Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

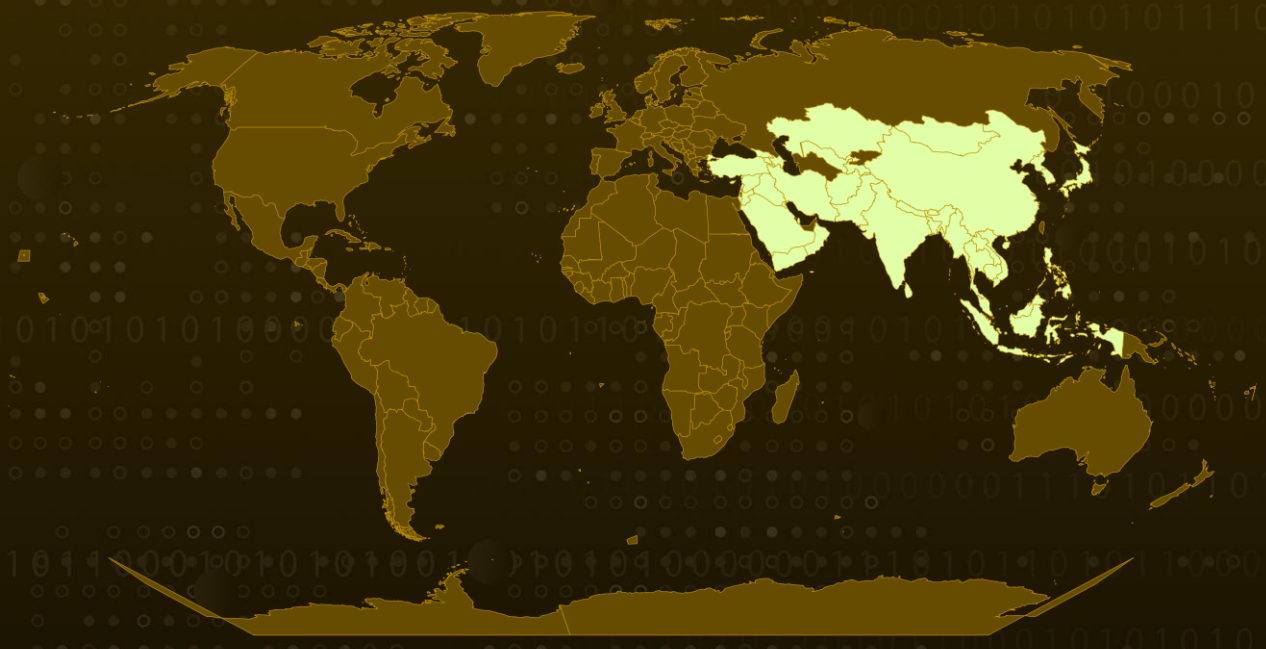
Unveiling The SuperBear RAT campaigns Targeting the Journalists

Date of Publication	Admiralty Code	TA Number
September 6, 2023	A1	TA2023354

Summary

First appeared: August 28, 2023
Malware: SuperBear RAT
Attack Region: Asia
Targeted Industry: Media
Affected Platform: Windows
Attack: A recently discovered remote access trojan (RAT) named "SuperBear" has come to attention as it is actively utilized by hackers to target journalists that focus on covering geopolitical developments in Asia. It appears that this campaign aimed at compromising civil society groups.

Attack Regions



Attack Details

#1 A new remote access trojan (RAT) known as SuperBear is currently being deployed by hackers and criminals, with their primary targets being journalists focusing on Asia's geopolitical landscape. A common tactic employed in this campaign involves sending victims a deceitful .LNK file via email, which is skillfully designed to mimic the appearance of an email from one of their organization's members.

#2 An AutoIT script was identified as part of this campaign, and it was employed to execute a process injection technique known as process hollowing. The specific targets of this campaign appear to be civil society groups.

#3 The attack exhibited a carefully organized series of steps aimed at maintaining stealth and avoiding detection. Following the execution of the deceptive .LNK file, a concealed PowerShell command was initiated. This action resulted in the emergence of a hidden PowerShell window, operating in parallel with the legitimate document.

#4 The PowerShell command was harnessed for obfuscation, executing a sequence of operations that culminated in the creation of a VBS script within the user's profile directory. Two payloads were extracted from a compromised WordPress instance belonging to a legitimate website.

#5 These payloads consisted of the AutoT3 executable and a compiled AutoT3 script. These components were employed to execute malicious code using the process injection technique. The malicious code attempts to generate a random filename for itself; if it cannot do so, it will be named SuperBear. This malicious code has been identified as a novel RAT (Remote Access Trojan) and has been dubbed the SuperBear RAT.

