Protecting customers from Octo Tempest attacks across multiple industries | Microsoft Security Blog

By Microsoft Defender Security Research Team

Published: 2025-07-16 · Archived: 2026-04-05 13:38:15 UTC

In recent weeks, Microsoft has observed Octo Tempest, also known as Scattered Spider, impacting the airlines sector, following previous activity impacting retail, food services, hospitality organizations, and insurance between April and July 2025. This aligns with Octo Tempest's typical patterns of concentrating on one industry for several weeks or months before moving on to new targets. Microsoft Security products continue to update protection coverage as these shifts occur.

To help protect and inform customers, this blog highlights the protection coverage across the Microsoft Defender and Microsoft Sentinel security ecosystem and provides security posture hardening recommendations to protect against threat actors like Octo Tempest.

Overview of Octo Tempest

Octo Tempest, also known in the industry as Scattered Spider, Muddled Libra, UNC3944, or 0ktapus, is a financially motivated cybercriminal group that has been observed impacting organizations using varying methods in their end-to-end attacks. Their approach includes:

- Gaining initial access using social engineering attacks and impersonating a user and contacting service desk support through phone calls, emails, and messages.
- Short Message Service (SMS)-based phishing using adversary-in-the-middle (AiTM) domains that mimic legitimate organizations.
- Using tools such as ngrok, Chisel, and AADInternals.
- Impacting hybrid identity infrastructures and exfiltrating data to support extortion or ransomware operations.

Recent activity shows Octo Tempest has deployed DragonForce ransomware with a particular focus on VMWare ESX hypervisor environments. In contrast to previous patterns where Octo Tempest used cloud identity privileges for on-premises access, recent activities have involved impacting both on-premises accounts and infrastructure at the initial stage of an intrusion before transitioning to cloud access.

Octo Tempest detection coverage

Microsoft Defender has a wide range of detections to detect Octo Tempest related activities and more. These detections span across all areas of the security portfolio including endpoints, identities, software as a service (SaaS) apps, email and collaboration tools, cloud workloads, and more to provide comprehensive protection coverage. Shown below is a list of known Octo Tempest tactics, techniques, and procedures (TTPs) observed in recent attack chains mapped to detection coverage.

Tactic	**Technique**	**Microsoft Protection Coverage (non-exhaustive)**
Initial Access	Initiating password reset on target's credentials	Unusual user password reset in your virtual machine; (MDC)
Discovery	Continuing environmental reconnaissance	Suspicious credential dump from NTDS.dit; (MDE) Account enumeration reconnaissance; (MDI) Network-mapping reconnaissance (DNS); (MDI) User and IP address reconnaissance (SMB); (MDI) User and Group membership reconnaissance (SAMR); (MDI) Active Directory attributes reconnaissance (LDAP); (MDI)
Credential Access, Lateral Movement	Identifying Tier-0 assets	Mimikatz credential theft tool; (MDE) ADExplorer collecting Active Directory information; (MDE) Security principal reconnaissance (LDAP); (MDI) Suspicious Azure role assignment detected; (MDC) Suspicious elevate access operation; (MDC) Suspicious domain added to Microsoft Entra ID; (MDA) Suspicious domain trust modification following risky sign-in; (MDA)

	Collecting additional credentials	Suspected DCSync attack (replication of directory services); (MDI) Suspected AD FS DKM key read; (MDI)
	Accessing enterprise environments with VPN and deploying VMs with tools to maintain access in compromised environments	'Ngrok' hacktool was prevented; (MDE) 'Chisel' hacktool was prevented; (MDE) Possibly malicious use of proxy or tunneling tool; (MDE) Possible Octo Tempest-related device registered (MDA)
Defense Evasion, Persistence	Leveraging EDR and management tooling	Tampering activity typical to ransomware attacks; (MDE)
Persistence, Execution	Installing a trusted backdoor	ADFS persistent backdoor; (MDE)
Actions on Objectives	Staging and exfiltrating stolen data	Possible exfiltration of archived data; (MDE) Data exfiltration over SMB; (MDI)
	Deploying ransomware	'DragonForce' ransomware was prevented; (MDE) Possible hands-on-keyboard pre-ransom activity; (MDE)

Note: The list is not exhaustive. A full list of available detections can be found in the Microsoft Defender portal.

Disrupting Octo Tempest attacks

Disrupt in-progress attacks with automatic attack disruption:
Attack disruption is Microsoft Defender's **unique, built-in self-defense capability** that consumes multi-domain signals, the latest threat intelligence, and AI-powered machine learning models to automatically predict and disrupt an attacker's next move by containing the compromised asset (user, device). This technology uses multiple potential indicators and behaviors, including all the detections listed above, possible Microsoft Entra ID sign-in attempts, **possible Octo Tempest-related sign-in activities** and correlate them across the Microsoft Defender workloads into a high-fidelity incident.

