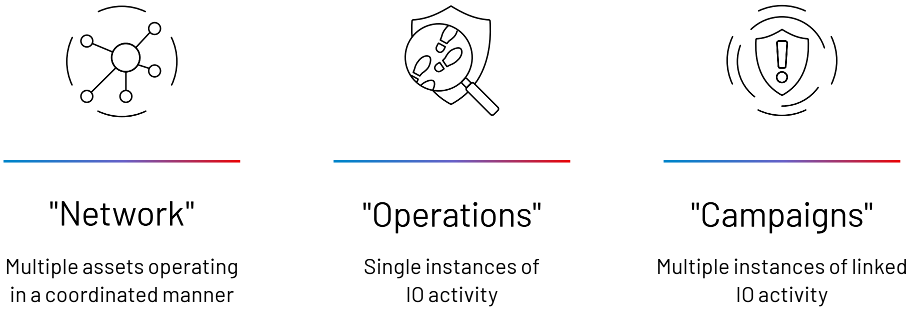
In June, Mandiant released a blog[1] on the DRAGONBRIDGE influence campaign, a pro-Chinese operation first identified in 2019 comprising a network of thousands of fake accounts across many platforms, sites and forums.

In late 2021, DRAGONBRIDGE began changing tactics, moving away from the blunt techniques typically seen in pro-Chinese influence campaigns in favor of a more nuanced approach. Rather than reposting fake news articles, DRAGONBRIDGE accounts began posing as local residents of a region in Texas and feigned concern over environmental and health issues surrounding a new rare-earth element refining plant being constructed by Lynas Rare Earths Ltd.

Evolving campaigns increase potential risks

This campaign attempted to spur local opposition to the construction and is part of a wider effort by pro-Chinese campaigns to use more nuanced and mature tactics to influence public opinion. Microtargeting audiences favorable to its messaging and leveraging criticism by real individuals to support its narratives and agenda are more sophisticated tactics that have also been deployed. However, it has performed poorly, limiting the campaign's ability to effectively garner significant engagement. In the past, DRAGONBRIDGE has used tactics like these to try to mobilize protesters in the U.S. and sow civil unrest.

DRAGONBRIDGE's broad targeting of the rare-earths industry and specific subset of those companies demonstrates an interest in industries of strategic importance to China that we had not previously observed from the campaign. Given Chinese President Xi Jinping's continued emphasis on a broad, holistic understanding of their national security that encompasses areas including information and resource security, we may see global competitors to Chinese firms in other industries targeted by such information operations.



"Network"

Multiple assets operating in a coordinated manner

"Operations"

Single instances of IO activity

"Campaigns"

Multiple instances of linked IO activity

Figure 1. How Mandiant classifies networks, operations, and campaigns as related to IO.

[1] Mandiant (June 28, 2022). Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance.

Information operations pose a very real threat to the security of nations, organizations and individuals, but the threats IO can bring to bear on these victims can vary drastically. For example, influence operations can:

- Damage the reputation of private, commercial and governmental entities
- Influence democratic elections and exacerbate political unrest
- Destabilize social dynamics in regions undergoing conflict
- Encourage or drive physical harm to organizations, individuals and marginalized groups
- Influence public discussion on various topics

Spectrum of government-aligned online influence

Online information environments can be shaped by a spectrum of state-aligned influence activity. Activity within the spectrum ranges from overt communications via official and public channels to covert communications leveraging deceptive tactics and assets so as not to disclose ties to the original sponsor. IO actors sometimes amplify the impact of threat activity by operating in parallel on different sections of the online influence spectrum.

Actors often use covert methods to disseminate or promote content containing desired narratives and disinformation techniques to influence their target audience. Mandiant also observes that some of the most effective IO involve strategically spreading true or partially true information.

Online influences (Fig. 2) include:

- **Official government communications.** Press releases, indictments and posts by official government entity accounts such as ministry of foreign affairs accounts. This public messaging may include factual information and disinformation aimed at swaying public opinion.
- **Individual officials' statements.** Posts or statements made by individuals actively employed or directly affiliated with a government. These statements may vary from the official policies and positions or rogue statements from government ministers.
- **State-linked media.** Outlets that are directly or indirectly controlled or financially supported by a government (such as articles published to state media outlets' webpages, television programs and social media posts by the outlets or their employees).
- **Government-aligned content producers.** Individuals or entities whose motives or objectives align with that of a government. May have varying or unknown degrees of affiliation with the government.
- **Information operations.** Politically motivated efforts to manipulate target information environments using deceptive tactics or coordinated, inauthentic online assets.

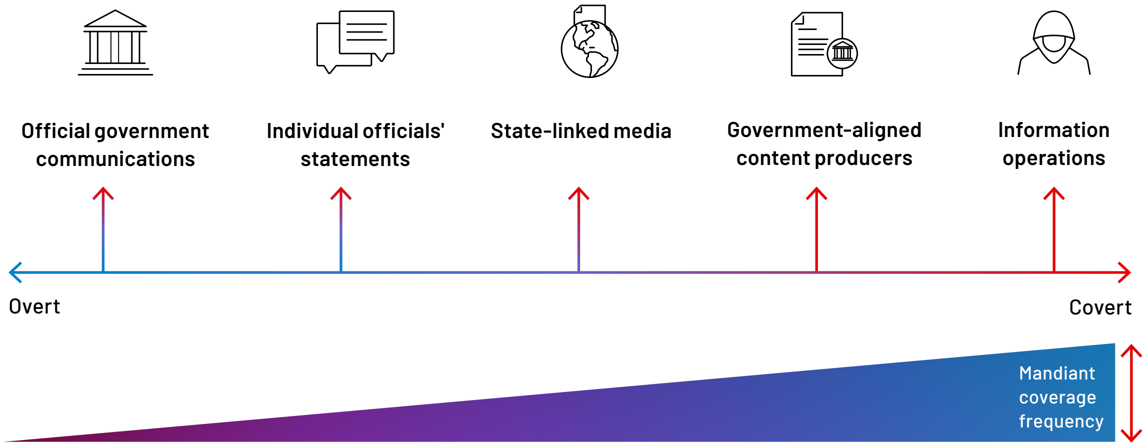
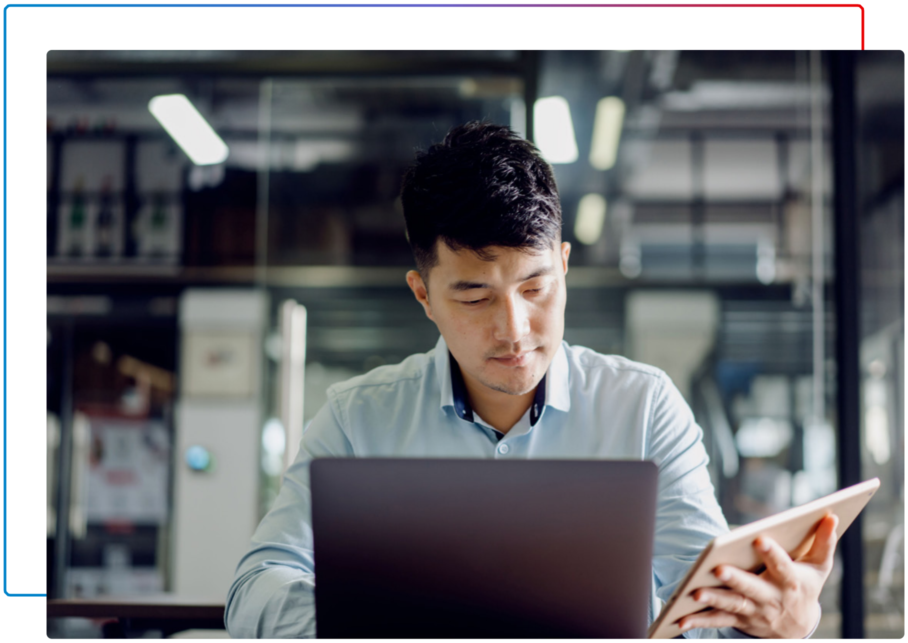

