Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Lazarus Group's Targeted Attacks on Korean Sectors

Date of Publication	Admiralty Code	TA Number
October 17, 2023	A1	TA2023419

Summary

Active Since: 2009
Malware: Volgmer and Scout
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)
Attack Region: Korea
Targeted Industries: Satellite, Software, Media, Defense, Manufacturing, ICT, And Financial Sectors.
Attack: The Lazarus a state-sponsored threat group, has been employing sophisticated tactics like spear phishing and supply chain attacks, and utilizing various types of malware for control.

Attack Regions

Attack Details

#1 The Lazarus threat group, state-backed, has a well-documented history of activity dating back to 2009. Typically, the group employed sophisticated tactics like spear phishing and supply chain attacks, skillfully disguising malware as authentic programs in their offensive maneuvers.

#2 In recent years, they shifted towards conducting watering hole attacks, targeting numerous South Korean enterprises and organizations in defense, satellite technology, software, and media. Their initial access strategy involved exploiting a security vulnerability within Korean financial security certification software, in addition to deploying a diverse array of backdoors for subsequent control over compromised systems.

#3 Volgmer, a DLL-type backdoor, has been discreetly installed by the Lazarus threat group since 2014, adopting a deceptive name to masquerade as a legitimate file. Alongside the initial version of Volgmer, a dropper was identified, installing Volgmer by creating a password-protected compressed version in the resource area before registering it as a service.

#4 Notably, Volgmer exhibits a unique characteristic of employing specific logic to randomly generate strings for the name of the Volgmer DLL file. Operating as a service, it decrypts registry values to acquire configuration data, subsequently transmitting them to the command and control (C&C) server.

#5 Introduced in 2014, Scout Downloader, once activated, manifests a graphical user interface (GUI), setting it apart from typical malware behaviors. Scout employs a file name-based lookup of the registry value housing encrypted configuration data.

#6 This malware, strategically employed by threat actors, facilitates control over compromised systems. Additionally, a noteworthy incident involved the utilization of BYOVD (Bring Your Own Vulnerable Driver), where the threat actor exploited a vulnerable driver module from a hardware supplier to disable security products.

Recommendations

Supply Chain Security: Strengthen supply chain security by vetting and monitoring third-party software and hardware suppliers. Implement measures to verify the integrity of products and services, reducing the risk of compromise through the supply chain.

Enable Audit Logging: Activate audit logging for DLL loading events on Windows endpoints. This allows for the collection of detailed information about DLL loads, helping security teams identify anomalous behavior.

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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0010 Exfiltration
T1071.001 Web Protocols	T1059 Command and Scripting Interpreter	T1573.001 Symmetric Cryptography	T1098 Account Manipulation
T1566 Phishing	T1195 Supply Chain Compromise	T1204 User Execution	T1047 Windows Management Instrumentation
T1543 Create or Modify System Process	T1574.002 DLL Side-Loading	T1070 Indicator Removal	T1573 Encrypted Channel
T1105 Ingress Tool Transfer			

Indicators of Compromise (IOCs)

TYPE	VALUE
Registry Keys	HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security, HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / 125463f3-2a9c-bdf0-d890-5a98b08d8898, HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / f0012345-2a9c-bdf8-345d-345d67b542a1, HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / 2d54931A-47A9-b749-8e23-311921741dcd, HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / c72a93f5-47e6-4a2a-b13e-6AFE0479cb01, HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / [First four letters of the file name]-5903-ed41-902f-e93a29dafef5, HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / “626e7376-5903-ed41-902f-e93a29dafef5”, HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / “626e7376-2790-10f2-dd2a-d92f482d094f”, HKLM\SYSTEM\CurrentControlSet\Control\Lsa / Security Packages, HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost / netsvcs
File Path	C:\Windows\system32{hlrmenum}.dll
MD5	0171c4a0a53188fe6f9c3dfcc5722be6, 05bb1d8b7e62f4305d97042f07c64679, 0b746394c9d23654577f4c0f2a39a543, 0b78347acf76d4bb66212bf9a41b9fb9, 0ed86587124f08325cd8f3d3d2556292, 17eacf4b4ae2ca4b07672dcc12e4d66d, 1c89fb4aee20020bfd75713264df97cd, 1e2acecce7b5e9045b07d65e9e8afe1f, 1ecd83ee7e4cfc8fed7ceb998e75b996, 1f1a3fe0a31bd0b17bc63967de0ccc29, 202a7eec39951e1c0b1c9d0a2e24a4c4, 225cdc9b452b6d5a3f7616dcc9333d7d, 226cc1f17c4625837b37b5976acbd68e, 35943aa640e122fcb127b2bfd6e29816, 35f9cfe5110471a82e330d904c97466a, 394b05394ebb9b239a063a6b5839edb9, 3e6119ebfacd1d88acbd2ca460c70b49, 43f218d3a4b2199468b00a0b43f51c79, 44fa8daa347ef5dd107bf123b4688797, 4753679cef5162000233d69330208420, 4b1f1db4f169ca6b57015b313d665045, 5473fa2c5823fbab2b94e8d5c44bc7b4, 5496adcd712d4378950ba62ad4c2423b, 570a4253ae80ee8c2b6b23386e273f3a,

