Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

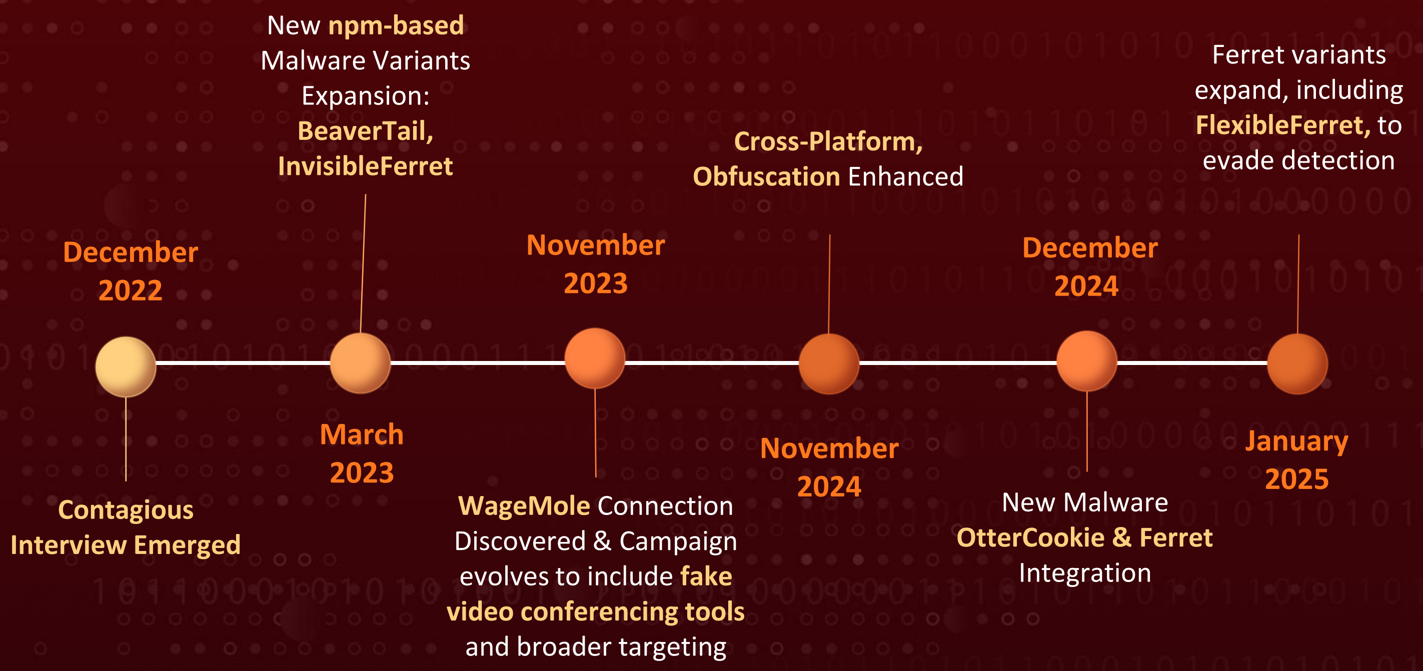
“Contagious Interview” Targets macOS with FlexibleFerret Malware

Date of Publication	Admiralty Code	TA Number
February 6, 2025	A1	TA2025031

Summary

Active Since: January 2025
Targeted Countries: Worldwide
Malware: FlexibleFerret, FRIENDLYFERRET, FROSTYFERRET_UI, and MULTI_FROSTYFERRET_CMDCODES
Targeted Industries: Cryptocurrency, Finance, Software Development
Affected Platform: macOS
Campaign Name: Contagious Interview (aka CL-STA-0240)
Attack: The macOS Ferret malware, linked to North Korean threat actors, targets job seekers and developers through the "Contagious Interview" campaign using fake software installations. A new variant, FlexibleFerret, evades Apple’s XProtect and gains persistence by masquerading as legitimate system processes. Attackers are expanding their tactics, using GitHub to distribute malware, emphasizing the need for enhanced security vigilance.

Campaign Timeline



December 2022
Contagious Interview Emerged

March 2023
New **npm-based** Malware Variants Expansion: **BeaverTail, InvisibleFerret**

