SECURITY ADVISORY

September, 2025

Lazarus Group Expands Malware Arsenal with New RAT Families

Context

The Lazarus Group, a North Korea–linked advanced persistent threat (APT), has introduced three new malware families — PondRAT, ThemeForestRAT, and RemotePE — into its operational toolkit.

The emergence of these new tools underscores a broader strategic shift by Lazarus: leveraging enhanced persistence, accelerated lateral movement, and a heightened focus on espionage to reinforce its operational advantage. By actively developing techniques that bypass traditional endpoint defences, the group is extending dwell time within high-value environments such as financial institutions, defence contractors, and critical infrastructure operators. This evolution demonstrates Lazarus's capacity to outpace conventional detection models and adapt with speed to advancing security controls.

This advisory details the technical capabilities of these malware families, outlines their strategic implications, and provides actionable recommendations for security leaders to strengthen their defensive posture.

Mitigation

Defending against Lazarus Groups' new malware families requires a proactive, layered security approach.

Restrict LOLBins and PowerShell — Abuse Lock down mshta.exe, rundll32.exe, regsvr32.exe, and enforce PowerShell Constrained Language Mode with full script logging to disrupt fileless execution.

Persistence Hunting & Drift Detection — Regularly audit Startup folders, Scheduled Tasks, and Services for disguised entries (e.g., AdobeUpdateService) and flag configuration drift to catch stealth persistence.

Segmentation and Credential Protection — Enforce strict network segmentation and monitor privileged account use (PsExec/SMB) to prevent RemotePE from propagating with stolen credentials.

Technical Details

PondRAT

Fileless Trojan with Modular Espionage Capabilities

PondRAT represents Lazarus's growing investment in fileless malware and modular plug-ins, allowing long-term access with minimal forensic footprint. Delivered via malicious Office macros and PowerShell stagers, it executes almost entirely in memory, leveraging reflective DLL injection to blend into core Windows processes. Its persistence mechanisms are deceptively simple, using scheduled tasks and Run keys disguised as legitimate update services, while its command set enables system reconnaissance, credential theft, and targeted exfiltration. The addition of modules such as a keylogger and browser credential exfiltrator highlights Lazarus's continued prioritisation of espionage and credential harvesting within financial and government networks.

Type: Remote Access Trojan (RAT) with obfuscation/masquerading.

Category	Details
Delivery/Loader	Malicious Office macros, PowerShell stagers. Core implant written in C/C++ with PowerShell loaders.
Execution	Fileless via `powershell.exe -EncodedCommand …`; reflective DLL injection into `explorer.exe` / `svchost.exe`. Typical chain: `winword.exe → powershell.exe → explorer.exe/svchost.exe`.
Persistence	Registry Run keys (`AdobeUpdateService`), disguised Scheduled Tasks.
C2	HTTPS (443) with Base64 + RC4 encryption. Commands: `GetSystemInfo`, `ExfilFile`, `InjectProcess`, `DownloadExec`.
Modules	Keylogger DLL injected into `winlogon.exe`; browser credential theft (Chrome/Edge); recon (`ipconfig /all`, `whoami`, WMI).
Evasion	Fileless design, LOLBin execution, minimal disk artefacts.
Hunt Focus	Encoded PowerShell (4688/Sysmon 1, 4104 ScriptBlock with `FromBase64String`); reflective loads into `explorer.exe` / `svchost.exe`; new Run keys & Tasks; RC4/Base64 strings in scripts.
ATT&CK	T1566.001, T1059.001, T1055, T1547.001, T1053.005, T1555.003, T1041, T1070.