Official government communications
Individual officials' statements
State-linked media
Government-aligned content producers
Information operations
Overt
Covert
Mandiant coverage frequency

Figure 2. Online influence spectrum.



The evolution of IO

Information operations and the actors who conduct them are evolving rapidly. State-aligned actors who sought to influence the 2016 presidential elections in the United States are now conducting widespread IO campaigns to bolster the positive perception of the Russian invasion of Ukraine to the Russian people. The Chinese-linked DRAGONBRIDGE campaign recently attempted to sway public opinion against the expansion of rare-earth minerals mining and refining operations in the U.S. and Canada, likely as an attempt to protect China's heavy investments in rare-earth production.

Mandiant finds that these kinds of campaigns are happening constantly. We regularly see new actors who operate on behalf of nation-states that have never before demonstrated a significant cyber capability.

The most concerning trends seen in the IO space concern hack-and-leak campaigns. Hack-and-leak IO campaigns are cyber operations in which an attacker breaks into a victim's network, steals sensitive, damaging data and leaks it publicly to influence a given audience. In many cases, hack-and-leak operators will alter the material they steal to make it seem even more damaging.

These IO campaigns have had significant impacts in the past, including during the 2016 presidential election in the U.S. As an increasing number of actors adopt IO as a viable means to achieve their goals every year, campaigns will continue to evolve as their capabilities improve.

Threats to Cryptocurrencies and NFTs

While cryptocurrencies are not inherently tied to illicit use, criminal and nation-state actors do abuse cryptocurrency platforms and users in two ways. The first is direct theft of digital assets for profit and the second is to use accounts, platforms and protocols to facilitate illicit transactions such as extortion payments, money laundering and sanctions evasion.

What is cryptocurrency?

A cryptocurrency is a type of virtual currency that uses cryptographic algorithms to control the generation of transactions using the currency. According to Pew Research Center, the number of users on cryptocurrency platforms, the number of platforms and the financial organizations leveraging cryptocurrencies have significantly increased in recent years, expanding the attack surface and number of potential victims for malicious actors.[2] In 2021, researchers at the University of Chicago reported that 13% of Americans traded cryptocurrency in one year, compared to 24% of Americans who had invested in stocks in the same period of time.[3] Cryptocurrency exchange Crypto.com reports indicate that there were approximately 221 million cryptocurrency users throughout the globe as of June 2021.[4]

Threats to cryptocurrencies

Mandiant has tracked financially motivated threat actors' interest in compromising cryptocurrency platforms and wallets for several years, including a notable rise beginning in early 2020.[5,6] The pace and size of cryptocurrency platform thefts accelerated in 2021[7] and early 2022. According to Chainalysis, the value of cryptocurrency stolen in 2021 reached approximately $3.2 billion, over five times the value stolen in 2020.[8]

[2] Pew Research Center (November 2021). 16% of Americans say they have ever invested in, traded or used cryptocurrency.
[3] CNBC (July 2021). PERSONAL FINANCE 13% of Americans traded crypto in the past year, survey finds.
[4] Mint (July 2021). Crypto users double to 200 million in 4 months fuelled by bitcoin, Shib, doge.
[5] Mandiant (2018). Cryptocurrency and Blockchain Networks: Facing New Security Paradigms.
[6] Mandiant (2018). How the Rise of Cryptocurrencies Is Shaping the Cyber Crime Landscape: The Growth of Miners.
[7] Mandiant (2022). Tracking Threat Actor Usage of Cryptocurrencies with Chainalysis.
[8] Chainalysis (2022). The Chainalysis 2022 Crypto Crime Report.

Mandiant observed threat actors exploit vulnerabilities and misconfigurations in websites, applications, authentication mechanisms and smart contracts to compromise cryptocurrency platforms and decentralized finance (DeFi) protocols and exchanges. Threat actors used fake cryptocurrency apps, credential collection malware and social engineering to compromise wallets. Many threat actors were identified on underground forums advertising sales of illicit accesses, vulnerabilities and databases associated with cryptocurrency exchanges and users.

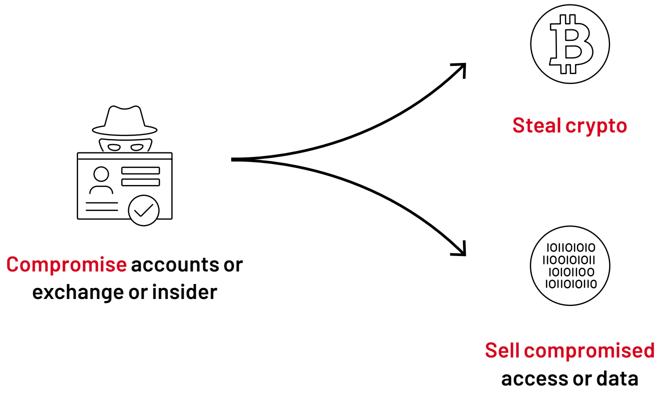

Compromise accounts or exchange or insider
Steal crypto
Sell compromised access or data

Figure 3. Targeting cryptocurrencies.

