Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

BbyStealer's Tactic for Targeting VPN Users

Date of Publication	Admiralty Code	TA Number
October 18, 2023	A1	TA2023421

Summary

First Seen: 2022
Malware: BbyStealer
Attack Region: Worldwide
Targeted Applications: TotalVPN, WolferVPN, CyberFortressVPN, FortresVPN, FlazerVPN, FlazerVPN-v18.16.0-x64, ProxtyVPN-v18.16.0-x64, iTropperVPN
Attack: The BbyStealer malware resurfaces and orchestrates a sophisticated information-theft campaign, utilizing numerous phishing domains to target users of VPN applications engaged in downloading activities, with a focus on collecting sensitive information.

Attack Regions

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

Attack Details

#1

The BbyStealer represents a sophisticated information-theft malware campaign that employs numerous phishing domains to target individuals engaged in downloading activities. Initially identified in early 2022, this malware has resurfaced with a distinct developer, with the aim of stealthily gathering sensitive information from various web browsers and cryptocurrency wallet extensions. The pilfered data is then discreetly transmitted to a remote server.

#2

Threat actors execute their tactics through phishing websites, often incorporating brand impersonation in campaigns using domains like "totalvpn[.]tech." These campaigns disseminate a RAR archive file, concealing within it the executable file known as BbyStealer. It's noteworthy that BbyStealer was previously linked to the "Try my game" Discord scam.

#3

Upon execution, the BbyStealer malware duplicates itself, placing the copy in the startup folder with the inconspicuous name "Updater.exe" to ensure persistence. Subsequently, it terminates web browser processes and proceeds to extract valuable information such as login credentials, personal particulars, and financial data from designated browser installation locations. This is achieved by creating duplicates of the user data folder, appending the ".bby" extension.

#4

Furthermore, the malware conducts a scan to identify specific browser extensions associated with cryptocurrency wallets. In an additional layer of sophistication, the malware engages in a clipper operation, actively monitoring the clipboard activity of the victim's system. In the final stage, the gathered sensitive data is processed, establishing a connection with a Command and Control (C&C) server for discreet transmission of the compromised information.

Recommendations

Secure Configuration Guidelines: Enforce secure configuration guidelines for web browsers and extensions, ensuring that unnecessary features or permissions are disabled to minimize the attack surface and mitigate potential exploitation by BbyStealer.

Network Traffic Analysis: Deploy network traffic analysis tools to monitor and analyze patterns of communication between endpoints and potential command and control servers associated with BbyStealer. This can aid in early detection.

Behavioral Anomaly Detection: Deploy advanced behavioral anomaly detection systems that can identify deviations from normal user and system behavior, flagging activities such as frequent and unusual execution of reconnaissance commands.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1003 OS Credential Dumping	T1005 Data from Local System	T1012 Query Registry	T1047 Windows Management Instrumentation
T1057 Process Discovery	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1071 Application Layer Protocol
T1115 Clipboard Data	T1547.001 Registry Run Keys / Startup Folder	T1566 Phishing	T1059 Command and Scripting Interpreter

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	totalvpn[.]tech, wolfervpn[.]com, vpncyberfortress[.]com, vpnfortres[.]online, itroppervpn[.]online,

TYPE	VALUE
Domains	rufflesrefined[.]com, taffylollipop[.]com
URLs	hxxps://totalvpn[.]tech/download/TotalVPN[.]rar, hxxps://wolf-ervpn[.]com/download/WolferVPN[.]rar, hxxps://vpnfortres[.]online/download/FortresVPN[.]rar, hxxps://itroppervpn[.]online/download/iTropperVPN[.]rar, hxxps://cdn.discordapp[.]com/attachments/1160770898966622230/1161087215963738174/CyberFortressVPN.rar?ex=653705bc&is=652490bc&hm=b9417ffe67ed173e46c662f30bd7f0d642770438b07040b99d4bd217c44c7942&
MD5	2cf6efb8104b5d4606fb1698ae97e4f5, 3cf9c1d65d59b63d479ec26e9fd98b57, f1da9126a48197897644a62135c0df46, 352ba438532e9a7a9941875f3824c1cd, 71e0b2a2372398776297cee13c8efa55, bbc3364d8040296b910cf61280cd6ad7, 0d2071be3f76d4b25f19b54d56ff6cb7, 1f8eda53714be873e2280d494c9eacbf, bcd419817ebb4d2ec7e21fbdaf61dd3b, 4ee5a9ffd40f8c0970e53e832bfb9acd
SHA1	effb88250fcb89bbab77f46c1022f3c9c0aad37e, eab9cf1e969b5d9a3fda7714c6ae2796aaf44fd0, 8fcbf76cccb573d3007032a2148da458f81ffbb1, d72c3e3b1fdaa271629676d7d0215cc396a106c4, c9fd398ed07a2daeeaf526ab094634adbd851934, bdd5dec13109f9cfe992ce325f746c0d3bad6c72, 8a7fab41932aa2dbe8da17697926d69b15dc6c63, aae16faf79be993b27791fb7a6a3663320067876, 61fd361edcfaecb87dbf3711ecb1dd448d6a2ab2, 0ee35e1992b93dbeb7adcd2ccdfcafcb3a1dfdae
SHA256	55a6a784d4acb7e9761a99fb38eb441519cdcd2943bfdf1a1558fe8513690c97, e97b03c98056d7c88bad83b7422767d51ac75fe959e7d1582cc645d6a2bae84b, 7a27aca062c7b4b180190452afbc6ba4026a13ca8c9503372459a5b214b68ff9, 50ab07bd922546f90d2d62565a3618ba7251459c8aaf007945feb3e7c9f29458, f46017c2c5c98d89a1d35510ed8eeae263a3f8f60092df2bb13db6918d691a32, 833ba04dfe7c93f397117690bf656bdf1cf2768b216f40f525bb0c7527897b9a,