ThemeForestRAT

Obfuscated RAT Masquerading as Legitimate Templates

ThemeForestRAT is designed around obfuscation, deception, and stealth, delivered through weaponised Office documents themed to appear legitimate. It achieves execution by hollowing into LOLBins such as mshta.exe or rundll32.exe, ensuring evasion from standard endpoint monitoring. Persistence relies on seemingly benign startup shortcuts, while its functionality includes screen capture, clipboard monitoring, and credential theft from KeePass databases. Its evasion capabilities — including sandbox checks, dynamic API resolution, and string obfuscation — highlight its resilience against both automated analysis and traditional AV/EDR solutions. This RAT reflects Lazarus's focus on hiding in plain sight and using commodity execution flows to blend seamlessly into enterprise environments.

Type: Remote Access Trojan (RAT) with obfuscation/masquerading.

Category	Details
Delivery/Loader	Weaponised Office docs using fake "ThemeForest" templates.
Execution	Process hollowing into mshta.exe / rundll32.exe. Chain: winword.exe ⍰ mshta.exe/rundll32.exe.
Persistence	LNK shortcuts in %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup.
C2	Custom HTTP POST; disguised UA: Mozilla/5.0 ThemeForest; tasking via JSON.
Functionality	In-memory screen capture; clipboard monitoring; KeePass credential theft; file enumeration; SMB-based lateral movement.
Evasion	XOR/Base64 obfuscation; dynamic API resolution; sandbox checks (e.g., vboxmouse.sys, low RAM).
Hunt Focus	Startup .lnk pointing to LOLBins; mshta.exe/rundll32.exe spawned from winword.exe; clipboard/screen capture anomalies; unusual LoadLibrary/GetProcAddress usage; HTTP POSTs with "ThemeForest" UA.
ATT&CK	T1218, T1055, T1547, T1027, T1115, T1005, T1021.002.

RemotePE

Memory-Resident Loader Enabling Lateral Propagation

RemotePE is a flexible in-memory loader and execution framework designed to extend Lazarus's reach across enterprise networks. By abusing DLL side-loading with signed Windows binaries such as msiexec.exe or notepad.exe, it enables covert payload injection into trusted processes like svchost.exe. RemotePE stands out for its support of lateral movement, leveraging stolen credentials with PsExec/SMB to propagate into additional hosts and maintain persistence via disguised service entries. With capabilities for remote shell access, encrypted payload delivery, and staged deployment of other malware families, RemotePE represents a strategic enabler of multi-stage intrusion campaigns. Its design reflects Lazarus's priority on resilience, cross-host persistence, and modular expansion during espionage operations.

Type: In-memory loader/execution framework.

Category	Details
Execution	DLL side-loading via trusted binaries (`msiexec.exe`, `notepad.exe`); payload injection into `svchost.exe`, `spoolsv.exe`.
Payload Delivery	AES-CBC encrypted payloads via HTTPS; staged delivery, including PondRAT.
Persistence	Registry services under `HKLM\SYSTEM\CurrentControlSet\Services\RemotePE`, disguised as printer/driver services.
Lateral Movement	PsExec/SMB using stolen admin creds; payloads written to `\\<target>\C$\Windows\Temp`.
C2	Beacon jitter 30–90s; AES-256-CBC encryption; multi-stage payload deployment.
Capabilities	File transfer, remote shell, cross-host PE injection.
Hunt Focus	New disguised services (Sysmon 6/12/13); DLL side-loading anomalies; PsExec/SMB activity with unexpected admin share writes; `msiexec.exe/notepad.exe` spawning `svchost.exe`; beaconing with jitter.
ATT&CK	T1574.002, T1543.003, T1021.002, T1035, T1055, T1105.

Persistent TTPs Favoured by Lazarus

These techniques endure because they continue to deliver results against modern enterprise defences. Lazarus relies on them not for their novelty, but for their proven reliability in exploiting blind spots that user training, EDR deployments, and conventional controls have yet to close. Their persistence in the Lazarus toolkit highlights a critical reality: even well-known tactics remain highly effective when they align with the constraints and gaps of everyday security operations.

- **Initial Access via Phishing:** Despite years of user awareness training, spear-phishing remains a dependable vector because attackers continuously refine lures with contextual, organisation-specific detail. Awareness programmes reduce but do not eliminate human error, making phishing a statistically reliable entry point.