TYPE	VALUE
MD5	5c87373eef090bed525b80aef398ee8a, 5dd1ccc8fb2a5615bf5656721339efed, 64965a88e819fb93dbabafc4e3ad7b6c, 64cac69ab1e9108e0035f9ce38b47db7, 693afaedf740492df2a09dfcc08a3dff, 695e5b8dc9615ec603fe2cbb7326a50f, 6da7d8aec65436e1350f1c0dfc4016b7, 6e21cc6669ada41e48b369b64ec5f37b, 72756e6ebb8274d9352d8d1e7e505906, 76f02ab112b8e077544d0c0a6e0c428a, 7ba37d662f19bef27c3da2fd2cee0e3a, 7f0e773397808b4328ad11d6948a683f, 7f953c6988d829c9c4ac2002572c9055, 80d34f9ca10b0e8b49c02139e4615b7a, 8543667917a318001d0e331aeae3fb9b, 855e26d530e69ddc77bb19561fb19d90, 85b6e4ea8707149b48e41454cbd0d5ad, 8b3ec4b9c7ad20af418e89ca6066a3ad, 947124467bd04b7624d9b31e02b5ee7f, 9a5fa5c5f3915b2297a1c379be9979f0, 9a87f19609f28d7f7d76f9759864bd08, 9ec3a4257564658f651896abc608680e, a545f548b09fdf61405f5cc07e4a7fa1, a76624578ed42cceba81c76660977562, b1225fa644eebafba07f0f5e404bd4fd, b457e8e9d92a1b31a4e2197037711783, b517e7ad07d1182feb4b8f61549ff233, bf5d815597018fe7f3dfb52d4f7e1f65, c07e04d388fb394ac190aace51c03c33, c16a6178a4910c6f3263a01929f306b9, c2ab2a8ffdc18c24080e889a634ef279, c41eb1ea59fab31147c5b107cc1c5a51, cc5a8a15d5808002e62d5daf2d4f31b3, cf2ff5b59c638a06d8b81159b9a435ea, d52b5d8c20964333f79ff1bce3385d0b, e273803ae6724a714b970dd86ca1acd0, e3d03829cbec1a8cca56c6ae730ba9a8, ea5d322648ff108b1c9cbdd1ef4a5959, eb9db98914207815d763e2e5cfbe96b9

References

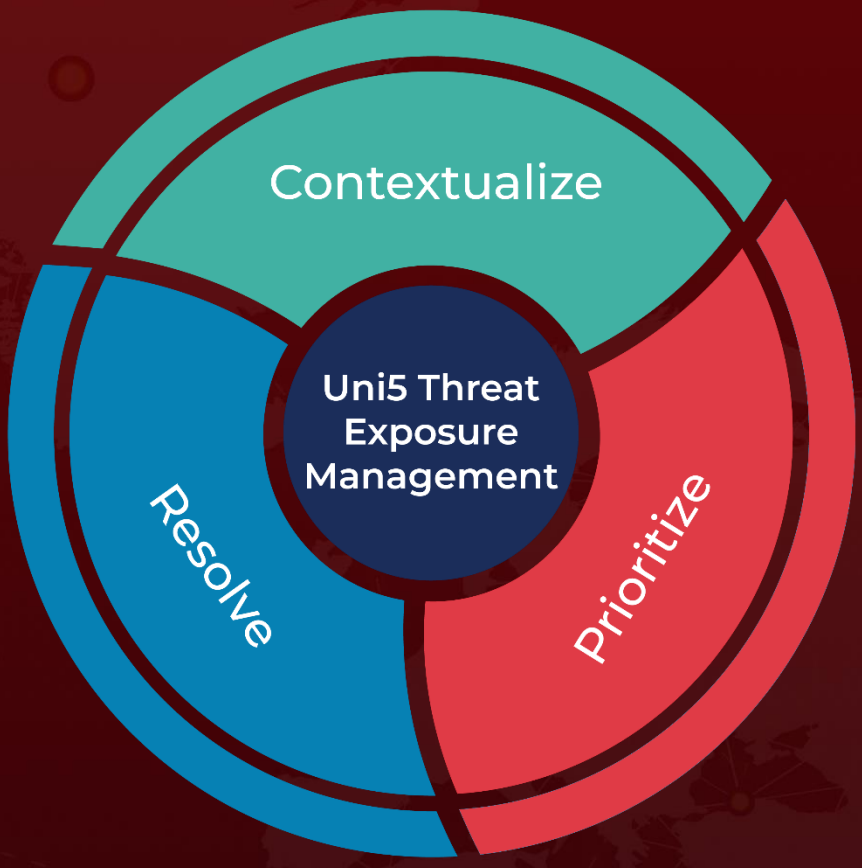
https://asec.ahnlab.com/en/57685/

https://attack.mitre.org/groups/G0032/

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 17, 2023 . 5:00 AM

More at www.hivepro.com