Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

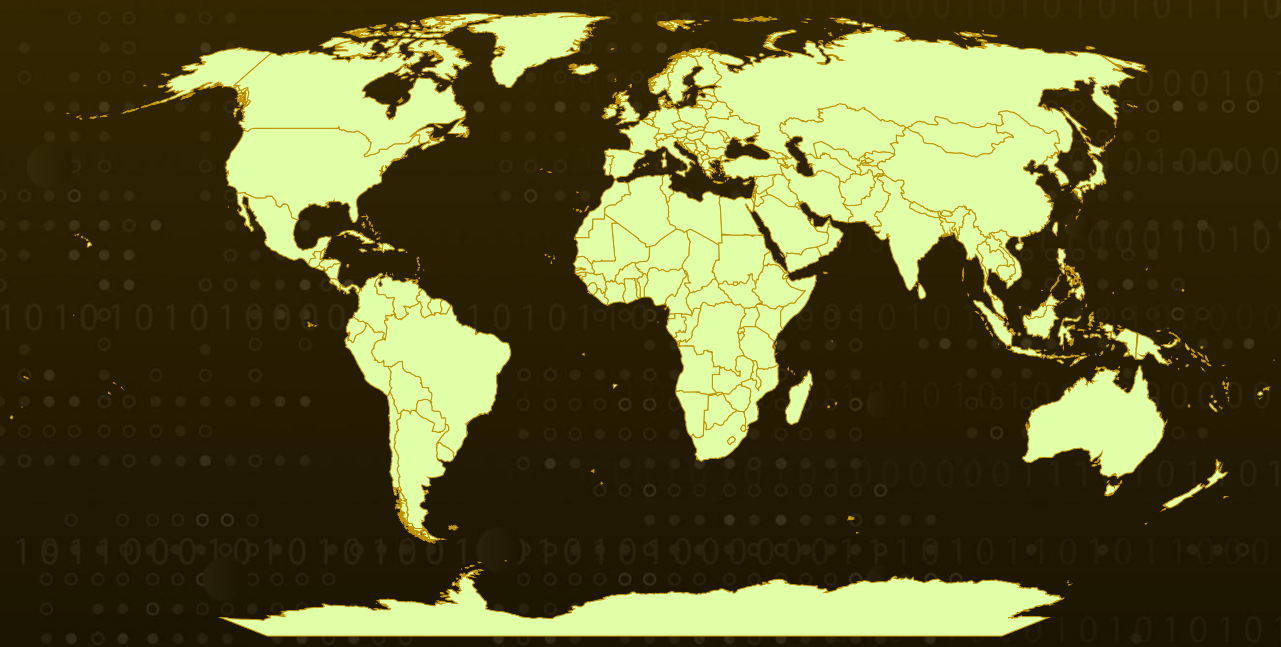
SynkLoader: When a Teams Message Fakes Your Lock Screen

Date of Publication	Admiralty Code	TA Number
August 25, 2026	A1	TA2026245

Summary

First Seen: Around July 28, 2026
Targeted Regions: Worldwide
Targeted Platform: Windows
Malware: SynkLoader
Attack: SynkLoader is a newly discovered, modular malware family spread through Microsoft Teams phishing. The attacker poses as the company's IT help desk and talks an employee into installing a fake "PowerShell Cleaner" MSI hosted on Microsoft Azure. That installer kicks off a Python-based loader that pulls a chain of memory-resident modules from its command-and-control server. The standout capability is a fake Windows lock screen that harvests the victim's real login password, which the operators can then pair with a built-in reverse proxy to log into internal and external company systems as the user.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

Microsoft Teams phishing is once again being used as the doorway to deliver malware, this time a new family called SynkLoader. An account using a company.onmicrosoft.com address, Microsoft 365's default domain for organizations, contacts a target under the name "IT Service Desk," borrowing the trust employees place in internal support. The attacker persuades the user to download and run an MSI installer from a Microsoft Azure file storage endpoint, which makes the file look as though it came straight from Microsoft. The installer presents itself as a helpful utility called "PowerShell Cleaner" and serves as the first stage of the attack.

#2

Once launched, the MSI drops a PowerShell script and a ZIP archive into the user's local application-data folder and runs the script automatically. The script opens a hidden PowerShell window and rebuilds its real payload from hex-encoded values, then decodes and decrypts a Base64, AES-CBC-protected command that runs entirely in memory, leaving nothing on disk from that point on. It creates a randomly named install folder, unpacks a self-contained Python environment shipped with the malware, and launches the main loader (ss.py). The loader picks one of three hardcoded C2 domains, beacons every 90 to 120 seconds, and encrypts its traffic with a modified ChaCha20 cipher keyed to a unique victim ID. Whatever Python code the server returns is run straight through exec, giving the operators arbitrary code execution. Persistence is handled by a module that manually maps a DLL into memory and creates a scheduled task through the Task Scheduler COM interface rather than the schtasks command line, sidestepping many behavioral detections. The task relaunches the loader at every logon and again daily at 10 a.m.

#3

After the loader checks in and profiles the machine, the operators push modules built for moving deeper into the network. The PhishLocker module renders a near-perfect copy of the Windows lock screen to trick the user into typing their password, capturing the raw credential instead of a hash and avoiding noisy tools like Mimikatz. Because many organizations rely on single sign-on, that one password opens the door to far more than the local machine. A companion TrafficRedirector module acts as a backconnect reverse proxy, connecting outward to the attacker's server and then relaying traffic to any internal or external endpoint the operators choose. Combined with the stolen password, this lets the attackers sign into corporate systems from the victim's own device and IP address, avoiding alerts tied to unfamiliar logins or geolocations.