- **LOLBins for Execution:** Tools like mshta.exe, rundll32.exe, and powershell.exe are natively trusted, signed by Microsoft, and essential for daily operations. Blocking them outright breaks business processes, while allowing them provides attackers a stealthy, low-cost execution path that blends into normal activity.

- **Simple Persistence Mechanisms:** Registry Run keys, Scheduled Tasks, and startup .lnk files remain favoured because they are trivial to deploy, often overlooked in audits, and rarely trigger strong alerts in EDR unless explicitly tuned.

- **Defence Evasion Techniques:** String obfuscation, sandbox checks, and process hollowing require minimal effort for attackers but add significant complexity for defenders. Automated sandboxing and signature-based AV/EDR struggle when binaries adapt dynamically or refuse to execute in virtualised analysis environments.

- **Encrypted HTTPS for C2:** By hiding within ubiquitous encrypted traffic on port 443, attackers exploit defenders' reliance on perimeter firewalls and limited TLS inspection. Most enterprises cannot afford full SSL decryption at scale, leaving adversary traffic concealed in "legitimate" sessions.

- **Compression Prior to Exfiltration:** Packing stolen data into compressed archives not only reduces size but also normalises the traffic pattern. To most monitoring solutions, a ZIP file upload over HTTPS looks indistinguishable from routine business activity like document sharing.

Why this matters: These TTPs endure because they strike the balance attackers want: low effort, low cost, and high reliability against environments where defenders depend too heavily on user training, endpoint agents, and automated detection. Lazarus can rely on them not because they are innovative, but because they are proven and difficult to eliminate without causing business disruption.

Tactics, Techniques and Procedures

The following TTPs have Lazarus's Core Operating Techniques

Tactic	Technique	Technique ID	Details
Initial Access	Spear-phishing via malicious attachments	T1566.001	Emails with weaponized Office documents
Execution	PowerShell / Script-based execution	T1059.001	Fileless and encoded commands
Persistence	Registry Run Keys / Scheduled Tasks	T1547.001	Maintain foothold
Defense Evasion	Obfuscated/ Encrypted payloads	T1027	String and resource padding
Lateral Movement	Remote Process Injection	T1055	RemotePE loading executables
Exfiltration	Exfiltration over C2 channel	T1041	Encrypted HTTPS traffic
C2	Web Protocols (HTTPS, custom)	T1071.001	Encrypted traffic for stealth

Strategic Recommendations Against Enduring TTPs

1. **Move Beyond Awareness and EDR Alone** User training reduces phishing success rates but will never eliminate them. Similarly, EDR can flag some malicious behaviours but cannot reliably stop fileless execution, LOLBin abuse, or in-memory payloads. Organisations need layered defences that assume compromise rather than relying on prevention.

2. **Continuously Hunt for Persistence and LOLBin Abuse** Lazarus favours techniques that blend seamlessly into normal system behaviour — Run keys, disguised services, scheduled tasks, and built-in binaries. Proactive hunting for these anomalies, combined with baselining "normal" execution of PowerShell, mshta.exe, and rundll32.exe, is critical to closing the gaps they exploit.

3. **Shift Detection to the Network and Identity Layers** Encrypted HTTPS traffic, SMB propagation, and stolen credential use can all bypass endpoint controls. Defenders must integrate **network detection, credential misuse monitoring, and segmentation** to reduce attacker dwell time and lateral movement opportunities.

4. **Normalise Data Exfiltration Monitoring** Attackers rely on blending data theft into "normal" traffic. Implementing outbound data size thresholds, unusual compression detection (ZIP/7z), and monitoring of bulk credential access makes exfiltration stand out against the baseline.

