Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

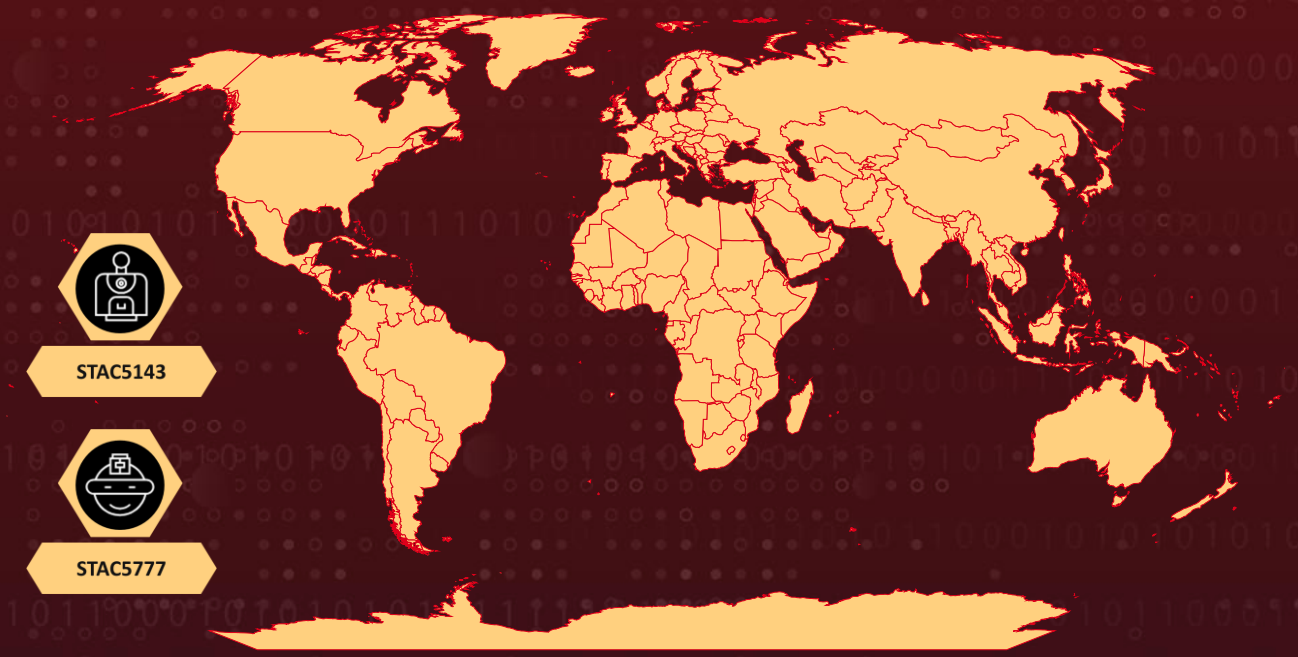
Exploiting Trust: Cybercriminals Abusing Teams Leading to Ransomware Deployment

Date of Publication	Admiralty Code	TA Number
January 23, 2025	A1	TA2025017

Summary

Attack Discovered: November 2024
Targeted Countries: Worldwide
Actor: STAC5143 and STAC5777
Attack: Ransomware gangs are increasingly using sophisticated tactics to infiltrate corporate networks, combining email bombing with impersonation schemes on Microsoft Teams. Threat actors identified as STAC5143 and STAC5777 overwhelm employees with thousands of spam emails in a short time, creating confusion and urgency, and then pose as tech support through Teams calls, exploiting default settings that allow external users to initiate chats and meetings. By masquerading as IT staff, they trick employees into granting remote access to their machines, using legitimate Microsoft tools to install malware, steal sensitive data, and deploy ransomware.

Attack Regions



Attack Details

#1 Sophisticated cyber campaigns have been uncovered involving two threat actors, STAC5143 and STAC5777, who are exploiting Microsoft's Office 365 platform to infiltrate targeted organizations. Both groups leverage a default Microsoft Teams configuration that permits external users to initiate chats or meetings with internal users. While STAC5777 shares similarities with Storm-1811, STAC5143 represents a newly identified cluster adopting similar tactics.

