Microsoft Security

CYBERATTACK REPORT No. 4

Octo Tempest Ransomware & Extortion

Octo Tempest tangles with CISOs

Octo Tempest is a financially motivated cyberthreat actor group which initially surfaced in March 2022. In August 2022 they increased the velocity of cyberattacks—both the time between victims and the time between initial access and impact at organizations. Octo Tempest often compromises regular users via phishing before performing reconnaissance to identify highly-privileged users at organizations. They may compromise these highly-privileged users by SIM swapping their phones or by socially engineering helpdesk staff to change passwords and manipulate multifactor authentication (MFA) settings. Once a privileged foothold has been established, they leverage federated identity back door to maintain persistence within organizations. Their tactics are constantly evolving, and they are known to impersonate and masquerade as staff, including CISOs, or other incident response firms. Octo Tempest moves swiftly to exfiltrate data in novel ways before ultimately deploying ransomware to financially extort victims. This cyberattack report will show the speed at which Octo Tempest moves and how Microsoft IR protects against this cyberthreat with swift and decisive takeback actions.

Timeline of Activities – Octo Tempest attack flow

Octo Tempest is a highly active cyberthreat actor group which utilizes varying social engineering campaigns with the goal of financial extortion across many business sectors through means of data exfiltration and ransomware.

Threat actor social engineering of helpdesk and other administrative staff, including impersonating legitimate users to coerce password resets or authentication method manipulation on targeted identities.

Threat actor conducts reconnaissance through querying group and role membership and enumeration of internal document libraries.

Threat actor begins identifying valuable Tier-0 assets and collecting additional credentials by utilizing third party credential harvesting tools against cloud and on-premises assets.

Threat actor installs trusted back door allowing for federated authentication from malicious identity provider (or IdP) infrastructure.
This allows for the forging of valid SAML tokens for any identity in the environment allowing for further access using valid identities.
Tunnelling and remote access tools to cloud and on premises assets are also used to maintain persistence.

Threat actor takes control of EDR and endpoint management tools utilizing built-in functionality for tool deployment via remote shell connectivity to devices across the environment . Device management solutions are also used to alter security settings and weaponized for malicious payload delivery.

Threat actor stages and attempts to exfiltrate stolen data via various hosting providers and file sharing services. Staging and attempts to deploy BlackCat ransomware to Windows and Linux systems are detected.

The BlackCat ransomware was detected, blocked, and remediated by devices with Microsoft Defender Antivirus enabled and / or Microsoft Defender for Endpoint onboarded.

EDR and Antivirus solutions prevent ransomware by detecting and blocking malicious activity, identifying suspicious behavior, and can contain or automatically remediate cyberthreats.

The ransomware was successfully deployed and executed, encrypting the systems that were not sufficiently protected by an EDR or an antivirus solution.

Microsoft Incident Response Post-Event

Investigation began by deploying forensic tools across the environment.

Log Analysis revealing threat actor activity against cloud and on-premises assets, including devices and identities.

Active Directory and Entra ID hardening to contain compromised identities including those that are highly privileged and to reduce additional attack vectors.

Take-back, hardening, and wide deployment of Microsoft Defender for Endpoints to systems in the environment to increase visibility and overall protection.

Removal of federated back door severing the ability to issue forged SAML tokens. Revocation of session and access tokens eliminating threat actor persistence. Remediation of threat actor created cloud resources and modified settings.

Use of EDR system to block known threat actor tooling and IP addresses as well as isolate compromised machines in the environment.

Partnered with customers internal security teams to perform collaborative knowledge transfer and threat hunting evolutions, surfacing additional opportunities for remediation actions.

Provided customers with an action plan showcasing a path towards modernization forged from Microsoft IR's investigation, enabling organizations to strengthen their security posture through a Microsoft IR partnership alongside the comprehensive/robust Microsoft Security suite/stack.

What happened?

The Microsoft Incident Response team was engaged with a customer who had been under a targeted phishing and smishing (SMS-based phishing) attack from Octo Tempest. They suspected they had been successfully compromised.