Based on previous learnings from popular Octo Tempest techniques, attack disruption will automatically **disable the user** account used by Octo Tempest and revokes all existing active sessions by the compromised user.

While attack disruption can contain the attack by cutting off the attacker, it is critical for security operations center (SOC) teams to conduct incident response activities and post-incident analysis to help ensure the threat is fully contained and remediated.

Investigate and hunt for Octo Tempest related activity:
Octo Tempest is infamously known for aggressive social engineering tactics, often impacting individuals with specific permissions to gain legitimate access and move laterally through networks. To help organizations identify these activities, customers can use Microsoft Defender's advanced hunting capability to proactively investigate and respond to threats across their environment. Analysts can query across both first- and third-party data sources powered by Microsoft Defender XDR and Microsoft Sentinel. In addition to these tables, analysts can also use exposure insights from Microsoft Security Exposure Management.

Using advanced hunting and the Exposure Graph, defenders can proactively assess and hunt for the threat actor's related activity and identify which users are most likely to be targeted and what will be the effect of a compromise, strengthening defenses before an attack occurs.

Proactive defense against Octo Tempest

Microsoft Security Exposure Management, available in the Microsoft Defender portal, equips security teams with capabilities such as critical asset protection, threat actor initiatives, and attack path analysis that enable security teams to proactively reduce exposure and mitigate the impact of Octo Tempest's hybrid attack tactics.

Ensure critical assets stay protected

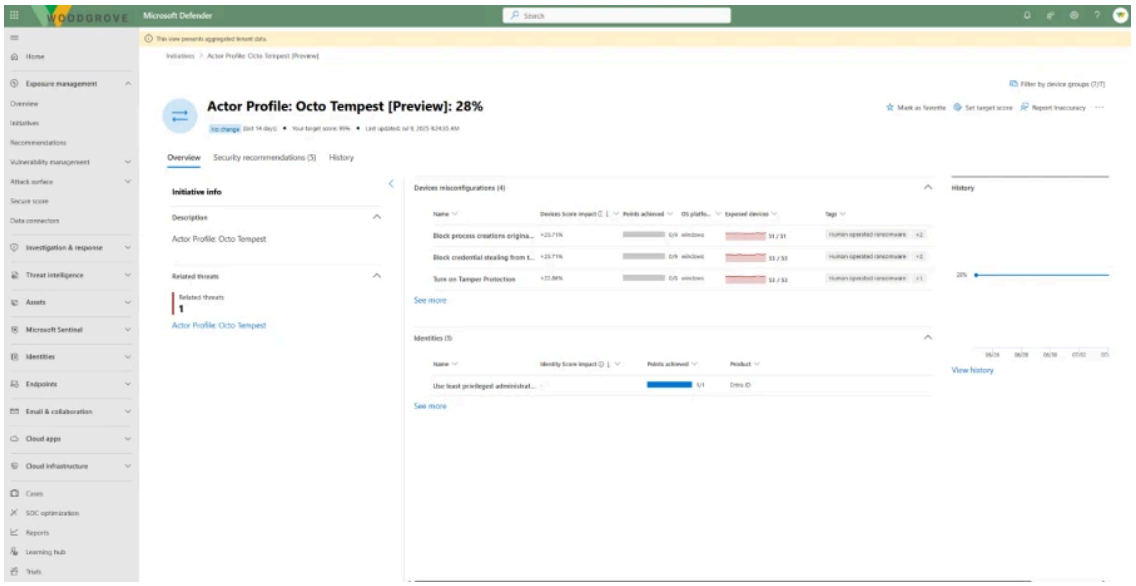
Customers should ensure critical assets are classified as critical in the Microsoft Defender portal to generate relevant attack paths and recommendations in initiatives. Microsoft Defender automatically identifies critical devices in your environment, but teams should also create custom rules and expand critical asset identifiers to enhance protection.

Take action to minimize impact with initiatives

Exposure Management's initiatives feature provides goal-driven programs that unify key insights to help teams harden defenses and act fast on real threats. To address the most pressing risks related to Octo Tempest, we recommend organizations begin with the initiatives below:

- **Octo Tempest Threat Initiative**: Octo Tempest is known for tactics like extracting credentials from Local Security Authority Subsystem Service (LSASS) using tools like Mimikatz and signing in from attacker-controlled IPs—both of which can be mitigated through controls like attack surface reduction (ASR) rules and sign-in policies. This initiative brings these mitigations together into a focused program, mapping real-world attacker behaviors to actionable controls that help reduce exposure and disrupt attack paths before they escalate.

