AccountabilIT
Security Amplified, Cloud Simplified

Threat Briefing

SEPTEMBER 00, 2025

Threat Briefing

ACTIVITY OVERVIEW

Trends

- Abuse of tunneling services
- Threats leveraging AI

Nation-state Threat Actors

- Daffodil Gust
- Storm-0727

Tools & Techniques

- Medusa Ransomware
- PipeMagic
- Bad Successor

Vulnerabilities

- CVE-2025-53786
- CVE-2025-7775

OSINT

- Malicious use of memory forensic tools
- Threats targeting Microsoft Teams

Trends

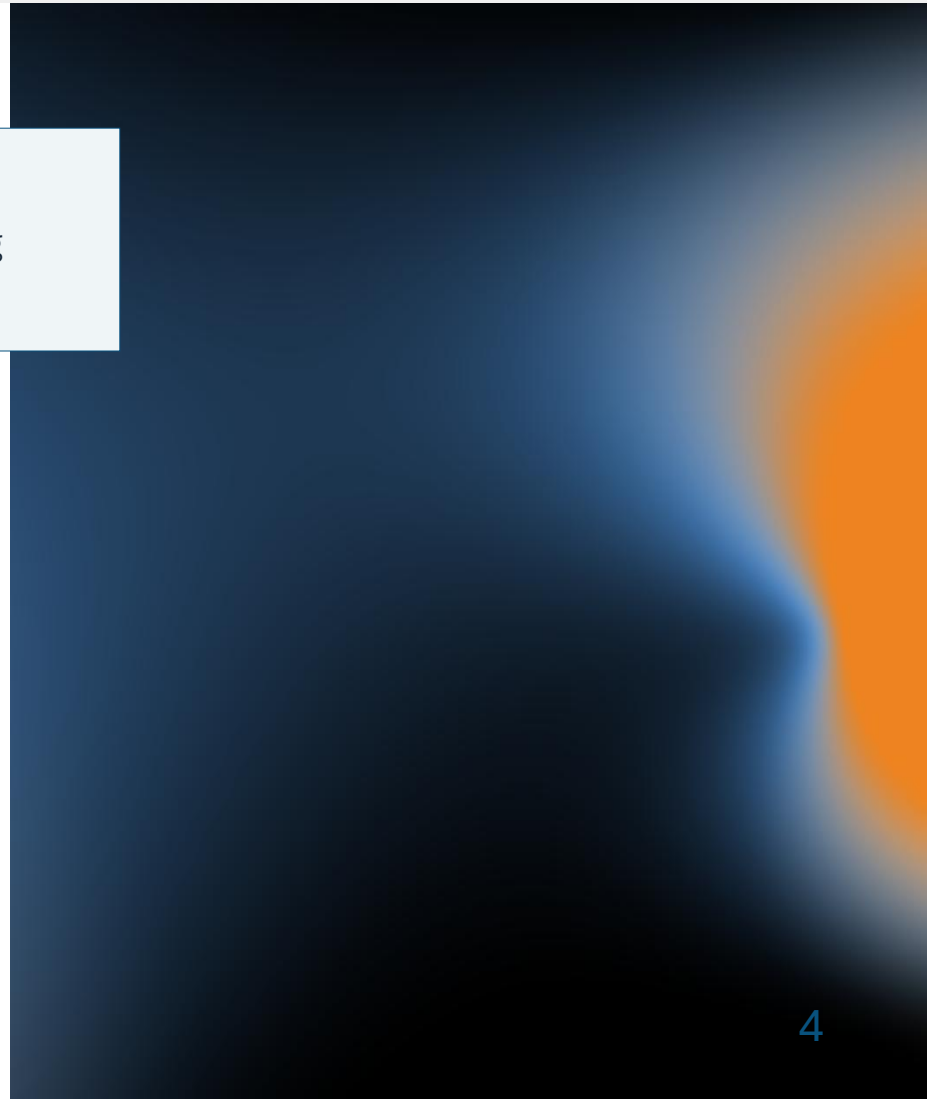
Abuse of Legitimate Tunneling Services

What is a tunneling service?

These are legitimate services often used by developers for exposing or collaborating on applications across the internet.