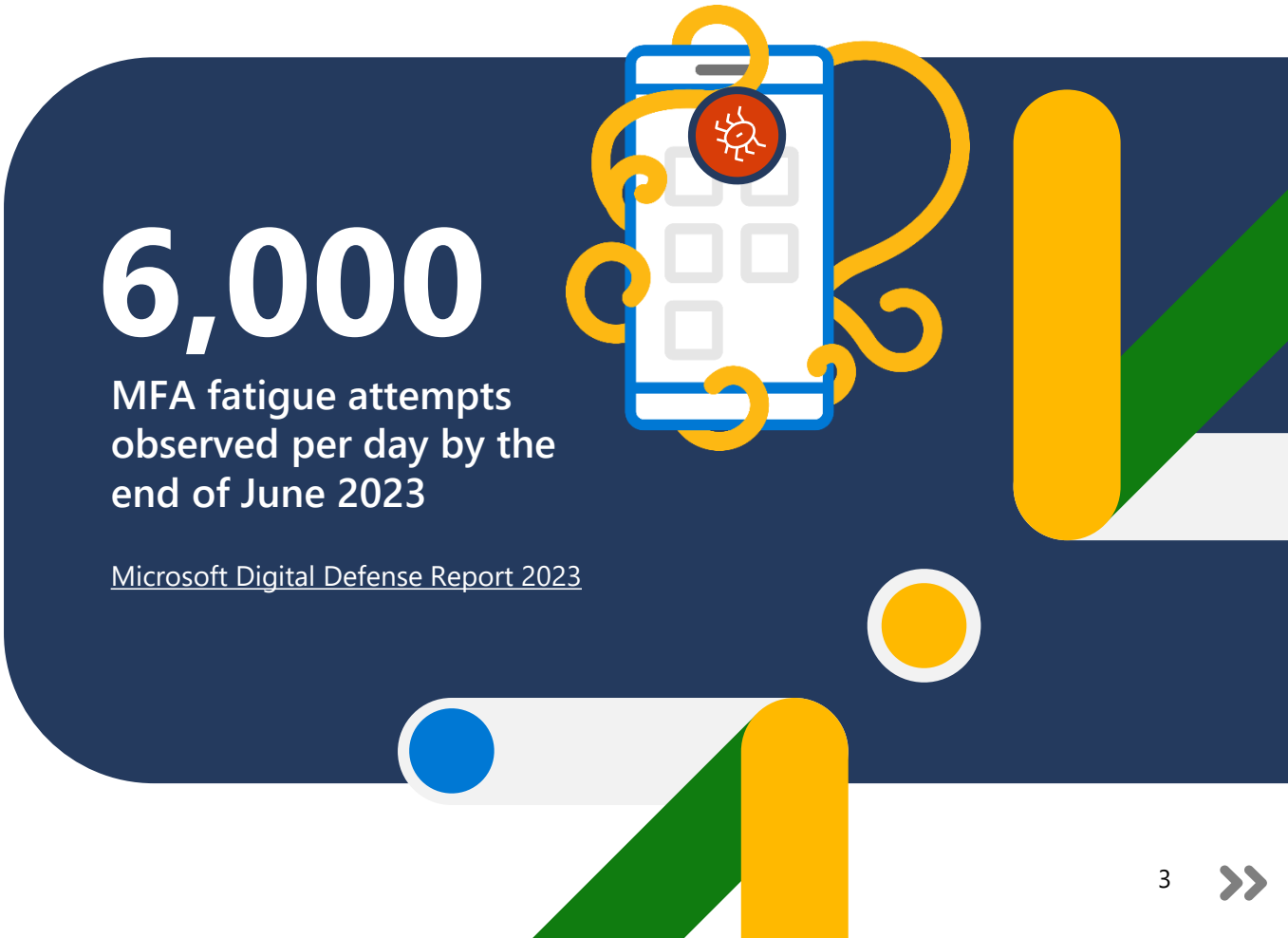
Upon initial investigation, we discovered Octo Tempest had successfully socially engineered the customer's help desk to remove a highly-privileged user's MFA device and reset their password using self-service password reset (SSPR) to gain initial access.

In this instance, Octo Tempest had personal information about the targeted victim, likely gained through a prior intrusion. They used this information to establish trust and credibility with the help desk agent.

Once they successfully logged into the victim's identity, they quickly registered their own authentication method to satisfy the customer's conditional access policies enforcing MFA. To maintain persistence in the environment, they utilized an open-source 3rd party tool to modify federated authentication flow, which allowed Octo Tempest to authenticate as any user in the organization, without requiring their credentials.

During the intrusion, they performed discovery on the customer's SharePoint and email for sensitive information about IT processes and VPN architecture.

Having located the documentation to access the organization's VPN solution, Octo Tempest was able to connect to the VPN leveraging the password and MFA device they had compromised earlier, facilitating an on-premises foothold. Once connected to the VPN, they located credentials for and accessed the customer's EDR solution. From the EDR portal, they modified the settings to allow a known ransomware hash to execute. Unfortunately, the lack of operational visibility over the EDR platform resulted in alerts that were not remediated by the customer. Octo Tempest then utilized the customer's own device management system to deploy this ransomware to all systems in the environment.



How did Microsoft respond?

As the prolific list of Octo Tempest's victims increases, so does their speed and efficiency. Their tactics, techniques, and procedures (TTPs) are quickly evolving, and time is not in the victim's favor. Such engagements need to be responded to with efficient containment, eviction, and detection capabilities. The Microsoft Incident Response (IR) team works in tandem with our Threat Intelligence Community (MSTIC) to identify and notify victims at the earliest opportunity by issuing Nation-State Notifications (NSN's). These notifications are designed to help security teams start preliminary investigations and recovery processes.

It is critical to act swiftly and strategically to protect the victim organization's assets and data. First and foremost, the incident response team will engage with the victim organization to gather critical information about the attack—such as the initial entry point, the extent of compromise, and any known TTPs. To evict the cyberthreat actor effectively, the IR team will collaborate closely with the victim organization's IT and security teams to isolate and contain the compromised systems to prevent or reduce the spread of the ransomware. Simultaneously, the IR team will focus on identifying and shutting down the cloud resources deployed by the cyberattacker. This may involve revoking access permissions, disabling malicious resource instances, and conducting forensic analysis to understand how the cyberattacker gained access to the environment.

