Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Boolka: From Scripting to Sophisticated Malware Attacks

Date of Publication

June 26, 2024

Admiralty Code

A2

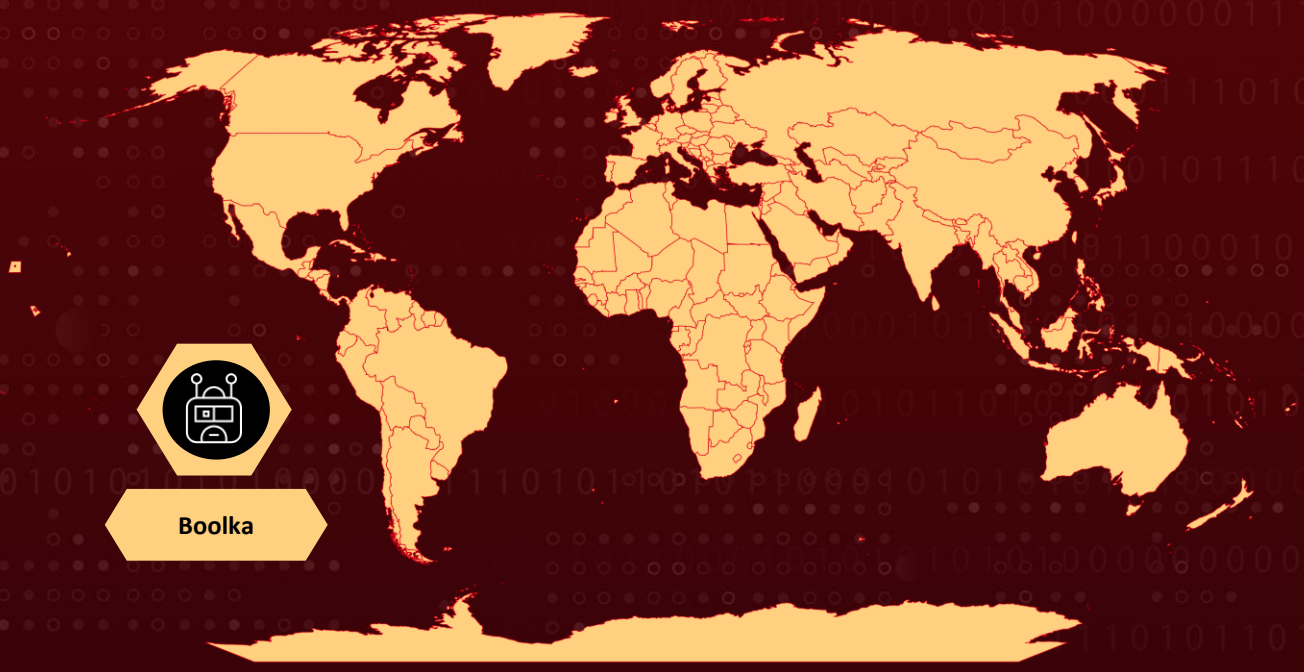
TA Number

TA2024246

Summary

First Appearance: 2022
Malware: BMANAGER
Targeted Countries: Worldwide
Threat Actor: Boolka
Affected Platforms: Windows
Attack: Boolka, a threat actor active since 2022, has steadily escalated their tactics. Initially, they relied on injecting websites with scripts to steal form data. By 2024, however, Boolka developed a custom malware delivery platform to distribute the BMANAGER trojan, highlighting Boolka's transition from simple web attacks to more sophisticated and potentially devastating malware-based assaults.

Attack Regions



Attack Details

#1 Boolka, a newly identified cyber threat actor, underwent a significant evolution in January 2024 with the deployment of the BMANAGER modular trojan. Prior to this development, Boolka was known for engaging in opportunistic SQL injection attacks against websites globally.

#2 These early attacks primarily involved the deployment of JavaScript scripts to steal form data. However, starting in January 2024, Boolka transitioned to more sophisticated cyber operations centered around the BMANAGER trojan.

#3 The BMANAGER trojan, distributed via the updatebrower[.]com domain, is a PyInstaller-packaged malware equipped with various modules including BMREADER (data exfiltration), BMLOG (keylogging), BMHOOK (application monitoring), and BMBACKUP (file theft).