How are these being abused?

- Legitimate tunneling service as a core C2 obfuscation layer
  - Threat actors integrate legitimate tunneling services as part of their C2 infrastructure.
- Tunnels appear earlier in the attack chain
  - These are no longer being used post-compromise. Even initial access and payload staging may use tunnel infrastructure to obfuscate activities.
- Tunneling is embedded in LOLBin-driven infection chains
  - LOLBin based TTPs are incorporating connections to tunneling platforms.



Threats Leveraging Artificial Intelligence

AI as a force-multiplier

- AI tools are being integrated into existing workflows to accelerate malware development, automate reconnaissance, and streamline day to day tasks (e.g. ransom negotiation, phishing email generation).

LLM-enabled adaptive malware

- LLMs embedded in the execution chain, using an LLM to dynamically generate malicious instructions at runtime. i.e. HumOR without the Hum.

AI supply chain attacks

- Much like other dev tool supply chain attacks, AI tools, libraries, extensions, etc. are at risk to attack and compromise and inadvertent use by developers.


Nation-state Threat Actors

Daffodil Gust

Targets

- Journalists, political activists, and government entities in the Middle East and Europe in support of Emirati intelligence collection priorities.

Objectives

- Support the Emirati regime's goals of ensuring internal security and stability. Additionally, targeting government institutions in the Gulf region and Europe along with Middle Eastern telecom, transportation, and IT targets.

Recent Activity Includes

- Exploitation of CVE-2025-33053 to remotely run malware on a compromised system. This is an exploitation of WebDAV to deploy malicious code to a compromised system.

Daffodil Gust

ACTIVITY OVERVIEW

- This actor frequently relies on spear-phishing emails to gain access. It is common to observe malicious links or file attachments intended to delivery malware.
- Daffodil Gust will set up fake online personas to add legitimacy to their spear phishing. Attackers may engage in a prolonged conversation before sending a weaponized link.
- Post compromise, Daffodil Gust includes DLL sideloading and LOLBin usage to obfuscate their activity and evade detection. They have also been observed using compromised endpoints to access M365 environments to conduct follow-on activity through manipulation of Enterprise Applications.

Storm-0727

Targets

- Cryptocurrency, finance, and government industries in South Korea.

Objectives

- They're a North Korean threat actor that targets South Korea.

ACTIVITY OVERVIEW

- They focus on using cryptocurrency and finance-themed macro-enabled malicious documents.
- They also will register domain infrastructure, commonly through NameCheap. Using TLDs such as .site, .website, and .store.


Tool & Techniques

AccountabilIT
Security Amplified, Cloud Simplified

Medusa Ransomware

Overview

- Medusa payload first appeared in 2021 and has progressed into a ransomware as a service offering.
- Operators typically double extort by encrypting the data and exfiltrating the data and threatening to disclose if the ransom is not paid

Recommendations

- Covering all recommendations associated with mitigating against ransomware is beyond the scope of this briefing but the following areas should be explored.
- Enable all security features of your chosen anti-malware and EDR solutions for tampering resistance, detection capabilities, and automated containment of artifacts and systems when a detection occurs.
- Enable Controlled Folder Access and Attack Surface Reduction rules within Windows Operating Systems.
- Strictly enforce strong MFA configuration (e.g. Passkey, CBA, Hello)

PipeMagic

Overview

- PipeMagic is a modular backdoor used by Storm-2460 masquerading as a ChatGPT Desktop Application.
- Once deployed, it can dynamically execute payloads while maintaining C2 communication via a dedicated networking module.

Recommendations

- Due to the extensive research done on this tool, EDR platforms should be universally able to detect activity from this tool.
- Otherwise, ensure that all EDR capabilities are enabled.

AccountabilIT
Security Amplified, Cloud Simplified

Bad Successor

Overview

- Exploit of a new MSA type for Server 2025 called a Delegated MSA.
- Uses the migration process for converting existing non-managed service accounts to dMSA to allow a dMSA already in the control of the threat actor to inherit the privilege of any account include Domain Admin users.
- Alternatively, any account with the ability to create child objects in an OU could use the same TTP.