Microsoft IR will also prioritize the removal of persistence mechanisms—including modifications to normal organizational authentication flows—such as federation changes that allow unauthorized access, which are frequently used by the cyberthreat actor. Analysis of the organization's security stack, particularly those products with remote execution capabilities, are frequently used by Octo Tempest for lateral movement and additional persistence. Analysis of these tools and products—particularly changes to security policy—is paramount in the early stages of containment. Additionally, Microsoft IR will work with the victim organization to enhance security measures, such as implementing MFA, strengthening access controls, and educating employees about phishing, smishing, and social engineering threats utilized by this group.

Throughout the entire process, effective communication and coordination between the incident response team and the victim organization is crucial. The team provides regular updates on their progress, shares threat intelligence, and offers guidance on remediation and prevention strategies. By working together seamlessly, the incident response team and the victim organization can mitigate the immediate cyberthreat, eradicate the cyberattacker's presence, and strengthen the organization's defenses against future cyberattacks.

How can organizations prevent more social engineering attacks?

- Educate and develop mitigation strategies to reduce social engineering attacks
- Implement Zero Trust and tiering models, establish SAW/PAW standard practices for privileged identities
- Monitor changes to security tools, Azure resources, and new installation of RMM tools

How should other customers prepare?

This incident highlights the importance of privileged identity best practices, effective monitoring, and the need for expert guidance when dealing with Octo Tempest cyberattacks. Here are some key takeaways for customers to help them prepare for similar incidents:

1. Implement Zero Trust

Implementation of best practices to further secure identity plane and highly scrutinize administrative account activities, such as Global, Enterprise, Domain, and Database administrators. Establish Secure/Privileged Access Workstation (SAW/PAW) standard practices for such account activities, establish Role Based Access Controls (RBAC) and Conditional Access Policies (CAP) for Trusted devices, and monitor for abnormalities.

- **Verify explicitly** - Leverage user identity and device compliance data points to for authentication and authorization.
- **Use least-privilege access** - Secure data by implementing Just-in-time and just-enough access (JIT/JEA).
- **Assume breach** - Continuously validate the trustworthiness of all requests and sessions across your environment.

Key Takeaways

5 proactive measures customers can take to better prevent and prepare for security incidents:

1. Implement Zero Trust
2. Monitor changes and use of security and RMM tools
3. Establish social engineering mitigation strategies
4. Secure and monitor cloud resources
5. Obtain expert guidance

2. Closely monitor changes and use of security and RMM tooling

Deployment of unsanctioned remote access tools and/or modifications to existing EDR/AV products are often used to laterally move further into environments, establish persistence, hinder security capability, and deploy ransomware. Modifications and new installations provide great detection opportunities. Ensure anti-tampering protection is enabled for Defender.

3. Educate and develop mitigation strategies to reduce social engineering attacks

Octo Tempest employs social engineering tactics, such as direct communication with users and help desk personnel. This frequently provides initial access, often with privileged accounts/identities. Implement phishing resistant MFA, where possible. Establish multiple verification steps for help desk personnel; direct management or video verification of users requesting password reset/MFA device changes.

4. Secure and monitor Azure and other cloud resources

Octo Tempest frequently leverages Azure services as part of their attack. Azure activities such as the creation and use of Azure virtual machines, Azure Bastion hosts, firewall modifications, snapshot creations of virtual machine disks, especially Domain Controllers running in Azure, and the export of virtual machine disks should be monitored for anomalies. Additionally, segmentation of critical workloads, such as those in the identity plane, is crucial to enhance the overall security posture.

5. Expert Guidance

Cybersecurity attacks can be complex and challenging to deal with, and customers need expert guidance to ensure that they respond effectively. Customers should engage with incident response experts to develop a comprehensive incident response plan and ensure security personnel are trained to respond to ransomware incidents.

- **Compromise Assessment** - Receive a point-in-time, deep analysis of your environment, including proactive investigation for persistent cyberthreats and security risks.
- **Incident Response** - Get global investigation and guidance all day, every day, to help evaluate incident scope, contain cyberattacks, and restore critical systems, with options for onsite and remote.

Conclusion

Octo Tempest is a cyberthreat actor that pushes the boundary of aggressive phishing and social engineering techniques to gain control of user accounts/identities. Once a foothold has been established, they move quickly to exfiltrate data and deploy ransomware. Many companies can detect user compromise but lack sufficient controls to prevent adversaries like Octo Tempest from being able to move laterally and escalate privilege.

Customers often do not have a tested incident response plan and do not invoke it in a timely manner when breaches are detected. In the early onset of an attack, making swift and decisive decisions is key to disrupting the attack and limiting damage.

Microsoft Incident Response follow a demonstrated and proven take-back methodology to regain positive control of customer environments and seek to limit and mitigate damage.

Learn more about how Microsoft Incident Response can help you before, during, and after a security incident.
Click here