Recommendations

Email Security: Implement robust email filtering to counteract spam, phishing, and malicious attachments, and exercise caution with unverified links and email attachments by validating their authenticity before opening.

URL Filtering: Utilize URL filtering to prevent access to malicious domains and reduce the risk of inadvertent malware downloads. Additionally, vigilantly monitor network beacons to halt data exfiltration driven by malware.

Endpoint Security: Implement robust endpoint security solutions that encompass antivirus and anti-malware software. Keep these security tools up-to-date to ensure comprehensive defense against emerging threats.

Network Segmentation: Implement proper network segmentation to limit the lateral movement of malware within the network. By dividing the network into smaller, isolated segments, organizations and can prevent it from accessing critical systems and sensitive data.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0011 Command and Control	TA0010 Exfiltration	TA0004 Privilege Escalation	TA0003 Persistence
T1566 Phishing	T1566.002 Spearphishing Link	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1204 User Execution	T1204.001 Malicious Link	T1036 Masquerading	T1055 Process Injection
T1001 Data Obfuscation	T1041 Exfiltration Over C2 Channel	T1055.012 Process Hollowing	T1106 Native API
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1059.005 Visual Basic	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	5305b8969b33549b6bd4b68a3f9a2db1e3b21c5497a5d82cec9beaeca007630e, 282e926eb90960a8a807dd0b9e8668e39b38e6961b0023b09f8b56d287ae11cb, 454cfe3be695d0a387d7877c11d3b224b3e2c7d22fc2f31f349b5c23799967ec
SHA1	557820050eaed5f32241346caeefdfff0ce44745
IP	89[.]117[.]139[.]230
Domain	hironchk[.]com
MD5	e49aaa9a5933c48feca39f3080a7b94d, 614dda72d95b5dfd732916aec0662598

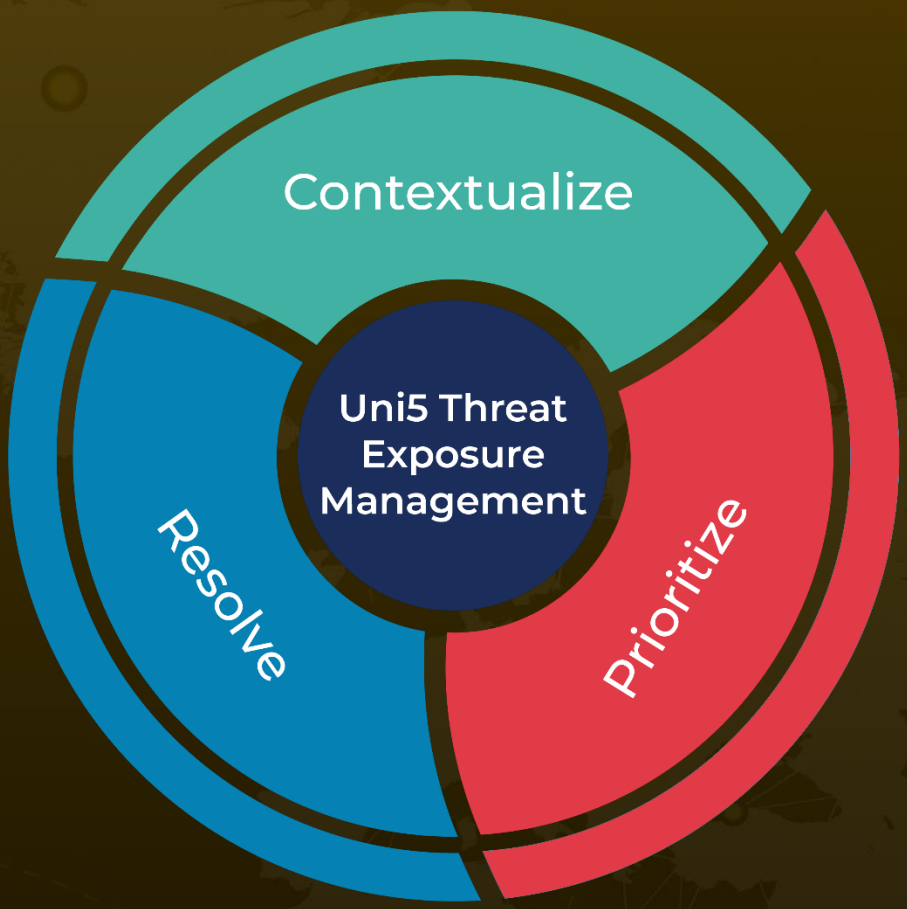
References

https://interlab.or.kr/archives/19416

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

September 6, 2023 • 12:30 AM

More at www.hivepro.com