#2 These campaigns relies heavily on advanced social engineering techniques, including email bombing and impersonation of IT support staff via Microsoft Teams. Email bombing involves overwhelming Outlook inboxes with spam to create confusion and urgency. Exploiting this distraction, attackers send Teams messages or make calls from adversary-controlled accounts, posing as internal support representatives like "Help Desk Manager." During these interactions, they persuade victims to start remote screen-sharing sessions, enabling attackers to gain control of their devices. Tools such as Microsoft Quick Assist and Windows Remote Management are then employed to deploy malware and secure a foothold within the compromised network.

#3 STAC5143 displays malware reminiscent of FIN7 but employs a unique attack chain, targeting smaller organizations across diverse industries. Their approach typically begins with spam emails, followed by a Teams call. Once connected, attackers open a command shell to execute Java-based malware and utilize PowerShell commands to download additional payloads. These include a 7zip archive containing ProtonVPN and a malicious DLL, which is side-loaded to establish connections to servers in Russia, the Netherlands, and the US. Further stages involve deploying Python-based payloads, renaming interpreters, and embedding malicious code to maintain control.

#4 STAC5777 adopts a more direct, hands-on strategy by posing as internal IT personnel to engage victims in real-time. Once users are convinced to install Microsoft Quick Assist, attackers gain remote access to the target's device. Malware is then deployed via compressed files saved in the AppData directory under "OneDriveUpdate." These files include legitimate executables combined with unsigned malicious DLLs. Persistence is achieved through PowerShell commands that create services and startup links, ensuring the malware remains active even after a system reboot.

#5 Both groups aim to deploy ransomware or exfiltrate sensitive, in one case they deployed Black Basta Ransomware, showcasing an evolution in tactics that abuse Office 365 features. This campaign highlights the urgent need for organizations to fortify collaboration tools, restrict external communication settings, and raise employee awareness about social engineering threats.

Recommendations

Keep an Eye on Email Bombing and Unusual Activity: Use monitoring tools to spot sudden surges in email traffic or logins from unfamiliar locations. Set up automated alerts to quickly flag these suspicious behaviors, helping you respond before they escalate.

Restrict Microsoft Teams From External Sources: Organizations should configure their Office 365 settings to restrict Microsoft Teams calls from external users, allowing communication only with trusted business partners or approved domains. This prevents unauthorized access and reduces the risk of ransomware gangs exploiting Teams to impersonate tech support and compromise networks.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup, kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Enforce Application Whitelisting: Implement strict application whitelisting policies to prevent unauthorized or malicious executables from running within your environment.

Strengthen Endpoint Defense: Implement advanced Endpoint Detection and Response (EDR) solutions to effectively detect, analyze, and mitigate in-memory malware activity, ensuring comprehensive protection against sophisticated threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	TA0040 Impact	T1090 Proxy	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1049 System Network Connections Discovery	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1105 Ingress Tool Transfer	T1018 Remote System Discovery	T1482 Domain Trust Discovery	T1656 Impersonation

T1036 Masquerading	**T1566** Phishing	**T1037** Boot or Logon Initialization Scripts	**T1021** Remote Services
T1021.001 Remote Desktop Protocol	**T1021.006** Windows Remote Management	**T1005** Data from Local System	**T1486** Data Encrypted for Impact
T1543 Create or Modify System Process	**T1543.003** Windows Service	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	C:\Users\<u>\Downloads\nethost.dll, C:\Users\<username>\Downloads\kb641812-filter-pack-2024-1.dat, C:\Users\<username>\Downloads\kb641812-filter-pack-2024-2.dat, C:\Users\<username>\Downloads\pack.zip, C:\Users\<username>\AppData\Local\OneDriveUpdate\upd2836a.bkt, C:\Users\<username>\AppData\Local\OneDriveUpdate\OneDriveStandaloneUpdater.exe, C:\Users\<username>\AppData\Local\OneDriveUpdate\settingsbackup.dat, C:\Users\<username>\AppData\Local\OneDriveUpdate\winhttp.dll, C:\ProgramData\winter\debug.exe, C:\Users\Public\Documents\MailQueue-Handler\jdk-23.0.1\bin\javaw.exe, C:\Users\Public\Documents\MailQueue-Handler\MailQueue-Handler.jar, C:\Users\Public\Documents\MailQueue-Handler\identity.jar, C:\ProgramData\winter\45_237_80.py, C:\ProgramData\winter\37_44.py, C:\ProgramData\winter\166_65.py, C:\ProgramData\winter.zip
IPv4	74[.]178[.]90[.]36, 195[.]123[.]241[.]24, 207[.]90[.]238[.]46, 78[.]46[.]67[.]201, 207[.]90[.]238[.]99, 109[.]107[.]170[.]2, 195[.]133[.]1[.]117, 206[.]206[.]123[.]75, 194[.]87[.]39[.]183

