INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 06:49 UTC

TA4922 Expands Into Europe Deploying Novel Atlas RAT With Suspected LLM-Assisted Development

THREAT ACTOR | HIGH | CVSS 7.5

SCC Item ID	SCC-TAC-2026-0022
Type	Threat Actor
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Google Chrome (credential theft target), AnyDesk (delivery/lateral movement vector), SyncFuture (delivery vector), Microsoft Teams (delivery vector), Microsoft Defender Application Guard (anti-sandbox evasion target)
Published	2026-06-03T17:45:27
Discovery Source	Rss

Executive Summary

A Chinese-speaking cybercrime group designated TA4922 has expanded operations into Germany, Italy, and the United Kingdom, deploying a newly documented remote access trojan called Atlas RAT alongside at least three other malware families. Proofpoint has identified TA4922 as the most prolific cybercrime actor by unique campaign volume as of early 2026, with delivery chains abusing Microsoft Teams voice phishing, AnyDesk remote access software, and the SyncFuture platform to gain initial footholds in enterprise environments. The group harvests credentials from Google Chrome, maintains persistent remote access, and its dual-use surveillance tooling raises credible risk of intelligence transfer to state-aligned operators.

Technical Analysis

TA4922 is a Chinese-speaking threat actor that pivoted from East Asian targeting to European enterprises in early 2026. The group deploys Atlas RAT, a newly documented remote access trojan with suspected LLM-assisted development, alongside additional malware families whose names are not confirmed in verified sources available for this report. Delivery vectors include Microsoft Teams vishing (T1566.004), spearphishing attachments and links (T1566.001, T1566.002), and abuse of AnyDesk (T1219) and SyncFuture as remote access and delivery platforms. Post-access tradecraft includes process injection (T1055, T1055.012), command and scripting interpreter abuse (T1059, T1059.006), obfuscated file execution (T1027), credential harvesting

from Google Chrome credential stores (T1555.003), cookie/session theft (T1539), keylogging (T1056.001), audio and video capture (T1123, T1125), screenshot capture (T1113), ingress tool transfer (T1105), sandbox evasion targeting Microsoft Defender Application Guard (T1497), and valid account abuse (T1078). Relevant CWEs include CWE-693 (Protection Mechanism Failure, reflecting sandbox bypass), CWE-506 (Embedded Malicious Code), and CWE-494 (Download of Code Without Integrity Check). No CVE identifiers are associated with this activity; exploitation relies on social engineering and tool abuse rather than known unpatched vulnerabilities. Source note: the primary BleepingComputer article URL could not be actively verified per session URL policy, human validation of that source is recommended before operationalizing specific IOCs or tooling details from this report. DarkGate-related sources in the source list are from late 2024 and reference a separate campaign; they were not used in this analysis.

Action Checklist

1. Containment, Audit and restrict AnyDesk deployment: identify all endpoints with AnyDesk installed (CIS 1.1, Asset Inventory), block unauthorized AnyDesk instances at the endpoint firewall (CIS 4.4, CIS 4.5), and enforce application allowlisting to prevent unapproved remote access tools. Block SyncFuture domains at the proxy and DNS layer pending threat confirmation. Restrict Microsoft Teams external communication to verified tenant domains only (NIST AC-4, Information Flow Enforcement).

2. Detection, Hunt for Atlas RAT and associated tooling using the following indicators: (a) AnyDesk process spawning child processes or initiating outbound connections to non-standard destinations; (b) Microsoft Teams client spawning PowerShell, cmd.exe, or mshta.exe (MITRE T1059, T1059.006, monitor Windows Security Event ID 4688 with command-line auditing enabled, per NIST AU-2, Event Logging and AU-12, Audit Record Generation); (c) Chrome credential store access from non-browser processes (target path: AppData\Local\Google\Chrome\User Data\Default\Login Data); (d) process injection artifacts including unusual parent-child process relationships and cross-process memory writes (T1055, T1055.012); (e) outbound connections to newly registered or low-reputation domains from endpoints (AU-6, Audit Record Review). Enable CIS 8.2 (Collect Audit Logs) across all endpoints if not already active. Note: specific IOC values (hashes, IPs, C2 domains) are not confirmed in verified sources available for this report, obtain from Proofpoint's published research or ISAC feeds before building signature-based detections.

