

Not Every Fox is Silver: Inside an AtlasRAT loader chain

A asec.ahnlab.com/en/94704

ATCP

July 27, 2026



Summary

AtlasRAT is a Windows-based remote access malware. This report analyzes a four-stage in-memory loader chain—which begins with a Delphi executable that is disguised as AGE Flash Player—and its final RAT functionality. The final payload performs TLS-based ChaCha20-encrypted C2 communication, executes modular plugins, performs offline keylogging, and injects DLLs into WeChat processes.

Group Characteristics

Public analysis remains limited, with only reports from Hexastrike and Proofpoint confirmed. A 180-day retrohunt of the VirusTotal corpus identified 146 unique samples, 6 versioned PDB builds, 2 development environment usernames, and 27 heuristic lineages. It is noted that such scale and diversity are inconsistent with management by a single operator, raising the possibility that the malware was commercially developed or distributed privately. However, the link to Silver Fox has only been suggested based on circumstantial evidence, and there is insufficient evidence to conclusively determine that they are the same operator.

Key Malware and Tools

Stage 1 of AtlasRAT is a Delphi application named FlashPlay.Exe, which acts as an in-memory PE loader. Stage 2 reconstructs encrypted fragments using Base64, XOR, and AES-256-CBC to create a 1,374-byte x86 downloader shellcode. Subsequently, the loader delivered from the C2 server is manually mapped and then calls ServiceRun, leading to the final DLL. The final payload is MainDll.Dll, which contains a self-signed certificate impersonating CN=update.Microsoft.Com for TLS client initialization. Command capabilities include executing plugins, downloading and executing files, checking for process presence, starting and stopping keylogging, termination actions, and remote LoadLibraryW injection targeting WeChat.Exe. The persistence plugin, persistence86.Dll, provides capabilities to tamper with the BITS database, achieve logon persistence via NTUSER.MAN, and bypass UAC using CMSTPLUA and registry hijacking.

Mitigation Strategies

The report did not directly propose specific defensive measures. However, detection and hunting are possible using the observed IOCs, C2 infrastructure, certificate fingerprints, and file hashes. In particular, relevant IP addresses distributed across Hong Kong and South Korea, By@V< configuration markers, variations in the BFuck\0\0\0 and SFuck\0\0\0 handshake strings, and paths related to persistence86.Dll and its PDB paths.

Conclusion

AtlasRAT is characterized not as an isolated, single payload, but as a modular malware framework with a repeatable, builder-based production system. Parallel x86 and x64 branches, iterative recompilation, a separate persistence module, and the phased introduction of embedded certificates have been confirmed. Current evidence suggests that understanding the development and distribution structure is more important than definitive attribution to a specific actor.

IOC

File IOC

- FlashPlay.Exe.
- MainDll.Dll.
- Persistence86.Dll.

- C:\Users\xxx857857\Desktop\atlasPro验证版
2026.6.2\Release\Plugin\x86\MainDll.PDB.
- C:\Users\xxx857857\Desktop\atlasPro Trial Version
2026.6.2\Release\Extend\x86\persistence86.PDB.

Network IOCs

- 150.158.50.175:443.
- 116.204.169.70.
- Bifa668.Com.
- 23.226.57.50.
- 27.124.20.172.
- 38.46.13.82.
- 82.23.246.175.
- 192.163.162.30.
- 206.119.191.242.

Others IOCs

- By@V<.
- BFuck\0\0\0.
- SFuck\0\0\0.
- CN=update.Microsoft.Com.
- Global\NtuserManPayload.
- C:\Users\Public\Documents\Wxfun.Dll.
- C:\Users\Public\Documents\offline.Ini.
- C:\Users\Public\Documents\MODIf.Html.

Threat Hunting Rules

- Check for 32-bit DLLs that contain a ServiceRun export.
- Look for samples where the By@V< marker appears alongside the strings BFuck\0\0\0 or SFuck\0\0\0.
- Look for traces of TLS client initialization containing a self-signed certificate with CN=update.Microsoft.Com.
- Investigate artifacts related to offline.Ini, MODIf.Html, Wxfun.DLL, and NTUSER.MAN.
- Check for traces of remote thread creation via LoadLibraryW targeting WeChat.Exe.

MITRE ATT&CK

- Initial Access: Social engineering-based distribution.
- Execution: In-memory PE loading, manual mapping, shellcode execution.
- Persistence: BITS, NTUSER.MAN, Run key, WPTask.
- Privilege Escalation: Bypassing UAC using CMSTPLUA, fodhelper.Exe, and eventvwr.Exe.
- Defense Evasion: Disguised as Flash Player, process spoofing, use of self-signed certificates.
- Credential Access: Offline keylogging.
- Discovery: System information, security product identification, process and window detection.
- Command and Control: TLS, ChaCha20, and encrypted C2 communications.
- Lateral Movement: Remote DLL injection and process injection.
- Impact: Termination behavior using ExitWindowsEx.

SHA2

03d93b56ac4219a8ac8a55fd4ba777618b5682cc84bec0efe8ea78e497dd3b3d
04bef2153417efeb408d8e027bd91bb6db5b957c43ceb7429a15cb76ef436af3
06abfcb1b253bb6722d01181dc4bf90f25d012ea585974e49a7bf839a20f0d24
06b06be9dfbc70557278ebd9622c6994b30be2642793d2fafec228240459fbb2
0941884daf94d347e4bdd793b2ecb8a0692ae8054ed7d62e0663a982af113a0e

Additional IOCs are available on AhnLab TIP.

FQDN

bifa668[.]com

IP

101[.]43[.]53[.]116

108[.]187[.]7[.]84

116[.]204[.]169[.]70

143[.]92[.]32[.]49

143[.]92[.]32[.]65

Additional IOCs are available on AhnLab TIP.



AhnLab TIP

Stay Ahead of Rapidly Evolving Threats Make the Best-Informed Decisions

Get Started with AhnLab's State-of-the-Art Threat Intelligence

atip.ahnlab.com