#4

Reconnaissance and remote control round out the toolkit. A system profiler gathers the hostname, logged-on user, privilege level, running processes, installed services, the Active Directory domain name, and a count of how many computers are joined to the domain, using a fake msvcp150.dll that quietly runs PowerShell in memory. An interactive shell module lets the operators run PowerShell commands in real time for hands-on-keyboard activity, and a VNC module named StreamMaster streams screenshots of the live session and relays mouse and keyboard input back to the attacker. Traffic to the C2 stays encrypted throughout. Expel found no reliable attribution but assessed with low-to-medium confidence that the heavy focus on measuring Active Directory size points toward a ransomware group or an initial access broker who sells access to one.

Recommendations

- **Verify Help Desk Requests Out of Band:** Treat any unexpected Teams message from "IT" that asks you to install software as suspicious. Confirm the request through a known internal channel or a verified support contact before downloading or running anything.
- **Restrict External Teams Messaging:** Limit or closely monitor chats and calls from external and onmicrosoft.com accounts impersonating internal staff, and preserve Teams audit records so suspicious helpdesk-impersonation activity can be investigated.
- **Block Unapproved MSI Execution:** Use application control or allow-listing to stop MSI packages from launching out of user-writable folders such as the Downloads and AppData directories, and flag MSI installs pulled from cloud storage endpoints like Azure Blob Storage.
- **Block the Known C2 Infrastructure:** Block or closely inspect traffic to the listed command-and-control domains (neversoftmain[.]net, rootfarmapp[.]net, tripinupdate[.]net, dondermicapp[.]net, aroclenetapp[.]net) at the DNS and network layer.
- **Hunt for Suspicious Scheduled Tasks:** Look for randomly named scheduled tasks that launch pythonw.exe from an AppData subfolder and trigger at logon and at 10 a.m. daily. Because the task is created via the COM interface, hunt on the task artifacts themselves rather than relying only on schtasks.exe command-line logging.

Watch for In-Memory PowerShell and Python Loaders: Alert on pythonw.exe running scripts from user-writable directories, on CPython loading DLLs that masquerade as Microsoft runtime libraries (msvcp150.dll, msvcp160.dll), and on in-memory PowerShell execution that does not touch disk.

Teach Users to Spot the Fake Lock Screen: Train staff that a genuine Windows lock screen cannot be bypassed with Alt+Tab and that a real login always blurs the background when the password box is focused. When faced with an unexpected lock screen, use Ctrl+Alt+Delete or Alt+Tab to test whether it is real.

Reset Credentials on Suspected Compromise: If a fake lock screen or SynkLoader activity is found, immediately reset the affected user's password and any linked SSO credentials, and review recent sign-ins from the host for signs of misuse.

Enforce Phishing-Resistant MFA and Conditional Access: Require phishing-resistant multi-factor authentication and conditional access policies so that a stolen password alone cannot grant access to sensitive internal and cloud systems.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
	T1656: Impersonation	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.006: Python
Defense Evasion	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	

Tactic	Technique	Sub-technique
Defense Evasion	T1620: Reflective Code Loading	
	T1559: Inter-Process Communication	T1559.001: Component Object Model
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Credential Access	T1056: Input Capture	T1056.002: GUI Input Capture
Discovery	T1082: System Information Discovery	
	T1033: System Owner/User Discovery	
	T1057: Process Discovery	
	T1007: System Service Discovery	
	T1018: Remote System Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1105: Ingress Tool Transfer	
	T1090: Proxy	T1090.002: External Proxy
	T1219: Remote Access Software	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	151d2a7f52f047638ca8ad80c859c6bfe04d7510fb10933817fa0e3ba5d07a11, 80f08360ba768b152b71abb1cab557f552a13de18c83fe8e6396a197feec9185, 209f69a6ca859f05c954096b30391a43fda33c9ed264dfdccf806697f04b06a8, d150c70d2732df17aa77991b9ebf4c896f044445e900978581d9598dfa5dc98c, 61f961cfebdf9967844526649b4b75bba5b1b83210b70aa1bffe3f64e6ac3112, 8207d8d949530ea063ffd5d47ee81b74bf718ec0a4755e2349e6af9b91e92dc1, c4acda412774c292f0db5d64467a2dd09282cdea43c41967e8bf90f6298accf3, 63622c1ddb3e2a9f11cac192e13ac7494f558516b19d5d8f140f6d0d4d38ea84, a335e75b78b601ebc5c258975d95fd79aa21f836fc6b79d82e9a22c596133f07, 0428fbdefa8dda10ce8fc12b1b516641e83cd5088388168e3f1a0be1432b4077, cb1c657f74b9e57f5e81126179128e8db949d1d4196be9dcb890341e222fd384
Domains	neversoftmain[.]net, rootfarmapp[.]net, tripinupdate[.]net, dondermicapp[.]net, aroclenetapp[.]net
URL	hxxps[:]//filereserve[.]blob[.]core[.]windows[.]net/vgnghuyk/331/331[.]msi

References

https://expel.com/blog/synkloader-when-you-throw-in-everything-but-the-kitchen-sink/

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 Demo of **HivePro**.

REPORT GENERATED ON

August 25, 2026 • 08:15 AM

More at www.hivepro.com