3. Eradication, Remove unauthorized AnyDesk installations and revoke any AnyDesk access IDs created during the suspected intrusion window (NIST AC-2, Account Management; D3-CRO, Credential Rotation). Rotate all credentials accessible from affected endpoints, prioritizing Chrome-stored passwords and session cookies (D3-CH, Credential Hardening). Disable or quarantine any endpoint where Atlas RAT execution is confirmed. Re-image compromised hosts rather than attempting in-place cleanup given the RAT's persistence and injection capabilities. Remove SyncFuture from authorized software inventory if not business-justified (CIS 2.3, Address Unauthorized Software).

4. Recovery, Validate endpoint integrity before returning hosts to production: confirm no persistence mechanisms remain in scheduled tasks, registry run keys, or startup directories (D3-SICA, System Init Config Analysis; D3-SFA, System File Analysis). Verify that Microsoft Teams external access policies are correctly scoped. Re-enroll affected users in MFA and confirm MFA enforcement on all externally exposed applications (CIS 6.3, CIS 6.5, Require MFA; D3-MFA, Multi-factor Authentication). Monitor re-introduced endpoints for 30 days using enhanced logging (NIST SI-4, System Monitoring) with alerts on the behavioral indicators identified in the Detection step.

5. Post-Incident, Review and close the control gaps this campaign exposed: (a) MFA enforcement gaps on Microsoft Teams external communications and remote access paths (CIS 6.3, 6.4, 6.5); (b) unauthorized software on endpoints, specifically remote access tools not approved through a formal process (CIS 2.1, 2.3, Software Inventory and Unauthorized Software); (c) absence of outbound proxy inspection for newly registered domains (NIST SC-7, Boundary Protection); (d) user awareness training on Teams-based vishing, which bypasses traditional email phishing controls (NIST AT-2, Literacy Training and Awareness). Document lessons learned in a formal post-incident review per NIST IR-4, Incident Handling.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior leadership, legal counsel, and relevant data protection authorities (ICO for UK, Garante for Italy, BfDI for Germany) immediately if forensic evidence confirms Chrome credential exfiltration from any endpoint, as the combination of TA4922's confirmed targeting of European operations and Atlas RAT's credential harvesting capability creates a high-probability personal data breach triggering GDPR Article 33 notification obligations within 72 hours of confirmation.
Recovery Notes	Before any compromised host is returned to production, obtain a clean OS image from vendor media rather than restoring from backup snapshots taken after the earliest possible intrusion date, as Atlas RAT's process injection capability (T1055.012) means pre-remediation backups may contain dormant malicious code. Monitor re-introduced endpoints for a minimum of 30 days with Sysmon verbose logging, specifically alerting on any process spawning from `AnyDesk.exe`, `Teams.exe`, or newly installed remote access utilities, and on any file access to Chrome credential stores from non-browser processes. Maintain enhanced DNS query logging at the resolver level for the same 30-day window to detect Atlas RAT C2 beacon attempts using domain generation or low-reputation infrastructure consistent with TA4922's documented use of newly registered domains.
Forensic Artifacts	AnyDesk session trace logs at `%ProgramData%\AnyDesk\ad_svc.trace` (service) and `%AppData%\AnyDesk\ad.trace` (user) — these record every inbound and outbound session ID, connecting IP address, session duration, and file transfer event, directly attributing TA4922 operator infrastructure to the compromise timeline. | Chrome SQLite credential database at `%LocalAppData%\Google\Chrome\User Data\Default\Login Data` — Atlas RAT targets this file for credential harvesting; examine `date_last_used`, `times_used`, and `date_password_changed` columns for entries accessed during the intrusion window by a non-Chrome process, identifiable via file system last-access timestamps and Sysmon Event ID 10 (Process Access) logs. | Windows Prefetch files at `C:\Windows\Prefetch\` — even if Atlas RAT binaries were deleted post-execution, Prefetch entries (readable with PECmd from Eric Zimmerman's tools, free) will record the executable name, run count, last run timestamp, and file paths accessed, providing evidence of staging tool execution during the AnyDesk session. | Microsoft Teams audit logs exported from the M365 Compliance Center (Unified Audit Log, `TeamsSessionsData` and `MeetingParticipantDetail` workloads) — these record the external tenant identity and IP address of the TA4922 vishing caller, establishing the initial access event timestamp and attacker infrastructure details independent of endpoint telemetry. | Windows Security Event ID 4688 (Process Creation with command-line auditing enabled) from affected hosts filtered on parent processes `AnyDesk.exe` and `Teams.exe` — this log source directly captures the execution chain from TA4922's remote access session through Atlas RAT staging commands, including any PowerShell or mshta.exe invocations used to deploy the RAT payload from SyncFuture or other delivery infrastructure.

