Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Gamaredon Deploys LitterDrifter USB Worm in Cyber Espionage Operations

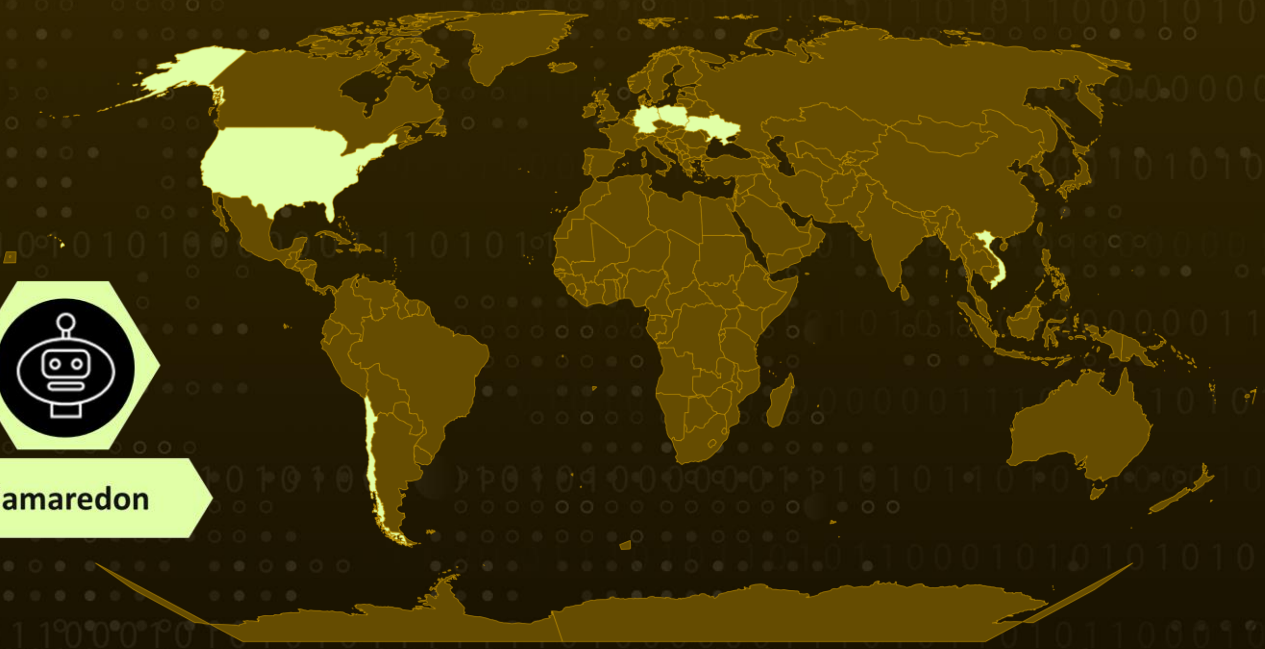
Date of Publication	Admiralty Code	TA Number
November 20, 2023	A1	TA2023467

Summary

Attack Discovered: November 17, 2023
Attack Region: Ukraine, USA, Vietnam, Chile, Poland, Germany, Hong Kong
Actor: Gamaredon (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard)
Malware: LitterDrifter
Attack: Russian cyber espionage group Gamaredon (aka Primitive Bear) has been observed utilizing a USB-propagating worm known as LitterDrifter in attacks targeting Ukrainian entities. This group has recently adopted LitterDrifter, a worm written in VBS, designed to spread through removable USB drives and establish a command-and-control channel.

Attack Regions

Gamaredon



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

Attack Details

#1 Gamaredon(aka Primitive Bear), a Russian espionage group focusing on Ukrainian entities, has incorporated a USB-propagating worm known as LitterDrifter into its operations. Crafted in VBS, LitterDrifter is designed to spread via removable USB drives and establish a secure C2 channel. Gamaredon's extensive campaigns aim at data collection and sustaining persistent access and control channels across diverse targets, utilizing LitterDrifter for automatic spreading and communication with command-and-control servers.

#2 The LitterDrifter is a self-propagating worm that spreads across drives and sets up a C2 channel connecting to Gamaredon's infrastructure. Operating within an orchestration component named "trash.dll," it decodes and executes various modules, ensuring initial persistence within the victim's environment.

#3 Following successful execution, the system activates two extracted modules: the Spreader module and the C2 Module. The Spreader module is responsible for distributing the malware, potentially spreading it to other environments by recursively accessing subfolders in each drive and creating LNK decoy shortcuts, alongside a hidden copy of the "trash.dll" file. The C2 Module retrieves an IP address for the command-and-control server and maintains a backup option for obtaining this information from a Telegram channel, facilitating communication with the attacker.

#4 LitterDrifter is a malware specifically crafted for large-scale collection operations, employing straightforward yet effective techniques to target a broad range of entities in the region. Its design aligns with Gamaredon's overall approach, showcasing significant effectiveness, particularly in the context of the group's persistent activities within Ukraine. Gamaredon primary targets being entities in Ukraine, there are indications of USB worm infections in USA, Vietnam, Chile, Poland, Germany, and Hong Kong as well.

Recommendations

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.

Device Control Policies: Implement device control policies to restrict the use of USB devices. This can include limiting the types of USB devices that are allowed, such as only allowing authorized devices.

