Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

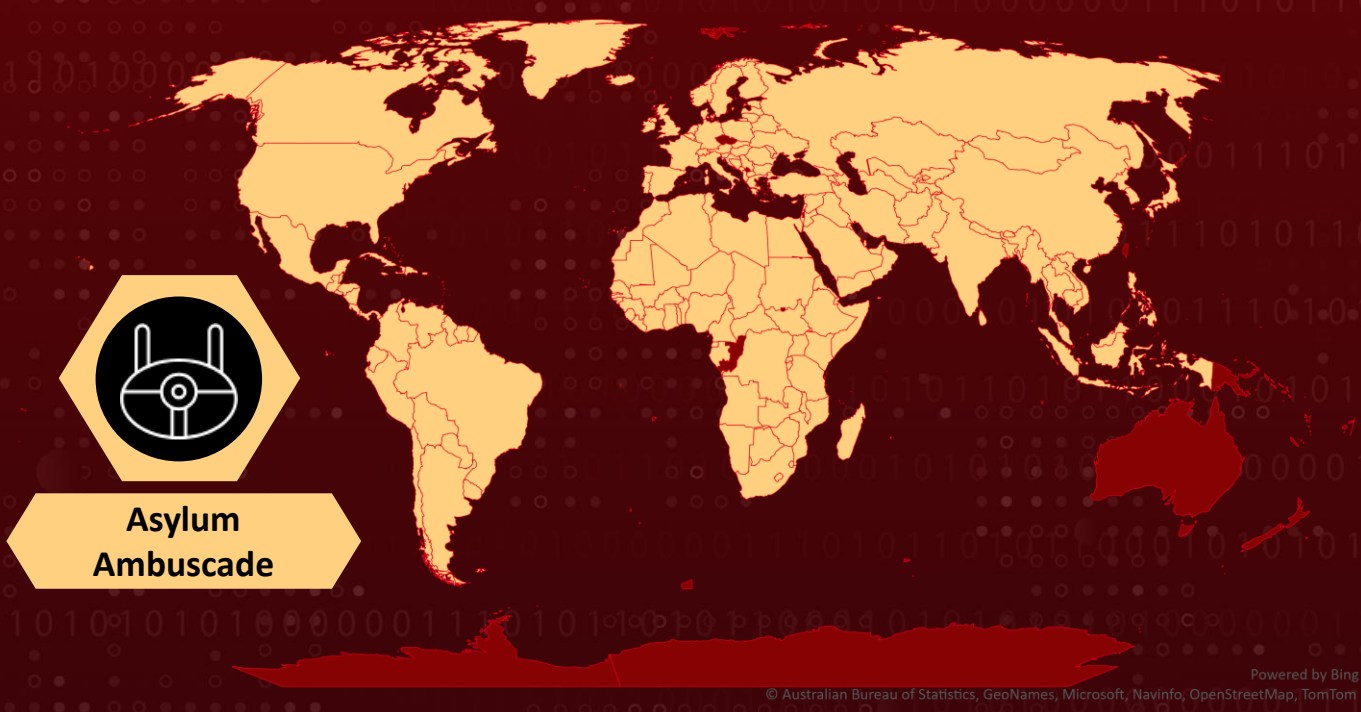
Asylum Ambuscade Unmasking the Hybrid Threat Group in Cybersecurity

Date of Publication	Admiralty code	TA Number
June 09, 2023	A1	TA2023257

Summary

First Appearance: 2020
Actor Name: Asylum Ambuscade
Target Region: North America, Europe, Asia, Africa, and South America
Target Sectors: Government entities, Financial, Cryptocurrency, Small and Medium Businesses including healthcare, manufacturing, technology, retail, and education.
Malware: NODEBOT, AHKBOT, SunSeed

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-30190	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓

Actor Details

#1

Asylum Ambuscade is a cybercrime group involved in cyberespionage operations. They have been active since 2020 and primarily target bank customers and cryptocurrency traders in North America and Europe. The group also engages in cyberespionage against government entities in Europe and Central Asia.

#2

They use script languages like AutoHotkey, JavaScript, Lua, Python, and VBS to develop their implants. Their cyberespionage campaigns involve spearphishing emails and malicious attachments or exploiting vulnerabilities such as CVE-2022-30190 (Follina). Additionally, Asylum Ambuscade has been involved in cybercrime campaigns, targeting individuals, cryptocurrency traders, and small to medium businesses worldwide.

#3

The group's toolset includes malicious JavaScript files and first-stage downloaders written in Lua, Tcl, and VBS. The main second-stage downloader is AHKBOT, developed in AutoHotkey, which downloads and interprets spy plugins, and a SunSeed downloader is written in Lua.

