Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

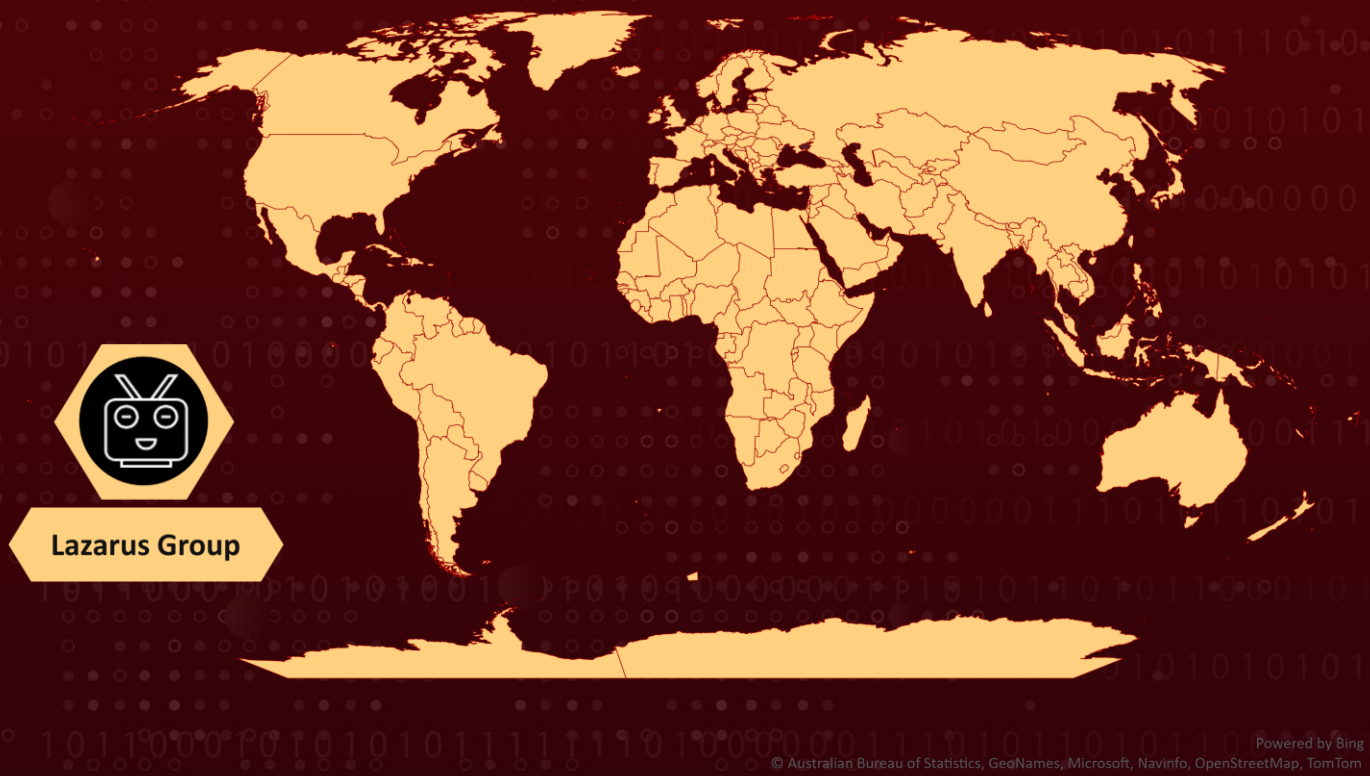
Lazarus Unleash SIGNBT Malware in Latest Campaign

Date of Publication	Admiralty Code	TA Number
October 30, 2023	A1	TA2023439

Summary

Active Since: July 2023
Threat Actor: Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)
Malware: SIGNBT, LPEClient
Attack Region: Worldwide
Targeted Industries: Defense, Nuclear, Cryptocurrency
Attack: The Lazarus Group has been identified as the mastermind behind a recent cyber campaign. They persistently targeted a software vendor, successfully compromising the vendor's systems by exploiting software vulnerabilities and introducing the SIGNBT malware to gain control over their victims.

Attack Regions



Attack Details

#1 The Lazarus Group, which is linked to North Korea, has been identified as the orchestrator behind a recent cyber campaign. In this campaign, they persistently targeted a software vendor, successfully compromising their systems. This was achieved by exploiting vulnerabilities in the software, despite the availability of multiple patches and prior warnings.

#2 The adversary displayed a high degree of sophistication, employing advanced evasion techniques and introducing the SIGNBT malware to gain control over their victims. Additionally, other malicious software found in the system's memory included the well-known LPEClient, a tool recognized for its role in profiling victims and delivering payloads. This tool has been previously observed in attacks targeting defense contractors and the cryptocurrency industry.