Network Segmentation: Implement network segmentation to isolate critical systems from less secure areas. This can help contain the impact of a potential USB-based attack.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0011 Command and Control	T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information
T1102 Web Service	T1008 Fallback Channels	T1053 Scheduled Task/Job	T1047 Windows Management Instrumentation
T1071 Application Layer Protocol	T1091 Replication Through Removable Media		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	cbeaedfa84b02a2bd41a70fa92a46c36, 6349dd85d9549f333117a84946972d06, 2239800bfc8fdfddf78229f2eb8a7b95, 42bc36d5debc21dff3559870ff300c4e, 4c2431e5f868228c1f286fca1033d221, 1536ec56d69cc7e9aebb8fbd0d3277c4, 49d1f9ce1d0f6dfa94ad9b0548384b3a, 83500309a878370722bc40c7b83e83e3, 8096dfaa954113242011e0d7aaaebffd, bbb464b327ad259ad5de7ce3e85a4081, cdae1c55ec154cd6cef4954519564c01,

TYPE	VALUE
MD5	2996a70d09fff69f209051ce75a9b4f8, 9d9851d672293dfd8354081fd0263c13, 96db6240acb1a3fca8add7c4f9472aa5, 1c49d04fc0eb8c9de9f2f6d661826d24, 88aba3f2d526b0ba3db9bc3dfee7db39, 86d28664fc7332eafb788a44ac82a5ed, 1da0bf901ae15a9a8aef89243516c818, 579f1883cdfd8534167e773341e27990, 495b118d11ceae029d186ffdbb157614
Domains	ozaharso[.]ru, nubiumbi[.]ru, acaenaso[.]ru, atonpi[.]ru, suizibel[.]ru, dakareypa[.]ru, ahmozpi[.]ru, nebtoizi[.]ru, squeamish[.]ru, nahtizi[.]ru, crisiumbi[.]ru, arabianos[.]ru, gayado[.]ru, quyenzo[.]ru, credomched[.]ru, lestemps[.]ru, urdevont[.]ru, hoanzo[.]ru, absorbeni[.]ru, aethionemaso[.]ru, aychobanpo[.]ru, ayzakpo[.]ru, badrupi[.]ru, barakapi[.]ru, boskatrem[.]ru, brudimar[.]ru, decorous[.]ru, dumerilipi[.]ru, heartbreaking[.]ru, judicious[.]ru, karoanpa[.]ru, lamentable[.]ru, procellarumbi[.]ru, ragibpo[.]ru, raidla[.]ru, ramizla[.]ru,

TYPE	VALUE
Domains	samiseto[.]ru, superficial[.]ru, talehgi[.]ru, undesirable[.]ru, valefgo[.]ru, vasifgo[.]ru, vilaverde[.]ru, vloperang[.]ru, zerodems[.]ru, geminiso[.]ru, sabirpo[.]ru, andamanos[.]ru, triticumos[.]ru

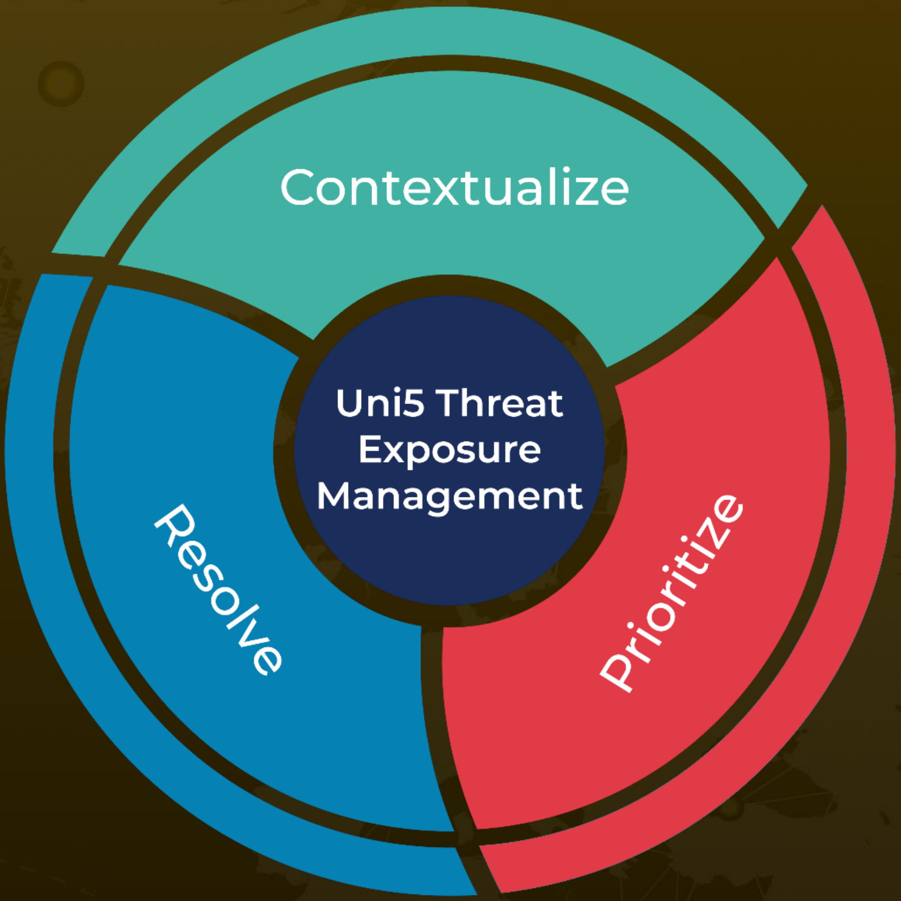
References

https://research.checkpoint.com/2023/malware-spotlight-into-the-trash-analyzing-litterdrifter/

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

November 20, 2023 • 3:30 AM

© 2023 All Rights are Reserved by Hive Pro®

More at www.hivepro.com