Cyber Threat Intelligence

The introduction of PondRAT, ThemeForestRAT, and RemotePE highlights Lazarus's sustained investment in bespoke malware engineered for resilience, stealth, and adaptability. By expanding beyond previously documented toolsets such as DTrack and RATs linked to Operation AppleJeus, Lazarus ensures redundancy across its arsenal, reducing the risk of disruption if one family is exposed or countered. This diversification reflects a deliberate strategy to maintain operational continuity across multiple campaigns.

Motivation

Lazarus's operations are consistently aligned with North Korea's strategic priorities, balancing state-driven espionage with financially motivated cybercrime:

- Espionage: Intelligence gathering on defence contractors, governments, and critical infrastructure provides geopolitical advantage, offering the regime insights into military posture, sanctions enforcement, and diplomatic strategies.
- Financial Gain: Theft of credentials, cryptocurrency, and financial assets funds the regime's economy and offsets the impact of international sanctions. The dual-use design of these malware families — equally capable of espionage and financial theft — maximises Lazarus's operational flexibility.

Target Profile

Current targeting remains heavily focused on financial institutions, defence sectors, and critical infrastructure operators.

- Financial institutions are attractive both for direct theft and for gaining access to broader economic intelligence.
- Defence and government organisations yield sensitive geopolitical and military information, critical to state-level decision-making.
- Critical infrastructure offers strategic leverage: even if immediate disruption is not the objective, persistent access provides North Korea with options for coercion or sabotage during heightened tensions.

Operational Flexibility

The design of these new families demonstrates Lazarus's ability to support both long-term strategic intrusions and short-term opportunistic campaigns:

- Long-term: Implants with stealth persistence (e.g., PondRAT's fileless execution, RemotePE's disguised services) ensure months or years of dwell time for intelligence gathering.
- Short-term: Data exfiltration modules, credential theft, and lateral propagation enable faster monetisation through financial fraud, cryptocurrency theft, or resale of access.

Strategic Implication

The evolution of Lazarus's toolkit underscores that the group is not merely recycling old code but actively innovating to sustain pressure on high-value targets. For defenders, this means Lazarus campaigns cannot be dismissed as "just another phishing + RAT intrusion." Instead, they should be recognised as state-aligned hybrid operations, where the same malware can serve intelligence requirements one day and financial theft objectives the next.

References

Indicators of Compromise (IOCs):

Type	Values
Domains	calendly[.]live, picktime[.]live, oncehub[.]co, go.oncehub[.]co, dpkgrepo[.]com, pypilibrary[.]com, pypistorage[.]com, keondigital[.]com, arcashop[.]org, jdkgradle[.]com, latamics[.]org, lmaxtrd[.]com, paxosfuture[.]com, www[.]plexisco[.]com, ftxstock[.]com, www[.]natefi[.]org, nansenpro[.]org, aes-secure[.]net, azureglobalaccelerator[.]com, azuredeploypackages[.]net
IP Addresses	144.172.74[.]120, 192.52.166[.]253
File Paths	%TEMP%\tmpntl.dat, C:\Windows\Temp\TMP01.dat, /var/crash/cups, /private/etc/imap, /private/etc/krb5d.conf, /etc/apdl.cf, %SystemRoot%\system32\apdl.cf, /tmp/xweb_log.md, %LocalAppData%\IconCache.log, /private/etc/pdpaste, /private/etc/xmem, /private/etc/tls3, %LocalAppData%\Microsoft\Software\Cache, C:\Windows\System32\cmui.exe
Filenames	netraid.inf, perfh011.dat, hsu.dat, pfu.dat, fpc.dat, fp.exe, tsvipsrv.dll, wlbsctrl.dll, adepfx.exe, hd.exe, msnprt.exe

Public Intelligence:

- https://thehackernews.com/2025/09/lazarus-group-expands-malware-arsenal.html
- https://socprime.com/blog/detect-lazarus-attacks-using-three-new-rats/
- https://cristianthous.com/lazarus-defi-attack
- https://blog.fox-it.com/2025/09/01/three-lazarus-rats-coming-for-your-cheese/

Stay Ahead

Access Emerging Threat Reports

Scan to Subscribe