Per-Action IR Details

Containment — Immediately audit and restrict AnyDesk deployment: identify all endpoints with AnyDesk installed (CIS 1.1 — Asset Inventory), block unauthorized AnyDesk instances at the endpoint firewall (CIS 4.4, CIS 4.5), and enforce application allowlisting to prevent unapproved remote access tools. Block SyncFuture domains at the proxy and DNS layer pending threat confirmation. Restrict Microsoft Teams external communication to verified tenant domains only (NIST AC-4 — Information Flow Enforcement).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), NIST CM-7 (Least Functionality), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run the following on Windows endpoints to enumerate AnyDesk installations: `Get-WmiObject Win32_Product | Where-Object { $_.Name -like '*AnyDesk*' } | Select-Object Name, InstallLocation, InstallDate` and `Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Where-Object { $_.DisplayName -like '*AnyDesk*' }`. Block AnyDesk network relay servers (relay.anydesk.com, *.relay.anydesk.com) and SyncFuture domains at the perimeter firewall using host-based Windows Firewall rules: `netsh advfirewall firewall add rule name='Block AnyDesk' dir=out action=block remotehost=relay.anydesk.com`. For Teams external access restriction, use the Microsoft Teams Admin Center (free with M365 tenancy) to set external access policy to allow only specific verified domains.

Evidence: Before restricting AnyDesk, capture: (1) AnyDesk installation logs at `%ProgramData%\AnyDesk\ad_svc.trace` and `%AppData%\AnyDesk\ad.trace` which record all session IDs, remote IP addresses, and connection timestamps used by TA4922 operators; (2) Windows Security Event ID 4698 (Scheduled Task Created) and Event ID 7045 (New Service Installed) from the System log to identify persistence mechanisms AnyDesk or Atlas RAT may have registered during the access window; (3) DNS query logs from the local DNS resolver or endpoint hosts file for any SyncFuture-related domains to establish delivery chain timing; (4) Microsoft Teams audit logs (via M365 Compliance Center) for external call and chat session records showing the vishing contact originating from outside verified tenant domains.

Detection — Hunt for Atlas RAT and associated tooling using the following indicators: (a) AnyDesk process spawning child processes or initiating outbound connections to non-standard destinations; (b) Microsoft Teams client spawning PowerShell, cmd.exe, or mshta.exe (MITRE T1059, T1059.006 — monitor Windows Security Event ID 4688 with command-line auditing enabled, per NIST AU-2 — Event Logging and AU-12 — Audit Record Generation); (c) Chrome credential store access from non-browser processes (target path: AppData\Local\Google\Chrome\User Data\Default\Login Data); (d) process injection artifacts including unusual parent-child process relationships and cross-process memory writes (T1055, T1055.012); (e) outbound connections to newly registered or low-reputation domains from endpoints (AU-6 — Audit Record Review). Enable CIS 8.2 (Collect Audit Logs) across all endpoints if not already active. Note: specific IOC values (hashes, IPs, C2 domains) are not confirmed in verified sources available for this report — obtain from Proofpoint's published research or ISAC feeds before building signature-based detections.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a community config (SwiftOnSecurity or Olaf Hartong's modular config) targeting: Sysmon Event ID 1 (Process Create) filtering on `ParentImage` containing `AnyDesk.exe` or `Teams.exe` with `Image` containing `powershell.exe`, `cmd.exe`, or `mshta.exe`; Sysmon Event ID 10 (Process Access) where `TargetImage` contains `chrome.exe` and `SourceImage` does NOT contain `chrome.exe` or `GoogleUpdate.exe` — this catches Atlas RAT's credential theft from Chrome's `Login Data` SQLite file. For injection detection, use Sysmon

Event ID 8 (CreateRemoteThread) filtered on cross-process writes from non-system parent processes. Write a YARA rule scanning for Atlas RAT staging directories and dropped payloads in `%TEMP%`, `%APPDATA%\Roaming`, and `%PROGRAMDATA%`. Use osquery to continuously query `SELECT pid, name, path, cmdline FROM processes WHERE name IN ('powershell.exe','cmd.exe','mshta.exe') AND parent IN (SELECT pid FROM processes WHERE name IN ('AnyDesk.exe','Teams.exe'))` on a 5-minute schedule.