Cryptocurrency payments and money laundering

Cyber criminals often use cryptocurrencies to pay for illicit goods and services, collect extortion payments or launder money stolen through other malicious activity.

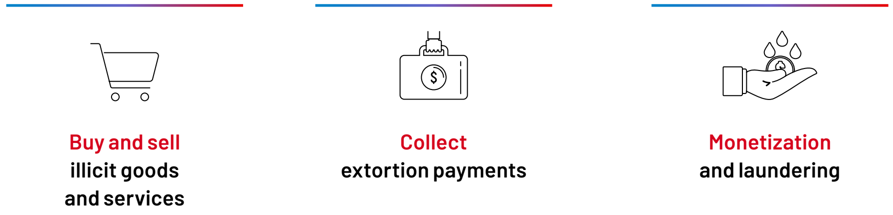

Buy and sell illicit goods and services
Collect extortion payments
Monetization and laundering

Figure 4. Transacting in cryptocurrencies.

In early 2022, the U.S. Department of Justice (DOJ) announced it had arrested a couple for an alleged conspiracy to launder cryptocurrency that was stolen during a 2016 breach of Bitfinex, a virtual currency exchange, valued at approximately $4.5 billion in February 2022.[9] Law enforcement seized more than $3.6 billion in cryptocurrency linked to the incident, but the couple purportedly successfully laundered $2.9 million worth of bitcoin, converting the illicit cryptocurrency into gold, non-fungible tokens (NFTs) and Walmart gift cards.[10]

State sponsored actors targeting crypto

Mandiant assesses with moderate confidence that state-sponsored threats, especially those from North Korea, regularly pose a moderate-to high-intensity risk to cryptocurrency platforms. Specifically, we believe North Korean actors including, but not limited to, APT38 have targeted financial entities, investment services, eCommerce, cryptocurrency users and exchanges and transaction processing organizations across the globe as part of an effort to identify alternative revenue streams and evade sanctions.[11]

CNN, Mandiant and open sources highlighted North Korean efforts to gain employment at cryptocurrency-focused organizations in April and May 2022.[12] These activities appear to be consistent with a May 2022 U.S. government advisory on North Korean IT workers posing as non-North Korean nationals to gain employment to generate revenue for Democratic People's Republic of Korea (DPRK) programs.[13]

Non-fungible tokens

Non-fungible tokens (NFTs) are marketed as unique and/or limited edition blockchain-based digital assets that can be used to represent media downloadable in a file form, including art and music. Notably, NFTs are not subject to copyright protection and ownership of a file's metadata is a far cry from outright ownership of an entity. NFTs have seen a rise in popularity over the last few years given their significantly high market valuations and perceived immutability. Open sources estimate the NFT marketplace represented $41 billion in 2021, closing in on the value of the conventional art and antiquities market at $50 billion.[14]

Because NFTs are bought, sold and stored similarly to other digital tokens such as cryptocurrency, they are susceptible to many of the same threats that target cryptocurrency platforms, users and smart contracts. Mandiant has observed that threat actors have leveraged social engineering and credential theft to compromise both NFT user accounts and exploit software vulnerabilities and misconfigurations in NFT marketplace platforms, all to steal digital assets. We have also detected threat actors advertising stolen databases, compromised user accounts, phishing pages, webinjects and soliciting partners for NFT scams in late 2021 and early 2022.

[9] Department of Justice (Februrary 2022). Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency.

[10] New York Magazine (February 2022). Many Lives of Crypto's Most Notorious Couple, How the accused bitcoin launderers spent their time.

[11] Mandiant (March 2022). Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations.

[12] CNN (July 2022). Here's how North Korean operatives are trying to infiltrate US crypto firms.

[13] U.S. Department of State, U.S. Department of the Treasury, Federal Bureau of Investigation (May 2022). Guidance On The Democratic People's Republic Of Korea Information Technology Workers.

[14] Markets Insider (January 2022). NFTs ballooned to a $41 billion market in 2021 and are catching up to the total size of the global fine art market.

Open-source reporting suggests that the NFT marketplace has also created opportunities for art fraud, copyright infringement and brand damage. Artists who have had their work tokenized into NFTs without their consent[15] have become the latest victims[16]. Additionally, multiple companies have begun using lawsuits as a means to prevent the sale of NFTs representing their products. Similar to other exchange platforms, threat actors have used insider trading to illegally profit from NFT marketplaces.[17] The Department of Justice made its first charge for insider trading of digital assets in June 2022.[18]

Mitigating cyber threats to cryptocurrency accounts

Cryptocurrency users should consider risk mitigation strategies to reduce account or wallet compromise. Such strategies include the use of multi-factor authentication and reputable anti-virus software to detect potential credential theft malware in downloaded files or web browsing. Users could benefit from cold wallets or wallets that have been encrypted on the client-side, as well as multi-signature wallets that require multiple keys to create and conduct a transaction. Users are also encouraged to scrutinize transaction requests and destination addresses carefully.

Outlook for malicious activity targeting cryptocurrencies and NFTs

In 2022, the value of many cryptocurrencies and NFTs declined, potentially making them less attractive targets for direct theft. However, in addition to asset value, attackers also consider return on investment and transaction costs: the amount of time, effort and other resources needed to acquire and monetize an asset. Given the frequency of reporting about operations targeting cryptocurrency and NFTs, as well as the relatively low overhead required for these operations (social engineering, vulnerability exploitation, credential collection), it is likely still worthwhile for threat actors to target these assets despite declines in value.

The value of cryptocurrencies compared to fiat currencies is not likely to significantly impact threat actor use of cryptocurrencies in illicit transactions and extortion payments. This is due to the utility of digital assets for global transfers and increased opportunities to obfuscate transactions compared to the formal financial sector. Increased law enforcement and industry scrutiny is more relevant to this risk vs reward equation and may dissuade some actors.