#3 In mid-July 2023, a series of attacks were launched against several victims who were targeted through the use of legitimate security software designed to encrypt web communications using digital certificates. The exact method by which this software was exploited to distribute the SIGNBT malware remains a mystery.

#4 SIGNBT primarily functions to establish communication with a remote server and retrieve further commands for execution on the infected host. This malicious tool possesses a wide range of capabilities to exert control over the victim's system, including process enumeration, file and directory operations, credential theft, and the deployment of additional payloads like LPEClient.

#5 LPEClient, an information-stealing tool, utilizes advanced techniques such as disabling user-mode syscall hooking and restoring system library memory sections. The Lazarus group continues to pose a highly active and adaptable threat, demonstrating a deep understanding of IT environments and continuously evolving their tactics, which includes exploiting vulnerabilities in widely-used software.

Recommendations

Vendor Risk Assessment: Evaluate the security measures of software vendors and third-party suppliers regularly. Ensure they are adhering to strong security practices to reduce the risk of compromise.

Encryption for Data in Transit and at Rest: Implement encryption for sensitive data both in transit and at rest. This safeguards against data interception during communication and protects stored data in case of unauthorized access.

Network Segmentation: Implement network segmentation to limit lateral movement for attackers who manage to breach one part of the network. This can minimize the extent of damage they can cause.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0011 Command and Control	**TA0010** Exfiltration	**T1189** Drive-by Compromise	**T1203** Exploitation for Client Execution
T1547.012 Print Processors	**T1574.002** DLL Side-Loading	**T1140** Deobfuscate/Decode Files or Information	**T1027.001** Binary Padding
T1027.002 Software Packing	**T1620** Reflective Code Loading	**T1003.001** LSASS Memory	**T1057** Process Discovery
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1113** Screen Capture	**T1071.001** Web Protocols
T1132.002 Non-Standard Encoding	**T1573.001** Symmetric Cryptography	**T1041** Exfiltration Over C2 Channel	**T1547** Boot or Logon Autostart Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	9cd90dff2d9d56654dbecdcd409e1ef3, 88a96f8730b35c7406d57f23bbba734d, 54df2984e833ba2854de670cce43b823, Ae00b0f490b122ebab614d98bb2361f7, e6fa116ef2705ecf9677021e5e2f691e, 31af3e7fff79bc48a99b8679ea74b589, 9b62352851c9f82157d1d7fcafeb49d3, 3a77b5054c36e6812f07366fb70b007d, e89fa6345d06da32f9c8786b65111928
File Paths	C:\GoogleD\Coding\JS\Node\winhttp.dll, %system%\ualapi.dll, %systme%\wbem\wbemcomn.dll, %ProgramData%\Microsoft\Windows\ServiceSetting\ESENT.dll, C:\GoogleD\Coding\JS\Node\SgrmLpac.exe, C:\GoogleD\Coding\JS\Node\winhttp.dll, C:\Windows\system32\config\systemprofile\appdata\Local\tw-100a-a00-e14d9.tmp, C:\Windows\system32\config\systemprofile\appdata\Local\tw-100b-a00-e14d9.tmp, C:\ProgramData\ntuser.008.dat, C:\ProgramData\ntuser.009.dat, C:\ProgramData\ntuser.001.dat, C:\ProgramData\ntuser.002.dat, C:\ProgramData\Microsoft\Windows\ServiceSetting\ESENT.dll
URLs	hxxp://ictm[.]or[.]kr/UPLOAD_file/board/free/edit/index[.]php, hxxp://samwoosystem[.]co[.]kr/board/list/write[.]asp, hxxp://theorigin[.]co[.]kr:443/admin/management/index[.]php, hxxp://ucware[.]net/skins/PHPMailer-master/index[.]php, hxxp://www[.]friendmc[.]com/upload/board/asp20062107[.]asp, hxxp://www[.]hankooktop[.]com/ko/company/info[.]asp, hxxp://www[.]khmcpharm[.]com/Lib/Modules/HtmlEditor/Util/read[.]cer, hxxp://www[.]vietjetairkorea[.]com/INFO/info[.]asp, hxxp://yoohannet[.]kr/min/tmp/process/proc[.]php, hxxps://admin[.]esangedu[.]kr/XPaySample/submit[.]php, hxxps://api[.]shw[.]kr/login_admin/member/login_fail[.]php, hxxps://hicar[.]kalo[.]kr/data/rental/Coupon/include/inc[.]asp, hxxps://hspje[.]com:80/menu6/teacher_qna[.]asp, hxxps://kscmfs[.]or[.]kr/member/handle/log_proc[.]php, hxxps://kstr[.]radiology[.]or[.]kr/upload/schedule/29431_1687715624[.]inc,