Evidence: Capture before or concurrent with hunting: (1) Sysmon Event ID 1 logs showing the full command-line of any child process spawned from `AnyDesk.exe` or `Teams.exe`, including base64-encoded PowerShell payloads characteristic of LLM-assisted malware with clean syntax; (2) file system artifacts at `%AppData%\Local\Google\Chrome\User Data\Default\Login Data` — check file last-accessed timestamp against the suspected intrusion window, as Atlas RAT accesses this SQLite database to extract stored credentials; (3) Windows Prefetch files (`C:\Windows\Prefetch\`) for evidence of Atlas RAT executable names and staging tools run during the access window, even if binaries have since been deleted; (4) network connection records via `netstat -anob` output (captured live) or Sysmon Event ID 3 (Network Connection) showing `AnyDesk.exe` connecting to IPs outside the known AnyDesk relay address range, indicating C2 tunneling; (5) Volume Shadow Copy or MFT entries for recently created and deleted executables in user-writable directories during the AnyDesk session window.

Eradication — Remove unauthorized AnyDesk installations and revoke any AnyDesk access IDs created during the suspected intrusion window (NIST AC-2 — Account Management; D3-CRO — Credential Rotation). Rotate all credentials accessible from affected endpoints, prioritizing Chrome-stored passwords and session cookies (D3-CH — Credential Hardening). Disable or quarantine any endpoint where Atlas RAT execution is confirmed. Re-image compromised hosts rather than attempting in-place cleanup given the RAT's persistence and injection capabilities. Remove SyncFuture from authorized software inventory if not business-justified (CIS 2.3 — Address Unauthorized Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST CM-7 (Least Functionality), NIST SI-2 (Flaw Remediation), CIS 2.3 (Address Unauthorized Software), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: To enumerate and revoke AnyDesk access IDs without enterprise tooling: check `%ProgramData%\AnyDesk\service.conf` and `%AppData%\AnyDesk\user.conf` for the assigned AnyDesk ID and any saved unattended-access passwords, then log into the AnyDesk web portal to revoke those IDs and reset the account namespace. For credential rotation on Chrome-stored secrets without a PAM tool, use the following PowerShell to identify which credential domains were stored: `$db = 'C:\Users\\AppData\Local\Google\Chrome\User Data\Default\Login Data'; Copy-Item $db $env:TEMP\LD_backup.db; sqlite3 $env:TEMP\LD_backup.db 'SELECT origin_url, username_value FROM logins'` — prioritize rotating accounts for any SaaS, VPN, or email services returned. For Atlas RAT persistence sweep prior to re-imaging decision, run Autoruns (Sysinternals, free) to enumerate all run keys, scheduled tasks, services, and browser extensions modified during the intrusion window.

Evidence: Before eradication actions, preserve: (1) a full forensic image or at minimum a memory capture (using WinPmem, free) of any host with confirmed Atlas RAT execution, as the RAT's injection capabilities (T1055.012 — Process Hollowing) mean artifacts exist in memory that will not survive re-image; (2) AnyDesk session logs at `%ProgramData%\AnyDesk\ad_svc.trace` documenting operator IP addresses, session durations, and file transfer events initiated by TA4922 during the intrusion; (3) a copy of the Chrome `Login Data` SQLite file from affected user profiles — the file's internal `date_last_used` and `times_used` fields per credential entry will show which stored passwords Atlas RAT specifically accessed or exfiltrated; (4) Windows Security Event ID 4720 (User Account Created) and 4732 (Member Added to Security-Enabled Local Group) from affected hosts to identify any backdoor local accounts TA4922 may have established for persistence independent of AnyDesk.