#4 These modules communicate with a command-and-control (C2) server through HTTP(S) GET requests, demonstrating advanced capabilities such as persistence via Windows tasks and dynamic C2 server selection based on response times.

#5 Boolka's strategic shift from basic website compromises to complex malware operations underscores the escalating sophistication of cyber threats in recent years. This evolution highlights the adaptability and growing technical prowess of cyber threat actors like Boolka, emphasizing the need for robust cybersecurity measures to mitigate such threats effectively.

Recommendations

Enhance Web Security: Implement robust web application security measures, including regular vulnerability assessments and patch management to mitigate risks from SQL injection attacks and malicious JavaScript injections.

Monitor Network Traffic: Employ network monitoring tools to detect and block suspicious HTTP(S) traffic, especially to domains like updatebrower[.]com, associated with malware distribution.

Endpoint Protection: Deploy advanced endpoint protection solutions capable of detecting and mitigating threats like the BMANAGER trojan, including behavior-based detection to combat sophisticated malware modules such as keyloggers and data exfiltration tools.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0009 Collection	TA0006 Credential Access	TA0001 Initial Access
TA0010 Exfiltration	TA0040 Impact	TA0007 Discovery	T1059 Command and Scripting Interpreter
T1036 Masquerading	T1204 User Execution	T1204.002 Malicious File	T1583.004 Server
T1584.003 Virtual Private Server	T1584 Compromise Infrastructure	T1588.002 Tool	T1588 Obtain Capabilities
T1056.001 Keylogging	T1056 Input Capture	T1583.001 Domains	T1583 Acquire Infrastructure
T1189 Drive-by Compromise	T1190 Exploit Public-Facing Application	T1059.007 JavaScript	T1203 Exploitation for Client Execution
T1569 System Services	T1569.002 Service Execution	T1543 Create or Modify System Process	T1543.003 Windows Service
T1001 Data Obfuscation	T1657 Financial Theft	T1082 System Information Discovery	T1083 File and Directory Discovery
T1210 Exploitation of Remote Services	T1005 Data from Local System	T1071.001 Web Protocols	T1071 Application Layer Protocol
T1041 Exfiltration Over C2 Channel	T1565 Data Manipulation	T1565.002 Transmitted Data Manipulation	T1608 Stage Capabilities
T1608.001 Upload Malware			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2f10a81bc5a1aad7230cec197af987d00e5008edca205141ac74bc6219ea1802, 7266f20123edcb2e0b92ac0b63225b8db2c5ff349818b339ef1553bff06719e4, 9434e2f277f764bb75302cd5355ed45f7624f1d993a454a7dbaf68b7e9b4b3a2, b2dbd3187c67883c0f77c17530f41e05950e9e38b2798773770fe37f5985e367, 94430690ac9516a25ca764bae8c4b5a88d6f0308f558aea43ca50b5f750685ee, 227b8233071da4d3015cb04b69285885100c9f2e5d98b803b37d23afb798375a
Domains	boolka[.]tk, boolka24[.]tk, beonlineboo[.]com, beef[.]beonlineboo[.]com, mainnode[.]beonlineboo[.]com, node[.]beonlineboo[.]com, updatebrower[.]com
URLs	hxxp://mainnode[.]beonlineboo[.]com, hxxp://mainnode[.]beonlineboo[.]com/client?guid={guid}, hxxp://mainnode[.]beonlineboo[.]com/getmainnodes?guid={guid}, hxxp://mainnode[.]beonlineboo[.]com/getprogramms?guid={guid}, hxxp://mainnode[.]beonlineboo[.]com/getinstall?guid={guid}, hxxp://mainnode[.]beonlineboo[.]com/install?guid={guid}&name={version}, hxxp://mainnode[.]beonlineboo[.]com/usednodes?guid={guid}&t={nodeping}&node=hxxp://node[.]beonlineboo[.]com, hxxp://node[.]beonlineboo[.]com, hxxp://node[.]beonlineboo[.]com/client?guid={guid}, hxxp://node[.]beonlineboo[.]com/clientdata?guid={guid}&programm={programm}&title={titleencode}&vars={resultencode}, hxxp://node[.]beonlineboo[.]com/clientprogramm?guid={guid}&vars={resultencode}, hxxp://node[.]beonlineboo[.]com/clientfiledata?guid={guid}&vars={resultencode}, hxxp://updatebrower[.]com/download/bmanager[.]txt , hxxp://updatebrower[.]com/download/bmbackup[.]txt, hxxp://updatebrower[.]com/download/bmhook[.]txt, hxxp://updatebrower[.]com/download/bmlog[.]txt, hxxp://updatebrower[.]com/download/bmreader[.]txt, hxxp://boolka[.]tk/js/support[.]js?host=, hxxp://beef[.]beonlineboo[.]com/check?url=, hxxp://beef[.]beonlineboo[.]com/hook[.]js, hxxp://beonlineboo[.]com/js/support[.]js?host=, hxxp://boolka24[.]tk/js/support[.]js?host=