[15] The Guardian (January 2022). Huge mess of theft and fraud: artists sound alarm as NFT crime proliferates.
[16] NBC News (January 2022). NFT art sales are booming. Just without some artists' permission.
[17] The National Law Review (March 2022). Rising Trend in NFT Litigation Over Popular Brands.
[18] U.S. Department of Justice (June 2022). Former Employee of NFT Marketplace Charged in First Ever Digital Insider Trading Scheme.

Insights Into the External Enterprise Attack Surface

Issue data referenced in this document is directly sourced from Mandiant Advantage Attack Surface Management, spanning 30,904 Collections. Collections define the scope of assets discovered and monitored by Attack Surface Management, yielding an enumerated inventory of external assets, applications and services and identified issues. The data set includes 6,022,027 issues identified from January 1, 2022, to June 30, 2022, 62,135 with issues of high or critical severity. Issues are a subset of Collections, which contain the asset inventory and associated technologies running on external attack surfaces. Issue severity is assigned based on the potential impact to the affected system. In situations where common vulnerabilities and exposures (CVE) are identified, the severity is tied to the Risk Rating from Mandiant Advantage Threat Intelligence.

An organization's digital footprint evolves organically through the adoption of cloud, new applications, devices and business relationships. Unfortunately, digital growth does not always occur under the purview of security or IT teams, commonly called shadow IT. This increases the risk of misconfigurations or applications and services receiving permissions that violate company security policies. From frontline observations and data gathered from the Mandiant Advantage platform, Mandiant has composed best practices for establishing and incorporating comprehensive attack surface management programs into cyber defense.

Quantifying the average external attack surface

The enterprise attack surface is comprised of devices, applications, services, libraries, people and partners, all of which can serve an exploitable entry point for a threat actor. Threat actors can use any vectors exposed to the internet to perform reconnaissance, move laterally, maintain access or achieve their overall mission.

Mandiant observed the following external attack surface trends over a six-month period associated with the "average" Collection:

- 2,746 exposed assets discovered, including DNS records, URLs, network services, AWS S3 buckets, GitHub repositories, mail servers and more
- 244 unique technology vendors and business relationships
- 13 unique applications with 150 instances of applications actively being used
- 9 unique supply chain service vendors with 102 instances of supply chain services being used
- Approximately 50% are multi-cloud, with usage across a combination of Microsoft Azure, Google Cloud Platform and AWS

Software supply chain and supply chain services

The largest Collections analyzed by Mandiant have more than 58 supply chain service vendors and over 1,200 unique instances of supply chain services detected at the external edge. Each vendor has a connection to the organization's infrastructure and is part of the larger supply chain ecosystem. As a best practice, Mandiant recommends performing an audit of all partners, along with SaaS and supply chain providers, being mindful of the criticality of the assets they interact with to assess the organization's potential risk. Mandiant M-Trends 2022[19] reported 17% of intrusions investigated by Mandiant came from supply chain compromise, highlighting the importance of integrating a strong supply chain management program into cyber defense operations.

Mapping assets to relevant applications and services provides insight into business relationships that a security team may not be aware of, including third- and fourth-party suppliers. CISA[20] recommends identifying upstream suppliers, or the suppliers' sources that can disrupt the broader ecosystem if breached. There are different types of supply chain vendors to account for, including commercial-off-the-shelf software (COTS), software-as-a-service (SaaS), and open-source software (OSS), as well as network infrastructure providers, physical infrastructure providers and parts suppliers.

Database exposures

Mandiant found 4.65% of Collections analyzed had databases exposed to the internet from January 1, 2022 to June 30, 2022. The Collections with database exposures saw 36 unique exposures on average, which implied underlying systemic issues that allowed these exposures.

Database exposures are high risk vectors, due to the potentially high volume of sensitive and confidential information that could be leaked. Organizations that identify database exposures should take immediate action to secure these assets, block common database ports, monitor cloud account access and perform a thorough investigation to assess the data sensitivity levels, identify any unauthorized access (if sufficient logging data is available) and the impact of the data exposure.

[19] Mandiant (2022). M-Trends 2022 Report.

[20] CISA. SCRM Essentials: Information and Communications Technology Supply Risk management (SCRM) in a Connected World.

An issue is a finding discovered on an external asset that warrants further investigation.

Critical severity, high priority

While it remains important to establish visibility into the enumerated asset inventory, technology vendors and related vulnerabilities, it's even more important to prioritize hardening and remediation efforts on the vectors that present the most risk. Mandiant recommends organizations prioritize critical and high severity issues, including CVEs with common vulnerability scoring system (CVSS) scores greater than 7.0 and focus on CVEs that have been or are likely to be exploited in the wild. Issues discovered by Attack Surface Management include vulnerabilities, misconfigurations, indicators of compromise (IOCs) or a data leak of any sort.

From January 1, 2022, to June 30, 2022, Mandiant identified over six million issues across small organizations and large enterprises. Of these, 62,135 (1.03%) were critical or high severity.

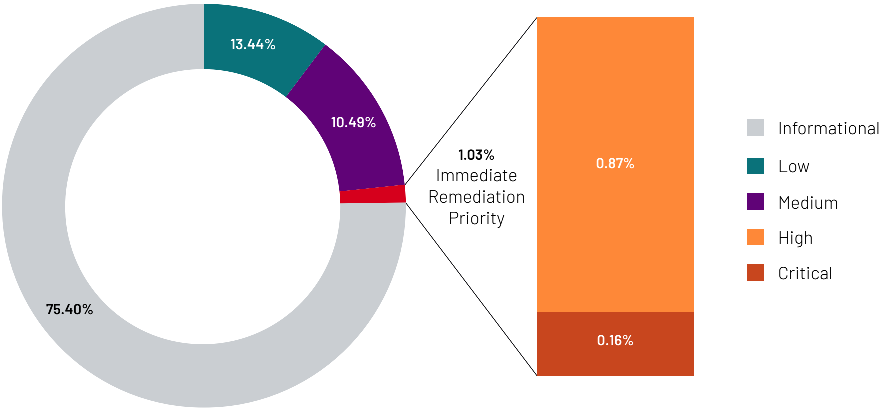


Figure 5. Issues observed by Mandiant Advantage Attack Surface Management from January 1, 2022 to June 30, 2022, assigned by severity.

Issues are identified and confirmed by testing known vulnerabilities and exposures. Organizations should remediate and patch the top five Critical Severity Issues (Table 1) immediately.

TABLE 1: Top 5 Critical Severity Issues identified by Mandiant Advantage Attack Surface Management from January 1, 2022 to June 30, 2022.

