Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

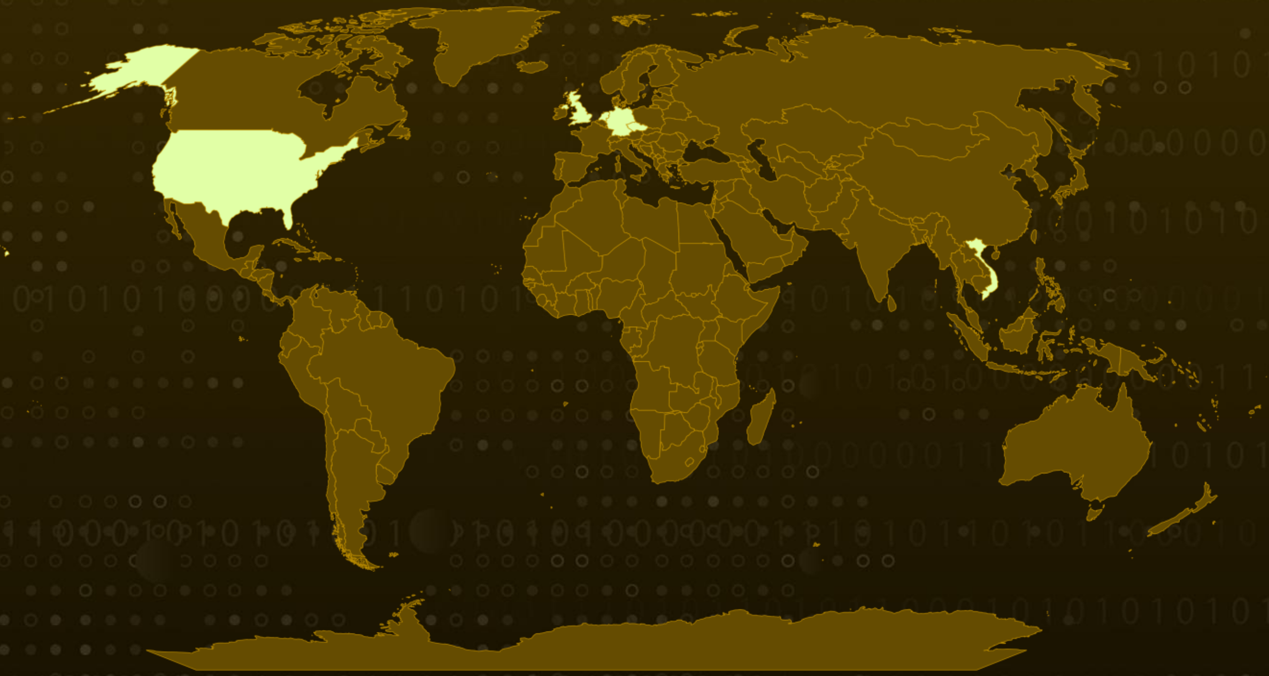
Braodo Stealer: The Rising Python-Based Cyber Menace

Date of Publication	Admiralty Code	TA Number
July 24, 2024	A1	TA2024283

Summary

Attack Discovered: Early 2024
Attack Region: US, Czechia, Germany, Netherlands, Singapore, Vietnam, United Kingdom
Malware: Braodo Stealer
Attack: Braodo Stealer is a Python-based malware that has been targeting users in Vietnam since early 2024, with additional victims in the US, Czechia, Germany, the Netherlands, Singapore, and the UK. It spreads through phishing and spear-phishing emails, utilizing GitHub and a Singapore-based VPS server to host and distribute its malicious code. The malware exfiltrates internet browser data via Telegram bots, stealing credentials from financial platforms and causing identity theft and financial losses.

Attack Regions



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

Attack Details

#1 Braodo Stealer is a Python-based malware that has been targeting users in Vietnam since early 2024. It spreads through phishing and spear-phishing emails, using GitHub and a Singapore-based VPS server to host and distribute its malicious code. The malware steals internet browser data via Telegram bots, capturing credentials from financial platforms, GitHub accounts, and various websites.

#2 Initially distributed as a zip file, Braodo Stealer self-deobfuscates and retrieves a second-stage payload from GitHub. Multiple variants of the downloader and Python payloads are hosted on an open directory HTTP server at a specified IP address. Two servers, one in Singapore and one in France host services for this stealer operation, with the Singapore IP hosting non-functional or possibly phishing pages mimicking Vietnamese government websites.

#3 The malware's batch script generates multiple instances of PowerShell and cmd.exe, eventually executing a 'sim.py' Python script. The batch script is padded with the bytes “FF FE 0D 0A,” causing it to be interpreted as gibberish characters. Once these extraneous bytes are stripped away, the actual script is exposed, revealing a PowerShell script that plays a vital role in the malware's operation.

#4 This PowerShell script downloads two files from a GitHub repository: update1.bat and 1.zip. Update1.bat maintains persistence by adding a batch script to the Windows Startup folder, while 1.zip contains the main source code of Braodo Stealer. These files are saved in the Windows Startup folder, unarchived, and executed from there, allowing the malware to establish persistence, retrieve its source code, and execute its core functionality. The main script of this information stealer is located at "Lib/sim.py".