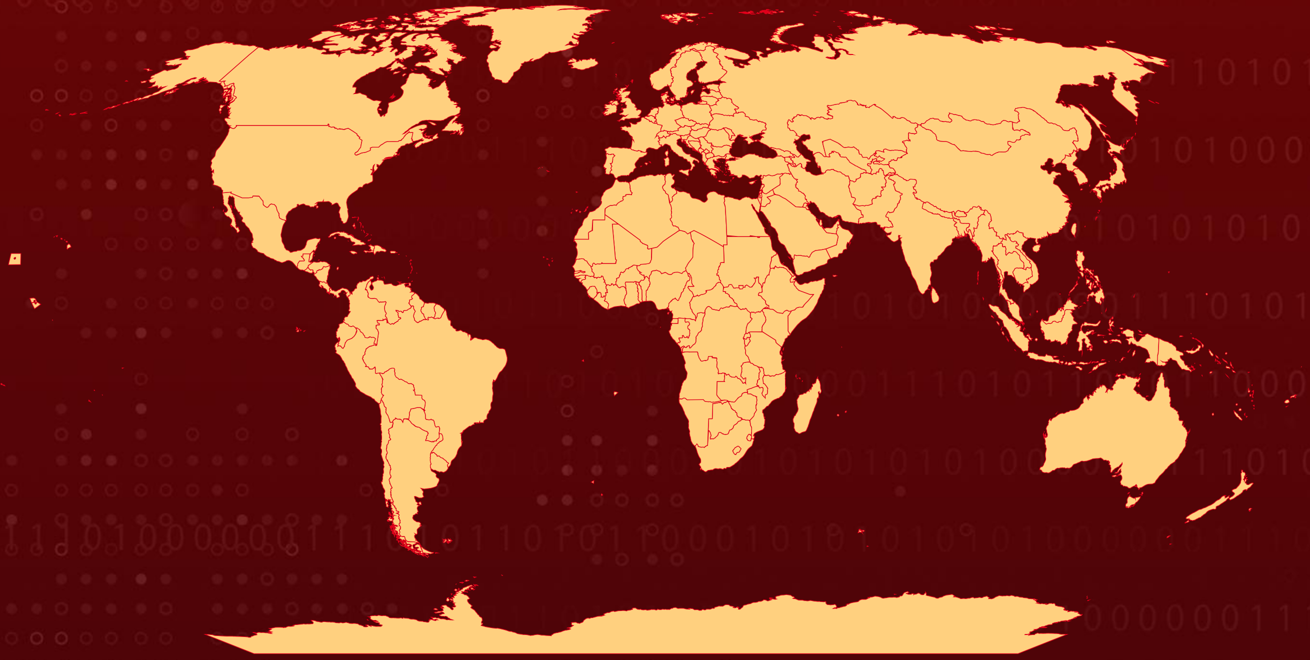
November 2023
WageMole Connection Discovered & Campaign evolves to include **fake video conferencing tools** and broader targeting

November 2024
Cross-Platform, Obfuscation Enhanced

December 2024
New Malware **OtterCookie & Ferret** Integration

January 2025
Ferret variants expand, including **FlexibleFerret,** to evade detection

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

A new wave of macOS malware, attributed to North Korean threat actors, is actively targeting users through the "Contagious Interview" campaign. This attack exploits job seekers and developers, tricking them into installing malware disguised as legitimate applications. Apple recently updated its XProtect malware detection tool to block several known variants, including FRIENDLYFERRET, FROSTYFERRET_UI, and MULTI_FROSTYFERRET_CMDCODES. These threats use deceptive persistence techniques and exfiltrate sensitive data via Dropbox.

#2

In addition to previously known FERRET malware variants, researchers have identified a new strain called FlexibleFerret. Distributed via an Apple Installer package ("versus.pkg"), this malware includes multiple components, such as InstallerAlert.app and a malicious Zoom binary. It employs persistence mechanisms by mimicking legitimate system processes and logging user activity. Additionally, it was signed with a revoked Apple Developer certificate, demonstrating attackers' adaptive tactics to bypass security measures.

#3

FlexibleFerret leverages social engineering techniques, deceiving victims with fake installation failure messages while executing malicious code in the background. The malware establishes persistence by modifying the User's Library LaunchAgents folder, masquerading as a legitimate system service. It also communicates with a fraudulent Zoom domain (zoom.callservice[.]us), potentially deploying additional payloads that facilitate data theft and remote access. These tactics align with previously documented North Korean cyber-espionage campaigns.

#4

Beyond targeting job seekers, attackers have expanded their reach to GitHub developers, creating fake issues on repositories to spread FERRET malware droppers. This shift highlights a broader strategy to infiltrate the tech industry. Security teams should remain vigilant, monitoring for suspicious installer scripts, unauthorized LaunchAgent modifications, and unexpected network activity.

Recommendations

Keep Security Tools Updated: Ensure XProtect and other endpoint security solutions are updated to detect and block known FERRET malware variants.

Verify Software Sources: Only download applications from official sources; avoid installing software from unsolicited links or job-related communications.

Monitor for Persistence Mechanisms: Regularly check ~/Library/LaunchAgents/ for suspicious entries like com.zoom.plist and unknown executables in /var/tmp/.