Recovery — Validate endpoint integrity before returning hosts to production: confirm no persistence mechanisms remain in scheduled tasks, registry run keys, or startup directories (D3-SICA — System Init Config Analysis; D3-SFA — System File Analysis). Verify that Microsoft Teams external access policies are correctly scoped. Re-enroll affected users in MFA and confirm MFA enforcement on all externally exposed

applications (CIS 6.3, CIS 6.5 — Require MFA; D3-MFA — Multi-factor Authentication). Monitor re-introduced endpoints for 30 days using enhanced logging (NIST SI-4 — System Monitoring) with alerts on the behavioral indicators identified in the Detection step.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST CP-10 (System Recovery and Reconstitution), NIST IA-5 (Authenticator Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For integrity validation without EDR, use Sysinternals Autoruns (`autorunsc.exe -a * -c -h -s > autoruns_baseline.csv`) on rebuilt hosts and diff against a known-clean baseline from an unaffected peer system — flag any entries in `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`, or `%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup` not present in the baseline. For Teams policy verification, run `Get-CsExternalAccessPolicy` via PowerShell (requires Microsoft Teams PowerShell module, free) to confirm `EnableFederationAccess` is constrained to approved tenant domains. For 30-day enhanced monitoring on re-introduced hosts, configure Sysmon with verbose network logging (Event ID 3) and centralize to a free ELK Stack or Graylog instance, alerting on the parent-child process relationships identified in the Detection step.

Evidence: Before returning endpoints to production, validate and retain: (1) Autoruns diff output comparing the rebuilt host against a clean baseline — any unexplained entries in shell extension or Winlogon locations should be treated as Atlas RAT reinfection until proven otherwise; (2) confirmation screenshot or export from the Microsoft Teams Admin Center showing external access policy scoped to verified tenant domains only, timestamped as post-remediation evidence for the incident record; (3) Windows Security Event ID 4648 (Logon Using Explicit Credentials) and 4624 (Successful Logon) from re-introduced hosts during the first 72 hours to detect any TA4922 re-entry attempts using credentials harvested by Atlas RAT from Chrome before eradication.

Post-Incident — Review and close the control gaps this campaign exposed: (a) MFA enforcement gaps on Microsoft Teams external communications and remote access paths (CIS 6.3, 6.4, 6.5); (b) unauthorized software on endpoints, specifically remote access tools not approved through a formal process (CIS 2.1, 2.3 — Software Inventory and Unauthorized Software); (c) absence of outbound proxy inspection for newly registered domains (NIST SC-7 — Boundary Protection); (d) user awareness training on Teams-based vishing, which bypasses traditional email phishing controls (NIST AT-2 — Literacy Training and Awareness). Document lessons learned in a formal post-incident review per NIST IR-4 — Incident Handling.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST AT-2 (Literacy Training and Awareness), NIST SC-7 (Boundary Protection), NIST RA-3 (Risk Assessment), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For outbound proxy inspection of newly registered domains without a commercial proxy: deploy Pi-hole or pfSense with pfBlockerNG (both free) configured with threat feed subscriptions (Abuse.ch URLhaus, CISA Known Bad Domains) that flag domains registered within the last 30 days. For Teams vishing awareness training specific to this campaign, create a tabletop exercise scenario where an external caller impersonates IT support via Teams voice call and requests AnyDesk installation — this directly mirrors TA4922's documented delivery chain and requires no budget beyond facilitator time. Document the formal lessons-learned report using NIST 800-61r3 Appendix B format, capturing: initial access vector (Teams vishing), dwell time, credential exposure scope from Chrome, and control gaps in remote access software governance.

Evidence: Retain for the post-incident record and potential regulatory reporting: (1) the complete AnyDesk session trace logs establishing the timeline from initial TA4922 contact through Atlas RAT deployment, required to calculate dwell time and scope of credential exposure for any breach notification assessment under GDPR (given confirmed

targeting of Germany, Italy, and UK); (2) a documented software inventory delta showing AnyDesk and SyncFuture present on endpoints without a formal approval record, as evidence for the CIS 2.1/2.3 control gap finding; (3) Microsoft Teams external access policy configuration export from before and after remediation, demonstrating the gap that allowed TA4922 to initiate unsolicited voice contact; (4) aggregate metrics from the 30-day enhanced monitoring period on re-introduced hosts, confirming no reinfection and establishing a behavioral baseline for future Atlas RAT detection rule tuning.