#5 Braodo Stealer collects information about the victim using ipinfo.io and targets specific browser paths. It dumps all running processes into a file called "window.txt" and initiates six threads to run the browser stealer function. This function targets browsers like Chrome, Firefox, Edge, Opera, Brave, and Chromium, gathering data such as cookies and passwords. The collected data is stored in an exfiltration directory, compressed into an archive, and sent to a Telegram channel. Braodo Stealer poses significant risks to sensitive information. Regular security updates and vigilance against phishing attempts are crucial defenses against this evolving threat.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1566** Phishing	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell
T1059.006 Python	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1555** Credentials from Password Stores
T1555.003 Credentials from Web Browsers	**T1606** Forge Web Credentials	**T1606.001** Web Cookies	**T1057** Process Discovery
T1083 File and Directory Discovery	**T1005** Data from Local System	**T1041** Exfiltration Over C2 Channel	**T1071** Application Layer Protocol

T1071.001 Web Protocols	T1027 Obfuscated Files or Information

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e246a68e4ff8098ffd08da24c27726a11daa84f63b27bf79b93b374d9757d032, f4f843853c7a08c08181516ae2a910dfeb712e32b4ab10df23149d9f57ab581e, 6ec111b78a9788fcbca92dcc48b0d5f78d4df6a5f8d0ce96390851e832eace0d, 4092ff03e7a69efd728a0dd2a181fdeef99df6ebdf0e6f39140718e805efe655, 4c3b91cd25650a7e1ee80164fd0598cdbf64e75ddf4ce08141aea42ee56cb134, b84dc0ea50ce08686d543cc08b87792026c233afee9b029768e0648cf5b06bd8, 998bb0d396dbf2ed6a412737f040228b00782267d473ceae502788451e076825, 76c0693dce55c0835ad73102541d4244b3b7ee91649890faca85290b4f9ab005, f735c170cee9e89c0318f266fc7469fde40d19eca406fbfa974b872a9b367a19, bde85da1206fa48ac5a66818023a495bb03418a32a2936afef3cdb332a2bce17, f65c51f438241475dd8856ffa578610cfabab4aa8b52a09febf5ae061a5f42f7, c15dee4fe227d6311f612f3aacc86080e2f8c450ad3b78d1271603891ec61a52, ea2312ad6f7ace12c5e9f54becead82927d23e6707c27a6db4c9fd82ebf62718
IPv4	103[.]54[.]153[.]116, 45[.]147[.]97[.]170
URLs	github[.]com/s123s1/s/, github[.]com/vtbg1/s/, github[.]com/zzhshsss/s/
Telegram Bot	bot7120180818:AAEBAEYZZ44zM8wICJ-bJTLHKbnhDEYwVrk, bot7120260932:AAE2zApf_cqTt57pmwxJUodvBar2l7x7fbA, bot6878187208:AAFjqOqPfUbezs5GaBB-x99QhDkXaXsWgpg, bot7094444204:AAFoaWZVfCF4ZyHvMpuAY0U15D3JlzxhNYg, bot7147346317:AAHcazkPzwexz-_QwcdWQr96JJMKueLC6MQ, bot7024022476:AAFClxu17D2YaSM8zOcRBkgmvgZ2horf6LU

References

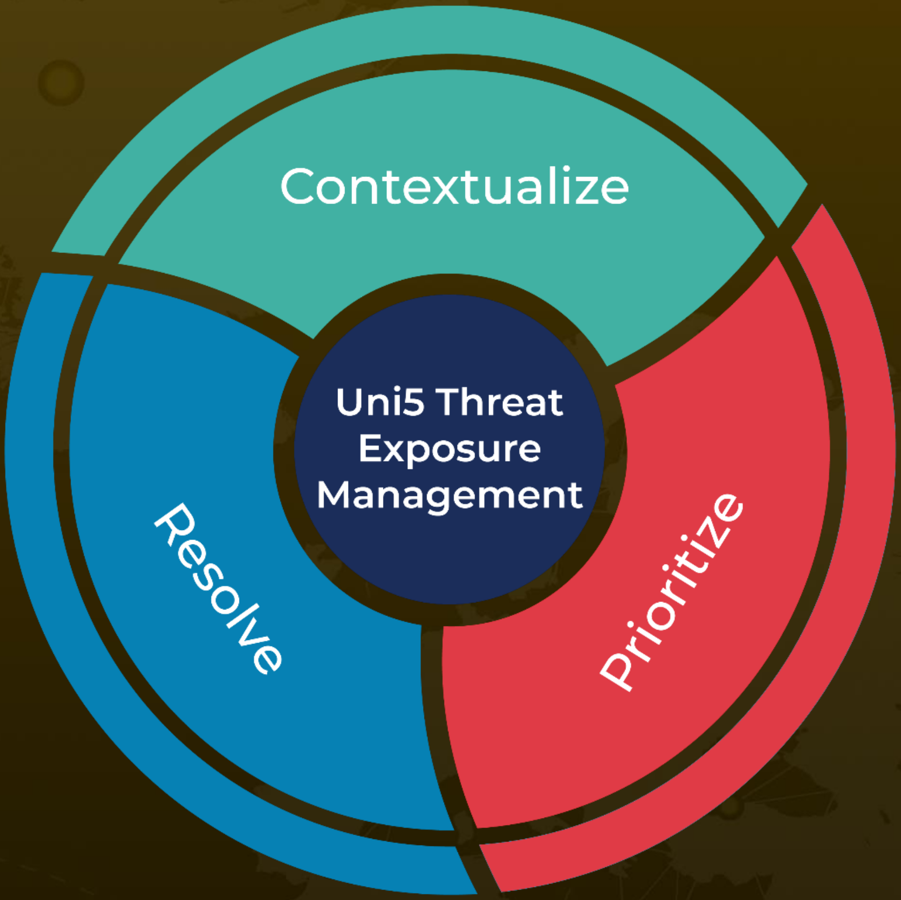
https://www.cyfirma.com/research/braodo-info-stealer-targeting-vietnam-and-abroad/

https://labs.k7computing.com/index.php/echoes-of-braodo-tales-from-the-cyber-underworld/

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

July 24, 2024 • 6:30 AM

More at www.hivepro.com