TYPE	VALUE
SHA256	8b93ed446668642a0d3b8dc45b794d76ce71ebd7552de8437975da2b228df9c7, a26a2a95b6ad1449bf4fe5814533b408cdcc67ad5c234c900b6e0b31300018b0, ae4ea904741b95f044edf0e16ce244dc5a4015050dd9ecf23f2f831435e1ccbc, 058caf0c1750391e8a625ee3310c804e1a0034ce890aef4773ef6cfff3ccced5

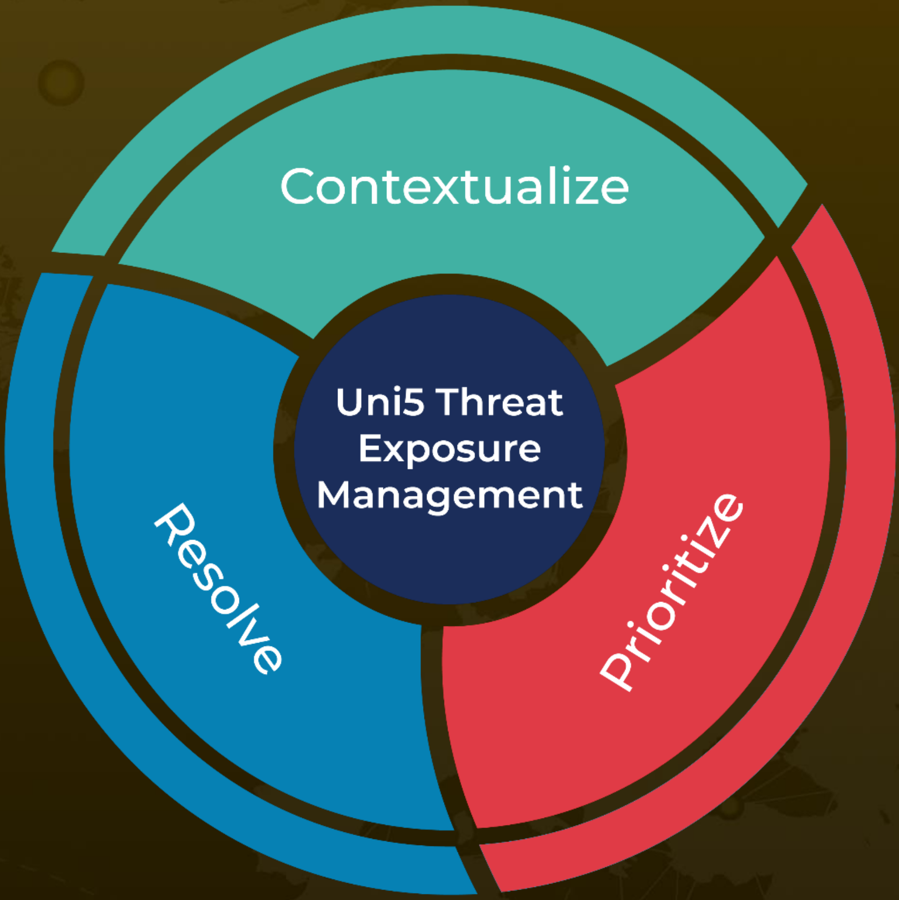
References

https://cyble.com/blog/bbystealer-malware-resurfaces-sets-sights-on-vpn-users/

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

October 18, 2023 • 5:30 AM

More at www.hivepro.com