Rank	Critical issue	Exploited in the wild	Potential impact	Remediation recommendation
1	Wordpress Configuration Information Leak	No	PHP configuration files can contain sensitive information, such as database host and name, username, password and security keys. Any number of those data points can be leveraged in conjunction with other information gathered during the reconnaissance process to further the mission of a threat actor.	1. Audit the contents of the configuration file to determine if sensitive information was exposed. 2. Set permissions on the configuration file to prevent anonymous users from being able to read it.
2	Drupal Remote Code Execution (CVE-2019-6340)	Yes	Some field types do not properly sanitize data from non-form sources in Drupal 8.5.x before 8.5.11 and Drupal 8.6x before 8.6.10. When exploited, a threat actor can remotely execute arbitrary PHP code. The proof-of-concept is publicly available and there are reports of exploitation in the wild. CISA added the vulnerability to the Known Exploited Vulnerabilities Catalog and required a remediation date of April 15, 2022.	1. Disable all web service modules or configure the web server to not allow GET/PUT/PATCH/POST 2. Apply Drupal Security Update[21]
3	Microsoft Exchange Server Remote Code Execution (CVE-2021-31206)	No	An attack could exploit a traversal vulnerability that exists within the parsing of CAB files, allowing them to execute arbitrary code. However, exploitation requires adjacent network access and user interaction.	1. Follow the guidance provided by Microsoft-(50004778) Security Update Information[22] 2. Restrict egress communications from the Exchange Server 3.Restrict lateral movement portal for internal communication paths (SMB, WMI, RDP) 4. Restrict privilege account
4	SAP Memory Pipes Desynchronization (CVE-2022-22536)	No	An authenticated threat actor could prepend a user's request with arbitrary data, essentially impersonating the user or poisoning intermediary Web caches. A successful attack could result in complete compromise of Confidentiality, Integrity and Availability of the systems. A proof-of-concept is publicly available.	1. Apply SAP Security Update[23]
5	Apache HTTP Server-Side Request Forgery (CVE-2021-40438)	Yes	An attacker could send a specially crafted HTTP request to forward arbitrary network requests to an attacker-specified endpoint to exploit the service-side request forgery vulnerability in Apache HTTP Server 2.4.48 and earlier. CISA added the vulnerability to the Known Exploited Vulnerabilities Catalog and required a remediation date of December 15, 2022.	1. Perform an audit to find all devices and applications using Apache HTTP Server 2.4.48 and earlier versions. 2. Upgrade

[21] Drupal (February 20, 2019). Drupal core - Highly critical - Remote Code Execution - SA-CORE-2019-003.
[22] Microsoft (July 13, 2021). Description of the security update for Microsoft Exchange Server 2013: July 13, 2021 (KB5004778).
[23] SAP (February 11, 2022). Remediation of CVE-2022-22536 Request smuggling and request concatenation in SAP NetWeaver, SAP Content Server and SAP Web Dispatcher.

Mandiant previously reviewed the top five critical and high severity Issues[24] commonly found across Collections. Remediation guidance from Mandiant experts can be found in our blog Preventing and Remediating External Asset Exposures.[25]

Assess and prioritize at scale

Based on Mandiant observations, many organizations have thousands of internet-facing assets and hundreds of application and service vendors interacting with their attack surfaces. To mitigate the risk of assets or supply chain vendors being used as initial compromise vectors, security teams need to establish and streamline asset enumeration, supply chain management and vulnerability detection. Improving visibility into all aspects of the attack surface informs risk mitigation and enables faster remediation and response times. Consistent visibility into an organization's entire external attack surface and accurate, intelligence-led, risk-based prioritization help ensure that organizations focus remediation activities on the most critical attack vectors.

[24] Mandiant (2022). The Defender's Advantage Cyber Snapshot, Issue 1.
[25] Mandiant (July 2022). Preventing and Remediating External Asset Exposures.

Step By Step Through Enterprise Password Resets

Incident remediation is comprised of four phases: posturing, containment, eradication and longer-term security enhancements. During an active incident, the most crucial phase is eradication, which encompasses the actions taken to completely eliminate an attacker's access to regain control of an environment. Based on observations during Mandiant Incident Response engagements, eradication commonly includes the coordinated completion of an enterprise password reset.

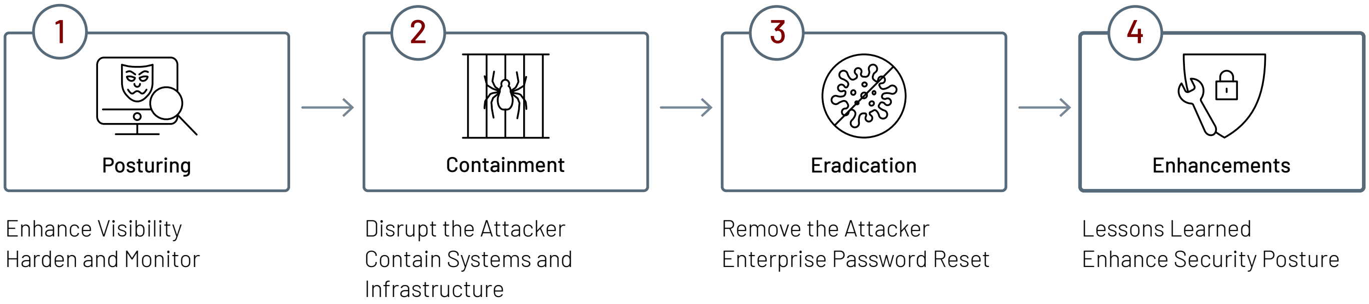


Figure 6. Phases of incident remediation.

Resetting passwords for all accounts in an environment is often a significant undertaking—particularly during an incident response engagement with an active attacker. A well-planned enterprise password reset can be performed with minimal impact. For best results, organizations need to understand what comprises an enterprise password reset event, as well as when, why and how should it be performed.