#4

They have recently incorporated new compromise vectors such as malicious Google Ads and introduced a new tool called "Nodebot." The group has been highly active, with approximately 265 victims per month since January 2022. While their primary motive appears to be financial gain from cryptocurrency and bank accounts, their targeting of SMBs suggests a possible interest in cyber espionage.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Asylum Ambuscade	Unknown **MOTIVE** Financial crime and espionage	North America, Europe, Asia, Africa, and South America	Government entities, Financial, Cryptocurrency, Small and Medium Businesses including healthcare, manufacturing, technology, retail, and education.

Recommendations

Robust Email Filtering and Anti-Phishing Measures: Implement advanced email filtering solutions and anti-phishing technologies to detect and block malicious emails containing suspicious attachments or links. This will significantly reduce the risk of employees interacting with Asylum Ambuscade's phishing attempts.

Patch Management and Endpoint Protection: Maintain up-to-date software and operating systems by promptly applying security patches. Deploy reliable endpoint protection solutions with anti-malware and anti-exploit capabilities to detect and remove Asylum Ambuscade's malicious software from endpoints.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0010 Exfiltration	TA0011 Command and Control	TA0009 Collection
TA0007 Discovery	TA0006 Credential Access	TA0005 Defense Evasion	TA0003 Persistence
TA0002 Execution	T1566 Phishing	T1583.003 Virtual Private Server	T1566.001 Spearphishing Attachment
T1190 Exploit Public-Facing Application	T1204.002 Malicious File	T1204 User Execution	T1059.001 PowerShell
T1059 Command and Scripting Interpreter	T1587.001 Malware	T1587 Develop Capabilities	T1059.006 Python
T1027 Obfuscated Files or Information	T1189 Drive-by Compromise	T1059.005 Visual Basic	T1059.007 JavaScript
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1027.010 Command Obfuscation	T1555.003 Credentials from Web Browsers

T1555 Credentials from Password Stores	T1087.002 Domain Account	T1087 Account Discovery	T1010 Application Window Discovery
T1482 Domain Trust Discovery	T1057 Process Discovery	T1518.001 Security Software Discovery	T1082 System Information Discovery
T1016 System Network Configuration Discovery	T1056.001 Keylogging	T1056 Input Capture	T1115 Clipboard Data
T1583 Acquire Infrastructure	T1071.001 Web Protocols	T1071 Application Layer Protocol	T1041 Exfiltration Over C2 Channel
T1113 Screen Capture			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	2B42FD41A1C8AC12221857DD2DF93164A71B95D7 D5F8ACAD643EE8E1D33D184DAEA0C8EA8E7FD6F8 57157C5D3C1BB3EB3E86B24B1F4240C867A5E94F 7DB446B95D5198330B2B25E4BA6429C57942CFC9 5F67279C195F5E8A35A24CBEA76E25BAD6AB6E8E C98061592DE61E34DA280AB179465580947890DE 519E388182DE055902C656B2D95CCF265A96CEAB AC3AFD14AD1AEA9E77A84C84022B4022DF1FC88B 64F5AC9F0C6C12F2A48A1CB941847B0662734FBF 557C5150A44F607EC4E7F4D0C0ED8EE6E9D12ADF F85B82805C6204F34DB0858E2F04DA9F620A0277 5492061DE582E71B2A5DA046536D4150F6F497F1 C554100C15ED3617EBFAAB00C983CED5FEC5DB11 AD8143DE4FC609608D8925478FD8EA3CD9A37C5D F2948C27F044FC6FB4849332657801F78C0F7D5E 7AA23E871E796F89C465537E6ECE962412CDA636 384961E19624437EB4EB22B1BF45953D7147FB8F 7FDB9A73B3F13DBD94D392132D896A5328DACA59 3E38D54CC55A48A3377A7E6A0800B09F2E281978 7F8742778FC848A6FBCFFEC9011B477402544171 296049970307529 19EA42B6D6CEE8D3AE28F527E 7A78AF75841C2A8D8A5929C214F08EB92739E9CB 441369397D0F8DB755282739A05CB4CF52113C40

TYPE	VALUE
SHA1	95EDC096000C5B8DA7C8F93867F736928EA32575 62FA77DAEF21772D599F2DC17DBBA0906B51F2D9 A9E3ACFE029E3A80372C0BB6B7C500531D09EDBE EE1CFEDD75CBA9028904C759740725E855AA46B5 117ECFA95BE19D5CF135A27AED786C98EC8CE50B D24A9C8A57C08D668F7D4A5B96FB7B5BA89D74C3
IPV4	5.39.222[.]150 5.44.42[.]27 5.230.68[.]137 5.230.71[.]166 5.230.72[.]38 5.230.72[.]148 5.230.73[.]57 5.230.73[.]63 5.230.73[.]241 5.230.73[.]247 5.230.73[.]248 5.230.73[.]250 5.252.118[.]132 5.252.118[.]204 5.255.88[.]222 23.106.123[.]119 31.192.105[.]28 45.76.211[.]131 45.77.185[.]151 45.132.1[.]238 45.147.229[.]20 46.17.98[.]190 46.151.24[.]197 46.151.24[.]226 46.151.25[.]15 46.151.25[.]49 46.151.28[.]18 51.83.182[.]153 51.83.189[.]185 62.84.99[.]195 62.204.41[.]171 77.83.197[.]138 79.137.196[.]121 79.137.197[.]187 80.66.88[.]155 84.32.188[.]29 84.32.188[.]96 85.192.49[.]106 85.192.63[.]13