Recommendations

- Install security updates to resolve the issue.
- This TTP amongst many other abuse of AD is detected by MDI.
- Keep working on your plans to retire AD.

Vulnerabilities

CVE-2025-53786 – Exchange Server

Impacted Technologies

- Exchange Server 2019 CU14, 2019 CU15, 2016 CU23, Subscription Edition RTM

Risk

- Improper authentication vulnerability that leads to elevation of privileges in a hybrid (or former hybrid) deployment.
- Requires admin access in on-prem to then gain elevation in Exchange Online.
- TTP results creates very few detectable or auditable traces.

Recommendations

- Apply April 2025 hotfix to Exchange
- Rotate auth certificate of the Exchange Server
- Remove all users who can access the certificate using the Exchange Server Certificates role.

CVE-2025-7775 – Citrix Netscaler ADC and NetScaler Gateway

Impacted Technologies

- Citrix NetScaler impacting Load Balancer, VPN, and Gateway components across versions 12.1, 13.1, and 14.1

Risk

- Pretty much all of them: RCE, DOS, and improper access control.
- Citrix has reported exploitation in-the-wild.

Recommendations

- Exploitation affects only certain configurations. See Citrix's notes on how to confirm the configuration of your appliance to confirm applicability.
- If affected, install the updates released by Citrix on August 26, 2025 ASAP!

OSINT

AccountabilIT
Security Amplified, Cloud Simplified

Malicious Use of Memory Forensic Tools

Overview

- Threat actors use memory forensic tools to collect data from physical memory on compromised devices.
- While everyone should be familiar with Mimikatz, there are other tools used to extract information other than just credentials that are less well known that could be less likely to be detected.
- MemProcFS, WinPmem, and Magnet RAM Capture are all such tools. Each goes about collecting memory differently but the result is the same.

Recommendations

- Your EDR is generally going to detect this activity though it may not necessarily directly correlate it to memory forensic tool activity.
- Any system compromised to the point of this level of exploit should just be replaced/rebuilt.

Threats Targeting Microsoft Teams

Overview

- Threat actors misuse trial subscriptions or compromised tenants to masquerade as a trusted user.
- Place calls or send chat message under a false pretense.
- Similar to other spear-phishing this may include other TTPs to create a credible persona to trick our users.
- Common persona usage is tech support as a pretext to engage in a Quick Assist session or remote screenshare which enables the deployment of persistence to the target.

Recommendations

- Ensure Teams deployment aligns to Microsoft good practice recommendations.
- Raise awareness with your users using simulation training

AccountabilIT
Security Amplified, Cloud Simplified

THANK YOU

FOR ATTENDING

Resources List

- Operation Digital Eye | Chinese APT Compromises Critical Digital Infrastructure via Visual Studio Code Tunnels | SentinelOne
- Njrat Campaign Using Microsoft Dev Tunnels - SANS ISC
- AsyncRAT Reloaded: Using Python and TryCloudflare for Malware Delivery Again – Forcepoint
- GLOBAL GROUP: Emerging Ransomware-as-a-Service, Supporting AI Driven Negotiation and Mobile Control Panel for Their Affiliates
- CERT-UA
- Special Report: Inside the UAE's secret hacking team of U.S. mercenaries | Reuters
- #StopRansomware: Medusa Ransomware | CISA
- Kaspersky uncovers PipeMagic backdoor attacks businesses through fake ChatGPT application
- BadSuccessor: Abusing dMSA to Escalate Privileges in Active Directory
- CVE-2025-53786 - Security Update Guide - Microsoft - Microsoft Exchange Server Hybrid Deployment Elevation of Privilege Vulnerability
- MDVM Guidance for CVE-2025-53786: Exchange Hybrid Privilege Escalation | Microsoft Community Hub
- https://security.microsoft.com/threatanalytics3/6ed815e8-b61e-4418-9edb-d44fc38ae41a
- Memory under siege: The silent evolution of credential theft | Microsoft Community Hub
- A familiar playbook with a twist: 3AM ransomware actors dropped virtual machine with vishing and Quick Assist – Sophos News
- Fake Microsoft Teams Emails Phish for Credentials