What an enterprise password reset comprises

An enterprise password reset involves the coordinated resetting of passwords for all accounts in an environment. The goal is to remove an attacker's ability to reuse stolen or compromised credentials. Depending on the scope of an incident, a successful enterprise password reset can include resetting passwords for:

- Domain-based privileged, user and service accounts
- Local accounts
- Application or technology-specific accounts
- API keys/secrets maintained within configuration files
- Cloud-based synchronization accounts
- Accounts that provide binding and integration with cloud-based/SaaS/ third-party components

Given its scale, this activity requires a coordinated effort of collaborative and synchronized teams across an organization. Aside from the security investigative team, stakeholders may include:

- System administrators and engineers
- Help and service desk personnel
- Endpoint and server administrators
- Cloud operations personnel
- Security operations personnel
- Application developers
- Corporate communications
- Internal counsel
- Executive leadership

When and why an enterprise password reset is required

From an attacker's perspective, compromising and maintaining persistence in an environment is vital to completing their objectives. They usually achieve this by compromising as many accounts as possible (including user, service, machine or application-specific accounts). During investigations, Mandiant often identifies evidence where an attacker has accessed or exfiltrated large sets of credentials or password hashes.

One common attack technique that always necessitates an enterprise password reset is the dumping of the NTDS.dit database from an Active Directory domain controller (DC). This file stores information about all domain-based accounts (user service or endpoints), groups and group membership – providing a potential avenue for complete domain-based credential compromise. Once an attacker has escalated privileges and is able to dump the NTDS.dit file, hashes can be extracted to perform pass-the-hash attacks or crack the passwords offline. In addition to NTDS dumping, many other Active Directory attacks, such as those involving DCSync, DCShadow, or Kerberoasting require this reponse.

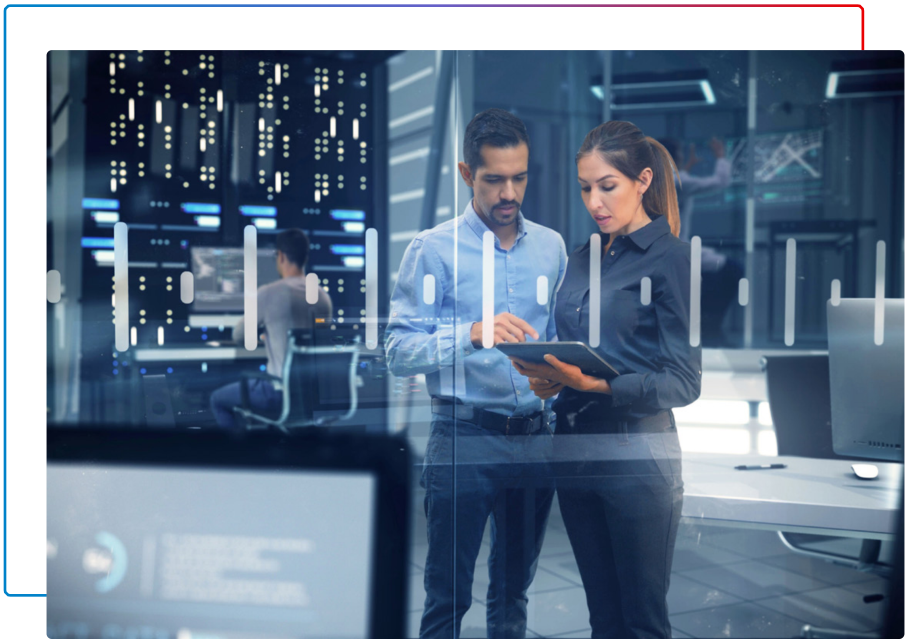
Mandiant has also observed attackers accessing plaintext files of passwords or secrets stored locally on workstations, file shares, code repositories, local password vaults, cloud storage or other locations.

While these scenarios provide a clear indication that an enterprise password reset should be initiated, there are many scenarios where attackers compromise privileged accounts in an environment. In such scenarios, even without direct evidence of mass credential access, an enterprise password reset is still recommended because an attacker’s scope of privileged access may have inferred access to a larger scope of accounts.

Resetting the passwords for only known-compromised accounts leaves open the possibility for an attacker to return using an account not previously identified as compromised during the investigation.

The decision to initiate an enterprise password reset should involve collaboration between the incident investigation and security teams. Once approved by the organization’s leadership, the reset planning should be aligned within the overall remediation plan and coordinated with the aforementioned teams.

An enterprise password reset is often the most complex remediation task. Planning for password resets can take time (especially for service and application accounts). Mandiant recommends organizations include plans for conducting mass password resets as part of incident response playbooks and tabletop exercises.



Processes for enterprise password reset

There are several actions that organizations can take to prepare for an enterprise password reset, many of which can be integrated into existing projects relating to asset management, authentication and identity and access management. Dedicated workstreams may need to be established to complete each task.

First, organizations should be sure they understand and have documented all existing authentication mechanisms used to store account and password information, such as Active Directory, SQL databases, cloud identity providers and third-party applications. This inventory will be required to properly scope a coordinated password reset process. This is also a good time to ensure that strong authentication (such as multifactor) and password policies for each identified account type are aligned to best practices and include specific password requirements for standard users, privileged users and service accounts.

When planning an enterprise password reset, it can be difficult to identify and inventory all accounts in the environment, especially privileged and service accounts. Having this information mapped can save valuable time during an active incident. The documentation should include explicit information on the scope of privileged accounts and data required to identify legacy, dormant and stale accounts.

According to NIST, a privileged account/user is one "that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform."[26] Some examples of privileged user accounts may include but are not limited to:

- Accounts within Active Directory domain-based privileged groups including Domain Admins, Enterprise Admins, Schema Admins and Account Operators
- Accounts with the ability to access or manage identities, passwords and security attributes
- Accounts with the ability to modify security configuration settings on endpoints
- Accounts with SSH keys on one or more systems
- Access keys and/or secrets associates with privileged users/accounts
- Accounts that have administrative access to databases, storage repositories or applications that house data deemed sensitive by the organization

Service accounts are typically the most challenging to fully correlate and assess the potential impact of a password change. To help assess impact, record the following information and attributes:

- Account name
- Account function/description
- System(s) where the account is used
- Operating system (such as Windows, Linux, Unix, Mac) where the service account is leveraged
- Log-on type performed by the account on identified systems (such as interactive, network, service, batch)
- Level of permissions or scope of access required (such as domain-level, local-level, application-specific permissions)
- Business owner of the account
- Technical owner or custodian of the account
- Manual or automated process for changing the password
  - If manual, note the specific technical process for changing the account password (including updating relevant documentation and configuration settings to reflect the new password)

While organizations can perform password reset actions using an automated process, a manual reset for specific accounts may be required. These specific accounts should be tracked and documented to ensure manual resets occur within the same timeframe as the enterprise password reset. Enforcing unique and randomized passwords for local administrative accounts on endpoints will also help ease the burden of an enterprise password reset.