TYPE	VALUE
File Path	%USERPROFILE%\AppData\Local\Temp\coollog[.]db, %USERPROFILE%\AppData\Local\Temp\coollog[.]db-journal, C:\Program Files\Full Browser Manager\1[.]0[.]0\bmanager[.]exe, C:\Program Files\Full Browser Manager\1[.]0[.]0\bmbackup[.]exe, C:\Program Files\Full Browser Manager\1[.]0[.]0\bmhook[.]exe, C:\Program Files\Full Browser Manager\1[.]0[.]0\bmlog[.]exe, C:\Program Files\Full Browser Manager\1[.]0[.]0\bmreader[.]exe, %USERPROFILE%\AppData\Local\Temp\{UUID}[.]tmp
IPv4	194[.]165[.]16[.]68, 141[.]98[.]81[.]23, 179[.]60[.]150[.]123, 141[.]98[.]9[.]152, 92[.]51[.]2[.]78, 179[.]60[.]147[.]74, 45[.]182[.]189[.]109

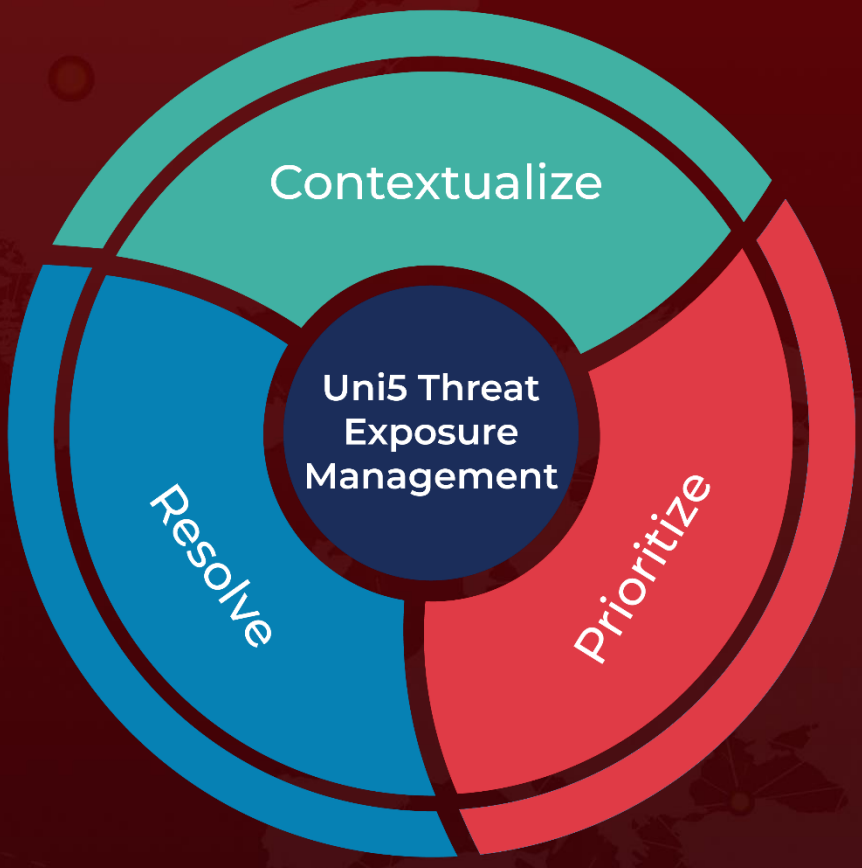
References

https://www.group-ib.com/blog/boolka/

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 26, 2024 • 7:30 AM

More at www.hivepro.com