TYPE	VALUE
URLs	hxxps://little-pet[.]com/web/board/skin/default/read[.]php, hxxps://mainbiz[.]or[.]kr/SmartEditor2/photo_uploader/popup/edit[.]asp, hxxps://mainbiz[.]or[.]kr/include/common[.]asp, hxxps://new-q-cells[.]com/upload/newsletter/cn/frame[.]php, hxxps://pediatrics[.]or[.]kr/PubReader/build_css[.]php, hxxps://pms[.]nninc[.]co[.]kr/app/content/board/inc_list[.]asp, hxxps://safemotors[.]co[.]kr/daumeditor/pages/template/template[.]asp, hxxps://swt-keystonevalve[.]com/data/editor/index[.]php, hxxps://vnfmal2022[.]com/niabbs5/upload/gongji/index[.]php, hxxps://warevalley[.]com/en/common/include/page_tab[.]asp, hxxps://www[.]blastedlevels[.]com/levels4SqR8/measure[.]asp, hxxps://www[.]droof[.]kr/Board/htmlEdit/PopupWin/Editor[.]asp, hxxps://www[.]friendmc[.]com:80/upload/board/asp20062107[.]asp, hxxps://www[.]hanlasangjo[.]com/editor/pages/page[.]asp, hxxps://www[.]happinesscc[.]com/mobile/include/func[.]asp, hxxps://www[.]healthpro[.]or[.]kr/upload/naver_editor/subview/view[.]inc, hxxps://www[.]medric[.]or[.]kr/Controls/Board/certificate[.]cer, hxxps://www[.]muijae[.]com/daumeditor/pages/template/simple[.]asp, hxxps://www[.]muijae[.]com/daumeditor/pages/template/template[.]asp, hxxps://www[.]nonstopexpress[.]com/community/include/index[.]asp, hxxps://www[.]seoulanesthesia[.]or[.]kr/mail/mail_211230[.]html, hxxps://www[.]seouldementia[.]or[.]kr/_manage/inc/bbs/jiyeuk1_ok[.]asp, hxxps://www[.]siriuskorea[.]co[.]kr/mall/community/bbs_read[.]asp, hxxps://yoohannet[.]kr/min/tmp/process/proc[.]php

References

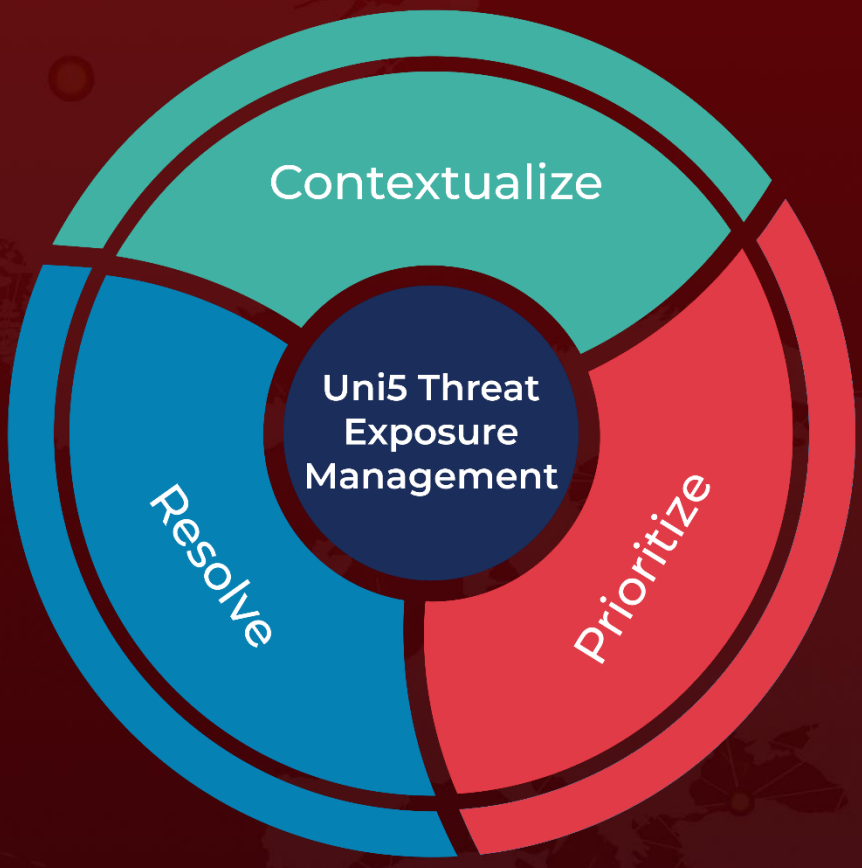
https://securelist.com/unveiling-lazarus-new-campaign/110888/

https://www.hivepro.com/smoothoperator-campaign-trojanizes-3cxdesktopapp/

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 30, 2023 . 5:30 AM

More at www.hivepro.com