TYPE	VALUE
IPV4	85.192.63[.]126 85.239.60[.]40 88.210.10[.]62 89.41.182[.]94 89.107.10[.]7 89.208.105[.]255 91.245.253[.]112 94.103.83[.]46 94.140.114[.]133 94.140.114[.]230 94.140.115[.]44 94.232.41[.]96 94.232.41[.]108 94.232.43[.]214 98.142.251[.]26 98.142.251[.]226 104.234.118[.]163 104.248.149[.]122 109.107.173[.]72 116.203.252[.]67 128.199.82[.]141 139.162.116[.]148 141.105.64[.]121 146.0.77[.]15 146.70.79[.]117 157.254.194[.]225 157.254.194[.]238 172.64.80[.]1 172.86.75[.]49 172.104.94[.]104 172.105.235[.]94 172.105.253[.]139 176.124.214[.]229 176.124.217[.]20 185.70.184[.]44 185.82.126[.]133 185.123.53[.]49 185.150.117[.]122 185.163.45[.]221 193.109.69[.]52 193.142.59[.]152 193.142.59[.]169 194.180.174[.]51 195.2.81[.]70

TYPE	VALUE
IPV4	195.133.196[.]230 212.113.106[.]27 212.113.116[.]147 212.118.43[.]231 213.109.192[.]230

Patch Link

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

References

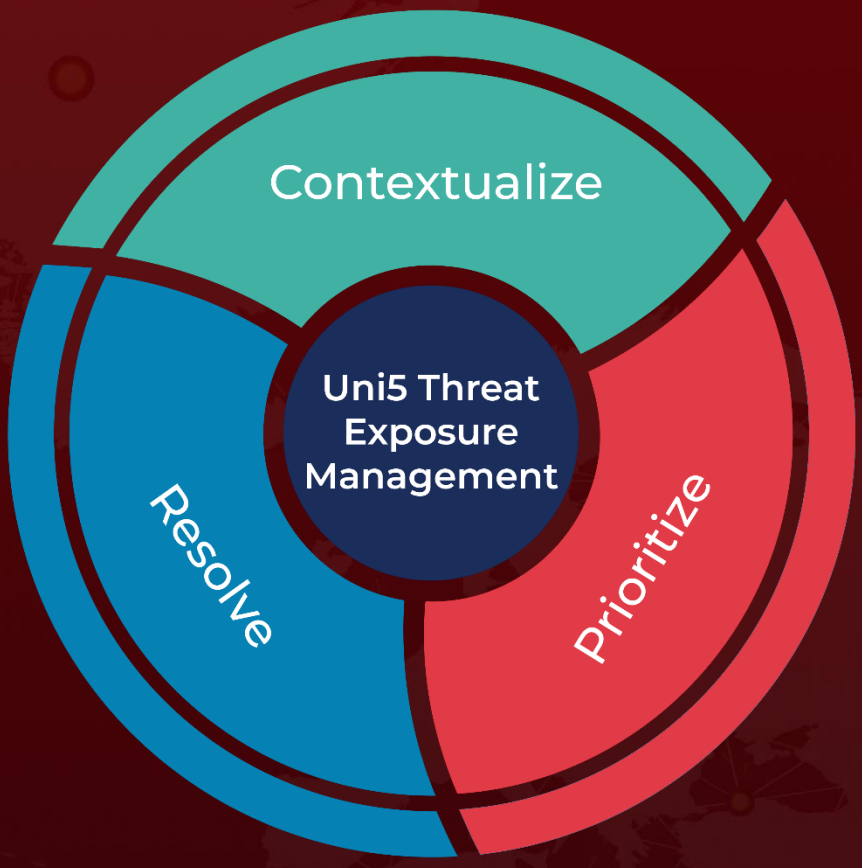
https://www.welivesecurity.com/2023/06/08/asylum-ambuscade-crimeware-or-cyberespionage/

https://www.bleepingcomputer.com/news/security/asylum-ambuscade-hackers-mix-cybercrime-with-espionage/

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

June 09, 2023. 5:30 AM

More at www.hivepro.com