Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

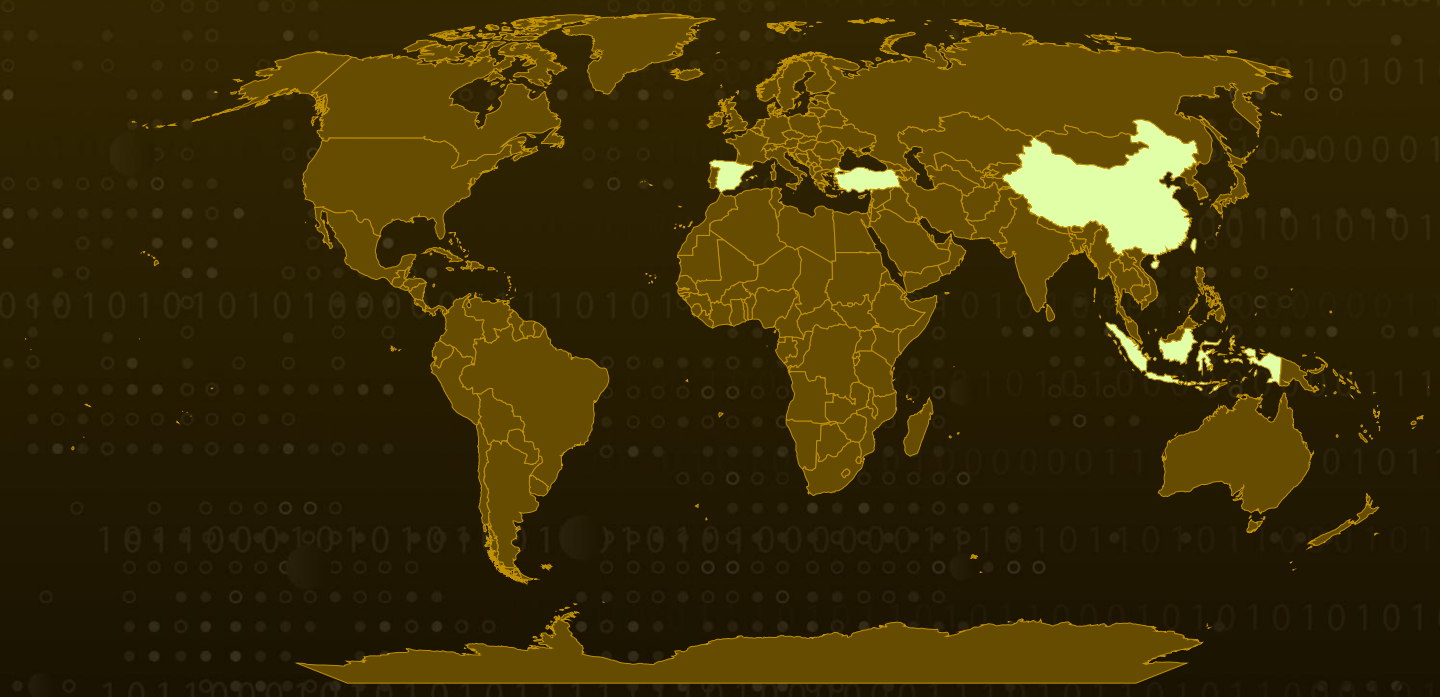
Snake Keylogger Strikes Again: A Stealthy Threat Targeting Millions

Date of Publication	Admiralty Code	TA Number
February 20, 2025	A1	TA2025051

Summary

Attack Discovered: 2025
Targeted Country: China, Turkey, Indonesia, Taiwan, and Spain
Affected Platform: Microsoft Windows
Malware: Snake Keylogger (aka 404 Keylogger)
Attack: A newly evolved and highly sophisticated variant of Snake Keylogger has surfaced, actively targeting Windows users across China, Turkey, Indonesia, Taiwan, and Spain. This persistent malware has already triggered over 280 million blocked infection attempts, underscoring its widespread impact. Designed for stealthy data theft, Snake Keylogger infiltrates popular web browsers such as Chrome, Edge, and Firefox, silently logging keystrokes, capturing credentials, and monitoring clipboard activity. By harvesting sensitive information, it enables cybercriminals to gain unauthorized access to accounts, financial data, and other personal details, making it a significant threat to users worldwide.

Attack Regions



Attack Details

#1 A new and highly sophisticated variant of Snake Keylogger (aka 404 Keylogger), has been identified, responsible for over 280 million blocked infection attempts globally. Snake Keylogger was first discovered in November 2020. The malware primarily targets Windows users and spreading through phishing emails. Once executed, it silently logs keystrokes, captures credentials, and monitors clipboard activity, stealing sensitive information from browsers like Chrome, Edge, and Firefox. The stolen data is then exfiltrated using SMTP and Telegram bots, giving attackers remote access to compromised credentials and other personal details.

#2 This modular malware is written in .NET and remains highly adaptable. Beyond keylogging, it can take screenshots, extract data from clipboards, and persist on infected machines. Most infections occur when a victim opens a malicious Office document or PDF, enabling macros or exploiting vulnerabilities in outdated software.

#3 This new variant of Snake Keylogger employs AutoIt, a scripting language commonly used for Windows automation, to obfuscate its payload and evade detection. The malware is compiled into an AutoIt binary, embedding its malicious code within a script, making static analysis more challenging.