Restrict Untrusted Developer Certificates: Block applications signed with revoked or unverified Apple Developer signatures to prevent execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0004 Privilege Escalation	TA0001 Initial Access	TA0002 Execution
TA0040 Impact	TA0008 Lateral Movement	TA0005 Defense Evasion	TA0010 Exfiltration
TA0011 Command and Control	T1566 Phishing	T1586 Compromise Accounts	T1204 User Execution
T1583 Acquire Infrastructure	T1583.001 Domains	T1566.002 Spearphishing Link	T1059 Command and Scripting Interpreter
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer	T1189 Drive-by Compromise
T1059.004 Unix Shell	T1567.002 Exfiltration to Cloud Storage	T1567 Exfiltration Over Web Service	T1036 Masquerading
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1068 Exploitation for Privilege Escalation	T1202 Indirect Command Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	203f7cfbf22b30408591e6148f5978350676268b, a25dff88aeeaaf9f956446151a9d786495e2c546, aa172bdccb8c14f53c059c8433c539049b6c2cdd, 7da429f6d2cdd8a63b3930074797b990c02dc108, 7e07765bf8ee2d0b2233039623016d6dfb610a6d, 828a323b92b24caa5f5e3eff438db4556d15f215, 831cdcde47b4edbe27524085a6706fbfb9526cef, 8667078a88dae5471f50473a332f6c80b583d3de, dba1454fbea1dd917712fbece9d6725244119f83,

TYPE	VALUE
SHA1	e876ba6e23e09206f358dbd3a3642a7fd311bb22, 17e3906f6c4c97b6f5d10e0e0e7f2a2e2c97ca54, 2e51218985afcaa18eadc5775e6b374c78e2d85f, 7e07765bf8ee2d0b2233039623016d6dfb610a6d, de3f83af6897a124d1e85a65818a80570b33c47c, 388ac48764927fa353328104d5a32ad825af51ce, 1a28013e4343fddf13e5c721f91970e942073b88, 3e16c6489bac4ac2d76c555eb1c263cd7e92c9a5, 76e3cb7be778f22d207623ce1907c1659f2c8215, b0caf49884d68f72d2a62aa32d5edf0e79fd9de1, bd73a1c03c24a8cdd744d8a513ae8d2ddfa2de5f, ccac0f0ba463c414b26ba67b5a3ddaabdef6d371, d8245cdf6f51216f29a71f25e70de827186bdf71, b071fbd9c42ff660e3f240e1921533e40f0067eb, ee7a557347a10f74696dc19512ccc5fcfca77bc5
Domain	Zoom[.]callservice[.]us

References

https://www.sentinelone.com/blog/macos-flexibleferret-further-variants-of-dprk-malware-family-unearthed/

https://www.zscaler.com/blogs/security-research/pyongyang-your-payroll-rise-north-korean-remote-workers-west

https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

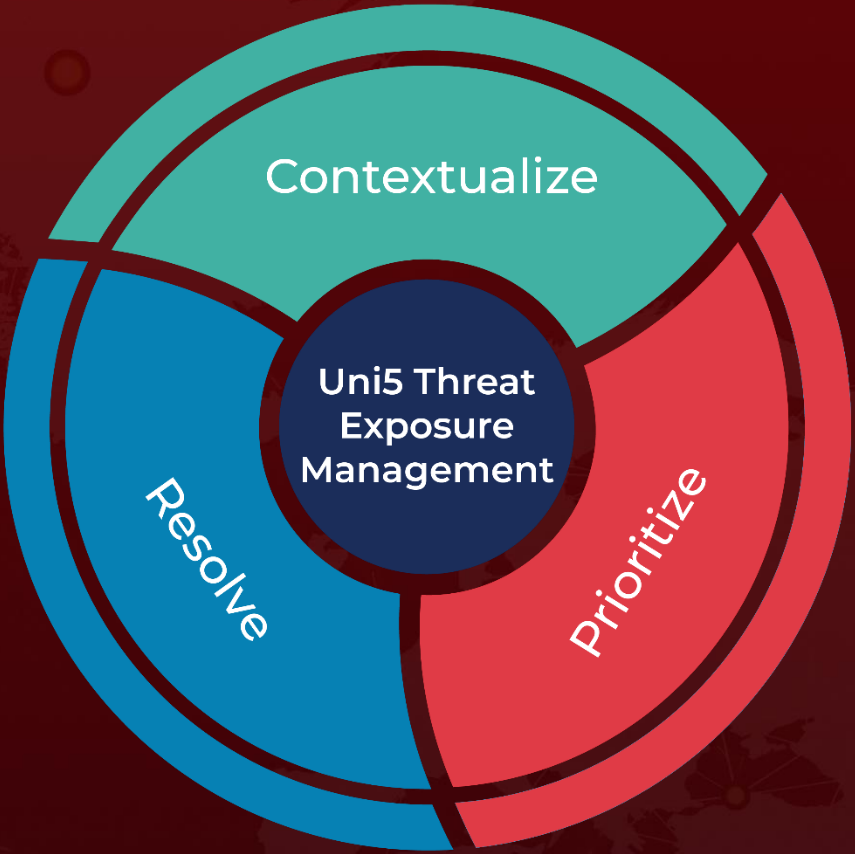
https://hivepro.com/threat-advisory/north-korean-hackers-go-after-remote-job-openings/

https://hivepro.com/threat-advisory/unmasking-ottercookie-malware-in-the-contagious-interview-campaign/

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

February 6, 2025 • 12:30 AM

More at www.hivepro.com