Detection Guidance

Primary behavioral indicators: (1) Microsoft Teams client spawning shell interpreters, monitor Event ID 4688 for parent process teams.exe or ms-teams.exe with children including powershell.exe, cmd.exe, wscript.exe, or mshta.exe; requires command-line auditing enabled per NIST AU-2. (2) AnyDesk initiating lateral movement, alert on AnyDesk processes making outbound connections outside approved management subnets, or spawning additional executables (T1219). (3) Chrome credential store access from non-browser processes, monitor file system access to AppData\Local\Google\Chrome\User Data\Default\Login Data and Cookies by any process other than chrome.exe (T1555.003, T1539). (4) Process injection artifacts, detect cross-process memory writes (OpenProcess + WriteProcessMemory API sequences), CreateRemoteThread calls, and unusual parent-child process trees inconsistent with normal application behavior (T1055, T1055.012). (5) Anti-sandbox probing, look for enumeration of Microsoft Defender Application Guard container artifacts or VM detection routines (T1497). (6) Outbound connections from endpoints to SyncFuture infrastructure or newly registered domains via non-standard ports. CIS 8.2 (Collect Audit Logs) must be active across all endpoints for these queries to be viable. Specific hash, IP, and C2 domain IOCs are not confirmed in verified sources available for this report; obtain current IOCs from Proofpoint's published research or your threat intelligence platform before deploying signature-based rules. Apply D3-LAM (Local Account Monitoring) to detect any local accounts created during the intrusion window.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`syncfuture[.]com or associated infrastructure`	SyncFuture platform abused as a malware delivery vector by TA4922; treat all SyncFuture-originating connections as suspicious in enterprise environments where this platform is not authorized	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1078** — Valid Accounts
- **T1497** — Virtualization/Sandbox Evasion
- **T1059.006** — Python
- **T1566.001** — Spearphishing Attachment

- **T1055** — Process Injection
- **T1123** — Audio Capture
- **T1027** — Obfuscated Files or Information
- **T1566** — Phishing
- **T1539** — Steal Web Session Cookie
- **T1566.002** — Spearphishing Link
- **T1555.003** — Credentials from Web Browsers
- **T1566.004** — Spearphishing Voice
- **T1055.012** — Process Hollowing
- **T1113** — Screen Capture
- **T1219** — Remote Access Tools
- **T1125** — Video Capture
- **T1056.001** — Keylogging
- **T1105** — Ingress Tool Transfer
- **T1204** — User Execution

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **CA-7** — Continuous Monitoring
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1078	Valid Accounts	Defense-Evasion
T1497	Virtualization/Sandbox Evasion	Defense-Evasion
T1059.006	Python	Execution
T1566.001	Spearphishing Attachment	Initial-Access
T1055	Process Injection	Defense-Evasion
T1123	Audio Capture	Collection
T1027	Obfuscated Files or Information	Defense-Evasion
T1566	Phishing	Initial-Access
T1539	Steal Web Session Cookie	Credential-Access
T1566.002	Spearphishing Link	Initial-Access
T1555.003	Credentials from Web Browsers	Credential-Access
T1566.004	Spearphishing Voice	Initial-Access
T1055.012	Process Hollowing	Defense-Evasion
T1113	Screen Capture	Collection
T1219	Remote Access Tools	Command-And-Control
T1125	Video Capture	Collection
T1056.001	Keylogging	Collection
T1105	Ingress Tool Transfer	Command-And-Control
T1204	User Execution	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/chinese-hackers-use-...	T3
Attackers Exploit Microsoft Teams and AnyDesk to Deploy DarkGate ...	https://thehackernews.com/2024/12/attackers-exploit-microsoft-teams...	T3
Vishing via Microsoft Teams Facilitates DarkGate Malware Intrusion	https://www.trendmicro.com/en_us/research/24/l/darkgate-malware.html	T3
Attackers Exploit Microsoft Teams and AnyDesk to Deliver DarkGate ...	https://logsentinel.com/blog/attackers-exploit-microsoft-tems-and-a...	T3
Garett Moreau 's Post - LinkedIn	https://www.linkedin.com/posts/garettm_attackers-exploit-microsoft-...	T3

Generated 2026-06-04 06:49 UTC by TJS Security Command Center