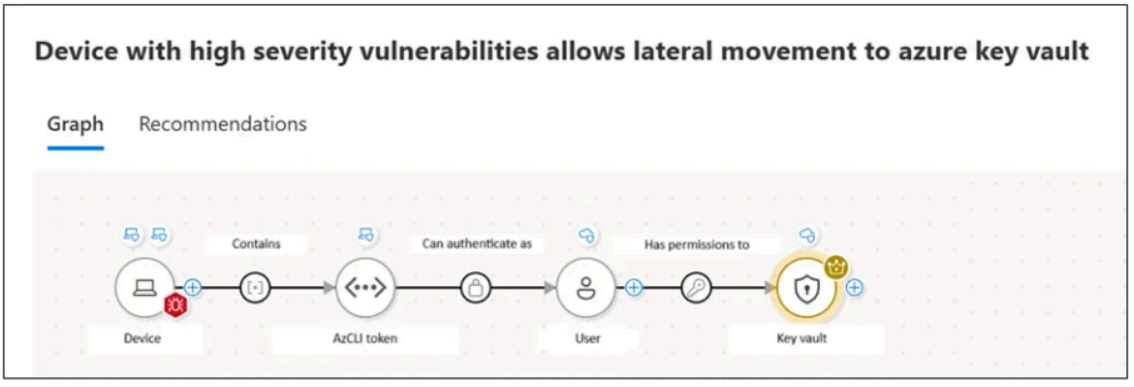
- **Ransomware Initiative**: A broader initiative focused on reducing exposure to extortion-driven attacks through hardening identity, endpoint, and infrastructure layers. This will provide recommendations tailored for your organization.



Investigate on-premises and hybrid attack paths

Security teams can use attack path analysis to trace cross-domain threats—like those used by Octo Tempest—who've exploited the critical Entra Connect server to pivot into cloud workloads, escalate privileges, and expand their reach. Teams can use the 'Chokepoint' view in the attack path dashboard to highlight entities appearing in multiple paths, making it easy to filter for helpdesk-linked accounts, a known Octo target, and prioritize their remediation.

Given Octo Tempest's hybrid attack strategy, a representative attack path may look like this:



Recommendations

In today's threat landscape, proactive security is essential. By following security best practices, you reduce the attack surface and limit the potential impact of adversaries like Octo Tempest. Microsoft recommends implementing the following to help strengthen your overall posture and stay ahead of threats:

Identity security recommendations

- Ensure multifactor authentication is enabled for all users: Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.
- Enable Microsoft Entra ID Identity Protection sign-in risk policies: Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for.
- Ensure phishing-resistant multifactor authentication strength is required for Administrators.
- Ensure Microsoft Azure overprovisioned identities should have only the necessary permissions.
- Enable Microsoft Entra Privileged Identity Management as well as other protective measures to mitigate the risk of unnecessary or unauthorized access.

Endpoint security recommendations

- Enable Microsoft Defender Antivirus cloud-delivered protection for Linux.
- Turn on Microsoft Defender Antivirus real-time protection for Linux.
- Enable Microsoft Defender for Endpoint EDR in block mode to block post breach malicious behavior on the device through behavior blocking and containment capabilities.
- Turn on tamper protection that essentially prevents Microsoft Defender for Endpoint (your security settings) from being modified.
- Block credential stealing from the Windows local security authority subsystem: Attack surface reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyber-attacks and malicious software.
- Turn on Microsoft Defender Credential Guard to isolate secrets so that only privileged system software can access them.

Cloud security recommendations

- Key Vaults should have purge protection enabled to prevent immediate, irreversible deletion of vaults and secrets.
- To reduce risks of overly permissive inbound rules on virtual machines' management ports, enable just-in-time (JIT) network access control.
- Microsoft Defender for Cloud recommends encrypting data with customer-managed keys (CMK) to support strict compliance or regulatory requirements. To reduce risk and increase control, enable CMK to manage your own encryption keys through Microsoft Azure Key Vault.
- Enable logs in Azure Key Vault and retain them for up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised.
- Microsoft Azure Backup should be enabled for virtual machines to protect the data on your Microsoft Azure virtual machines, and to create recovery points that are stored in geo-redundant recovery vaults.

Explore security solutions

To learn more about Microsoft Security solutions, visit our website. Bookmark the Microsoft Security blog to keep up with our expert coverage on security matters.

Also, follow us on Microsoft Security LinkedIn and @MSFTSecurity on X for the latest news and updates on cybersecurity.