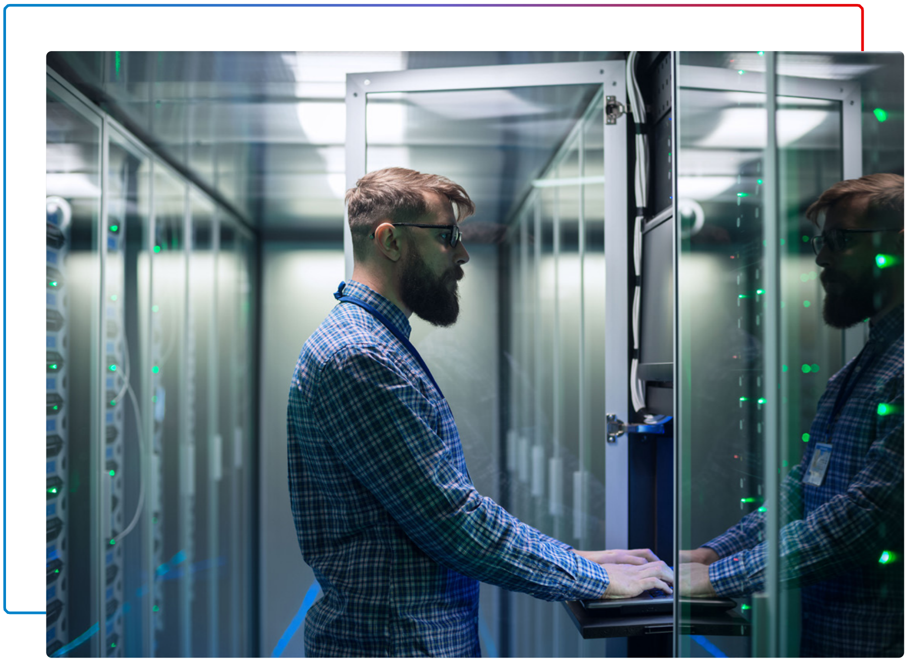
[26] NIST. Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

Communication and project management

A dedicated project leader should be designated to coordinate all stakeholders and drive the enterprise password reset to completion. Prior to the enforcement of a password reset, the impacted user base must be notified in a secure manner. When identifying who needs to be contacted before performing an enterprise password reset, organizations should coordinate with external and internal counsel and agree on the language to be included in the communications.

The planning process should also include guardrails for the password reset process, including:

- How new password/multifactor authentication (MFA) onboarding requirements will be communicated to all employees
- How and where users can change their passwords (on-premises, on VPN, only from trusted IP ranges, and other options)
- If MFA onboarding will be part of the password reset process, how secure onboarding of MFA devices/tokens will be conducted
- How long users will have to reset their passwords before their account is disabled
- The process for helpdesk/service desk staff to securely verify users that need assistance with resetting their password/unlocking their account(s)



Checklist items for enterprise password reset (partial)

Every organization should have a checklist of the accounts, secrets and keys that need to be reset. The following components are often in scope for an enterprise password reset:

- **KRBTGT.** This Active Directory account is responsible for encrypting and signing all Kerberos tickets for the domain. When resetting the password for this account, it should be conducted at least twice per domain (ten hours apart) and be performed first within the overall enterprise password reset process.
- **Privileged, User, Service and Local Accounts.** This password reset workstream should be performed across each account in the domain, using the inventory from preparation. Priority should be given to any compromised accounts identified during the investigation, followed by all privileged accounts. Any local accounts on systems accessed by the attacker should be reset.
- **Directory Services Restore Mode (DSRM) Account.** The DSRM account is a break glass local administrator account on every domain controller and requires a manual reset to ensure positive control of Active Directory. Mandiant recommends having a unique DSRM password per domain controller and storing these credentials in a secured privileged account management database or offline vault.
- **Domain Trust Keys.** Trust keys are stored on domain controllers and facilitate the trust relationship between domains in an Active Directory Forest. Resetting the trust key passwords is vital to prevent lateral movement to trusted domains. Depending on the trust type, organizations may need to reset the trust keys on both the trusting and trusted domains.
- **Active Directory Federated Services (AD FS) Service Account.** For a service account used for AD FS, a manual password reset may be required. Mandiant recommends using Group Managed Service Accounts (gMSAs) for the AD FS service account, to ensure automated password rotation occurs repeatedly and on a regular basis. Mandiant also recommends "rolling" the AD FS Token-Signing and Token-Decrypting certificate twice. Our whitepaper, **Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452,**[27] contains details of how to achieve this. If another platform is used to federate identities, then the service account associated with that Identity Provider (IdP) should be reset as well.
- **AZUREADSSOACC Account:** If seamless single sign-on (SSO) is utilized with Azure Active Directory Connect, the "AZUREADSSOACC" computer account is an on-premises account synchronized with Azure AD. To prevent vertical movement between on-premises and cloud services, the Kerberos decryption key for this account should be changed.
- **Azure AD Connect Sync Accounts:** If Azure AD Connect is used, the passwords for the various cloud connector and sync accounts should be changed.
  This includes the:
  - Azure AD Connector Account
  - Azure AD DS Account
  - ADSync Service Account

[27] Mandiant. Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452.

- **Rotate Secrets and Keys:** Organizations should prioritize the rotation of compromised secrets and access keys that may have been accessible to an attacker. Mandiant recommends proactively rotating keys and secrets across all platforms and services, even if they have not been identified as compromised during an investigation.

Successful eradication and remediation of an attacker depends on an organization’s ability to conduct a timely, well-coordinated enterprise password reset. Mandiant recommendations enable organizations to drastically minimize operational loss and ensure an attacker’s access has been eradicated post-incident.

Attackers Don't Follow Your Rules

> To know your enemy, you must become your enemy.
>
> —Sun Tzu

If you want to defeat an adversary, you must at least understand their capabilities. This is especially true for cyber adversaries, and a tenet at the heart of red team engagements.

Red teaming is the practice of safely conducting real-world attacks against an organization to identify vulnerabilities and misconfigurations in network architecture, gaps in security controls and deficiencies within security operations. While generic penetration testing can be useful, deeper mission-based exercises guided by threat intelligence are far more effective. They can reveal the most relevant actions needed to protect an organization's critical assets, improve technical controls and create resilience through operational enhancements and overhauls.