TYPE	VALUE
SHA256	f009ec775b2daa5a0f38dc2593a3c231611bea7cb579363915d9be1135b00455, 3d0e55bd3c84e6cb35559ef1d0f2ef72a21e0f3793a9158d514f12f46b0aff85, 801525d7239e46f9c22d7e7bcd163abcfb29fc0770ff417f5fc62bfb005ec7ac, ea2b3bf32cc27e959e19c365fa2f6e5310ef2e76d3d0ed2df3fb5945f9afc9e7, 4b6a008c8b85803dc19a8286f33cad963425d37c4ca0b1a9454a854db3273dad, a23560a3b9a9578dcd70bcd01434b2053940d6be36e543df8e4d36931ca9ea63, 4b33c3e3b4b26df0e8efd58e88594a7ee2bd98899451b63d1140eabbca2180a171dc88874b9dcae1f43e312d9e556826b60c1fb, 42d09288a78363cac90759ddce814a420f22d174768c1e406bf2d8fed2c38ade, 8abc8c92ebfe78f54e7488a467d1b6e90d28382067b49a954e31133691112eba, 697d5213d69cdfbd943c6d395f907b8fe210bbfc9d78a9d41a046ba55bebb5ff
Registry Key	HKEY_LOCAL_MACHINE\SOFTWARE\TitanPlus\
Email	helpdesk@llladminhlpll[.]onmicrosoft[.]com

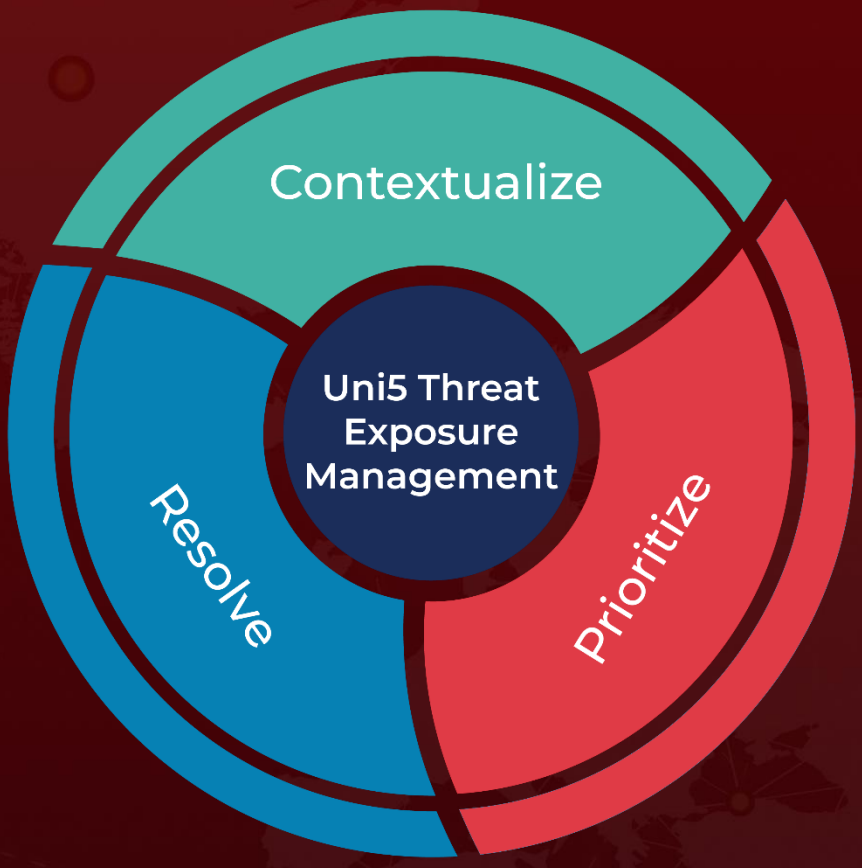
References

https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 23, 2025 • 6:30 AM

More at www.hivepro.com