#4 Upon execution, Snake Keylogger copies itself to the system's folder under the name ageless.exe, setting its attributes to hidden. To ensure persistence, it drops a secondary file, ageless.vbs, into the %Startup% folder. This script executes ageless.exe upon system startup, allowing the malware to persist even after a reboot.

#5 Once active, Snake Keylogger injects its payload into a legitimate .NET process using process hollowing, a technique that replaces the memory of a legitimate process with malicious code. This method conceals the malware's presence, making it significantly harder for traditional security solutions to detect or remove the infection.

#6 Beyond credential theft, Snake Keylogger gathers additional information about victims, including their geolocation. The stolen data is then securely transmitted via HTTP Post requests to its command-and-control server. With its ability to operate undetected, steal sensitive data, and communicate with attackers through multiple channels, Snake Keylogger remains a significant cybersecurity threat.

Recommendations

- **Stay Alert with Unfamiliar Emails:** Be wary of emails from unknown senders, especially if they contain attachments or links. Before clicking or downloading anything, take a moment to verify the sender's legitimacy to avoid potential threats.
- **Keep Macros Disabled in Office Documents:** Since Snake Keylogger spreads through malicious Office files, it's best to keep macros disabled by default. Only enable them if absolutely necessary and from trusted sources.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.
- **Monitor and Restrict Network Traffic:** Continuously analyze outbound connections to identify potential communication with malicious command-and-control (C2) servers. Implement DNS filtering and block access to known harmful domains to prevent unauthorized data exfiltration.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement
TA0009 Collection	**TA0010** Exfiltration	**TA0011** Command and Control	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1091** Replication Through Removable Media	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell
T1106 Native API	**T1057** Process Discovery	**T1018** Remote System Discovery	**T1497** Virtualization/Sandbox Evasion

T1548 Abuse Elevation Control Mechanism	T1548.004 Elevated Execution with Prompt	T1211 Exploitation for Defense Evasion	T1055 Process Injection
T1055.012 Process Hollowing	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1056 Input Capture
T1056.001 Keylogging	T1027 Obfuscated Files or Information	T1614 System Location Discovery	T1071 Application Layer Protocol
T1566 Phishing			

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxp[:]//51[.]38[.]247[.]67[:]8081/_send_php?L
MD5	f8410bcd14256d6d355d7076a78c074f, 77f8db41b320c0ba463c1b9b259cfd1b
SHA256	7e9b9833268dae6e33c83b582ec7fb353f0dc6514f869e3228f0effa161da00f

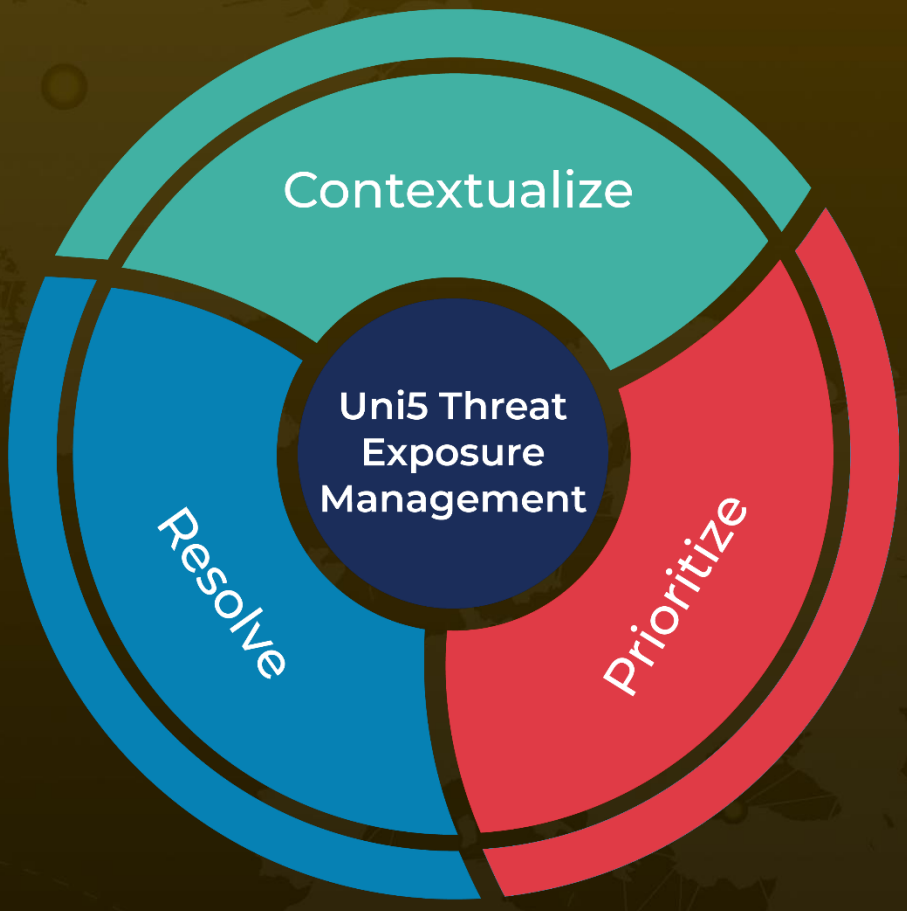
References

https://www.fortinet.com/blog/threat-research/fortisandbox-detects-evolving-snake-keylogger-variant

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 20, 2025 • 3:45 AM

More at www.hivepro.com