Case study: Nation-state CEO attack

A recent Mandiant client was concerned about news reports of attackers specifically targeting CEOs and the uptick in the use of zero-day attacks.[28] Mandiant was contacted to undertake a red team exercise, solely focusing on email access and applied only to the primary organization.

Following a review of the initial brief, Mandiant highlighted limitations in the original scope and suggested a more realistic threat scenario:

1. It was practical to assume that zero-day access, by its nature, would be successful against the targeted resource. Initial recon of the organization's attack surface showed that a Microsoft Exchange or VPN server would be a good initial starting point.
2. The CEO's email, while always an interesting target, was not the primary goal of this organization's adversaries. Mandiant determined that nation-state actors such as APT29, seeking access to research information and government connections were a more realistic attack scenario.
3. As a bilateral trust setup exists between the organization and its holdings, a compromise in any single subsidiary would mean a compromise for all. A supply-chain attack or subsidiary breach would be the easiest way in for an attacker.

[28] Mandiant (April 21, 2022). Zero Tolerance: More Zero-Days Exploited in 2021 Than Ever Before.

The exercise also focused on assessing whether post-exploitation attacker activities within the network could be detected. Phishing emails eventually get past email defenses; whether through luck, misconfiguration, exploit usage or a combination of all three. The defenses that trigger after a payload has been deployed should therefore be tested.

To enhance the exercise, the team used the phishing elements of APT29's attack campaign.[29] New techniques that APT29 might use to remain stealthy inside the organization were noted and new C2 channels via third-party storage solutions were added to the setup.

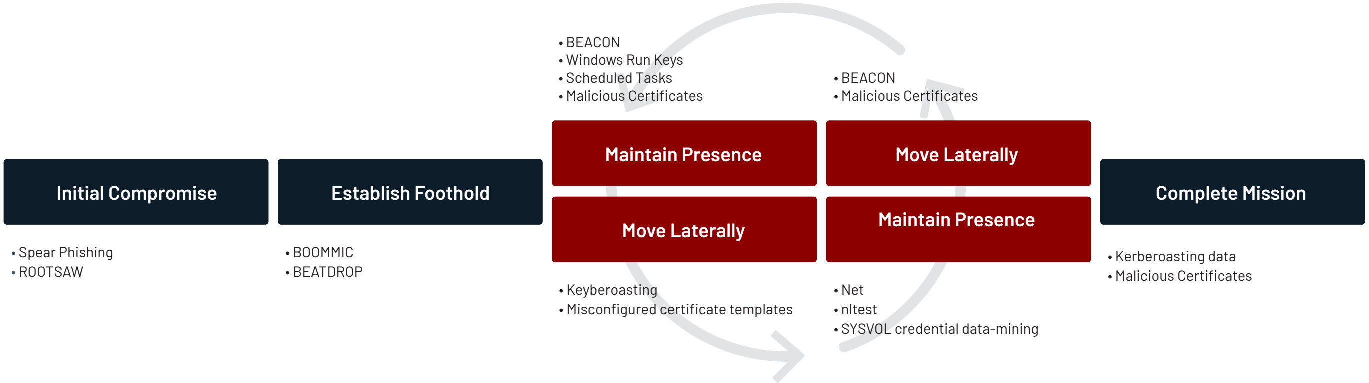


Figure 7. Attack lifecycle for the APT29 threat group.

Execution

As expected, the phishing controls and training performed well. In the first few weeks, they thwarted all efforts to get a foothold into the system. However, by subtly altering the content of the phishing message and switching from wide-spread targeting to spear-phishing, a single visit to the red team hosted website resulted in the download of the ISO file. The file did not contain the mark-of-the-web indicator, so no security warnings were displayed to the victim user and the hidden files executed as a DLL search-order hijack attack, giving the red team access to a single user system.

Endpoint detection and response (EDR) was bypassed by exploiting permissive "safe folders" on the system. Quick lateral movement of the system was achieved via the victim user's access to files containing clear-text passwords in a source code sharing solution. This gave admin rights on several database servers, one of which did not have active security solutions running.

[29] Mandiant (April 28, 2022). Trello From the Other Side: Tracking APT29 Phishing Campaigns.

In parallel, the supply-chain simulation performed on an information exchange system managed to escalate their privileges to administrator and dump credentials from memory through a version of Mimikatz, changed to reflect custom threat actor techniques. The credentials revealed the past presence of a user from the central domain and lateral movement into the network was secured by using these credentials against the originating system.

The two paths converged to exploit weaknesses in the Active Directory configuration, escalate privileges and acquire domain administrator level access and full control over the internal network. In the original scenario this would have been the end of our mission, but the current objective was defined as "access to critical IP."

Using the high-level access acquired, Mandiant identified systems within a segregated subnet and cloud resources, which contained information required to access the organization's critical IP. By using the internal package deployment system within the domain, a permit-listed version of the Mandiant implant was moved to the identified research lead's system and then run.

Various methods to access the research systems were explored; having access to the user password via keylogging was not enough. A custom piece of code was written to trigger a very realistic but fake two-factor authentication prompt on the victim machine to steal the temporary token and log in with full access. The theft of a critical piece of data could now be simulated and the mission was complete.

Expanding the original red team mission from basic email compromise to mimicking APT29 tactics, techniques and procedures (TTPs) provided the organization with deeper insights. They were now able to identify and address controls that provided only surface level coverage, could be bypassed or were perhaps never encountered at all.

Closing Thoughts

Knowledge is one of our greatest advantages in the fight against cyber adversaries. *The Defender's Advantage Cyber Snapshot* is designed to provide just that—intelligence that informs security teams and enables leaders to make smart decisions.

This edition of *The Defender's Advantage Cyber Snapshot* showed how effective disinformation operations can be, and how they are growing in scale, frequency and scope. It also looked at threats to cryptocurrencies and NFTs, and how these newer technologies are factoring into cyber attacks.

Leaning towards defense, best practices were presented to help organizations stay ahead of misconfigurations related to digital growth. Specific guidance was included on performing an enterprise-wide password reset, and describing how red teaming greatly helps security teams prepare for real world attacks.

Attackers are constantly innovating and attack surfaces are constantly expanding; it can seem impossible for defenders to keep up. The cyber security industry must share information and work together to help keep responders in the fight, and *The Defender's Advantage Cyber Snapshot* is just one way Mandiant supports the cause.

Learn more at www.mandiant.com

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.