Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

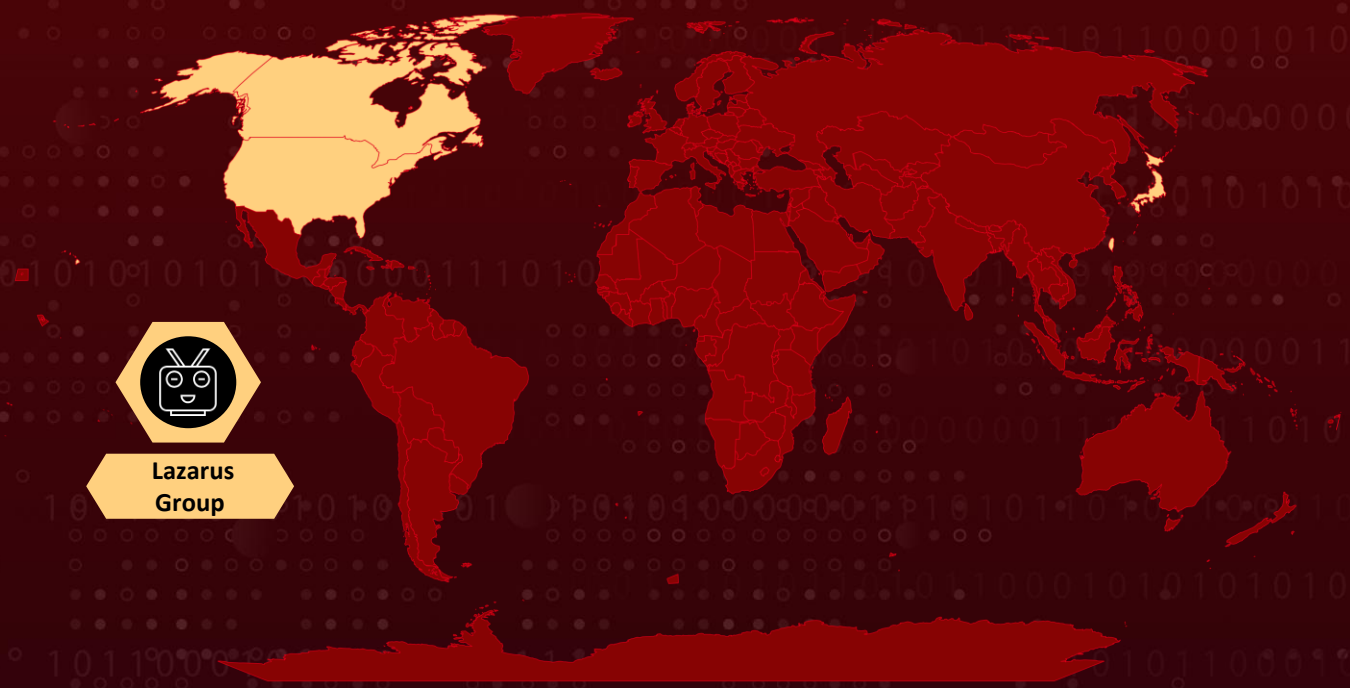
Lazarus Group Orchestrates Supply Chain Attack on CyberLink Corp

Date of Publication	Admiralty Code	TA Number
November 24, 2023	A1	TA2023475

Summary

Attack Began: October 20, 2023
Attack Region: Japan, Taiwan, Canada, and the United States
Actor Name: 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) and Andariel (aka Silent Chollima, Stonefly, Plutonium, Onyx Sleet)
Malware: LambLoad
Targeted Industries: Media, Defense, Information Technology
Attack: The Lazarus Group (Labyrinth Chollima) orchestrated a supply chain attack on CyberLink Corp., manipulating a legitimate application installer to impact over 100 devices globally. The attack involves a second-stage payload, labeled LambLoad, communicating with compromised infrastructure and reflecting Lazarus Group's focus on espionage and trojanized software use.

Attack Regions



Attack Details

#1 The Lazarus Group (Labyrinth Chollima), a North Korean threat actor, has been identified in a supply chain attack targeting CyberLink Corp., a multimedia software company. In this attack, a legitimate CyberLink application installer was manipulated by embedding malicious code to download, decrypt, and execute a second-stage payload. The manipulated file, signed with a valid CyberLink Corp. certificate, is hosted on CyberLink's genuine update infrastructure and employs evasion techniques against security product detection.

#2 The impact of this malicious activity extends to over 100 devices across countries such as Japan, Taiwan, Canada, and the United States. Lazarus Group is confidently attributed to this activity, which involves a second-stage payload communicating with compromised infrastructure linked to the threat actor. The group is observed using trojanized open-source and proprietary software, with a focus on industries like information technology, defense, and media.

#3 Lazarus Group specializes in espionage, data theft, financial gain, and disruption of corporate networks. The group employs custom malware tailored to its operations, and recent activities include the use of trojanized software and exploitation of N-day vulnerabilities.

#4 The weaponized downloader and loader, identified as LambLoad, is integrated into a legitimate CyberLink application. LambLoad performs specific checks to ensure operation in environments lacking protection from certain security software. If conditions are met, it downloads a second-stage payload from compromised domains, concealing it as a PNG file. This payload establishes communication with compromised infrastructure controlled by Lazarus Group.

Recommendations

Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.

Enhance Endpoint Security: Deploy advanced endpoint security solutions, such as endpoint detection and response (EDR) tools, to identify and respond to malicious activities promptly. Keep security software, including antivirus and endpoint protection, up to date to defend against known threats.

Update and Monitor Software Supply Chains: Regularly update and validate the integrity of software supply chains to identify potential vulnerabilities or unauthorized modifications. Establish a thorough vetting process for software updates and installations, especially from third-party vendors.

Maintain a Disallowed Certificate List: Establish and maintain a disallowed certificate list, including certificates associated with known or suspected malicious activities. Regularly update this list based on threat intelligence and incidents to prevent the use of compromised certificates in future attacks.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0001 Initial Access	TA0006 Credential Access	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0002 Execution	TA0003 Persistence
T1041 Exfiltration Over C2 Channel	T1588.003 Code Signing Certificates	T1588 Obtain Capabilities	T1505 Server Software Component
T1005 Data from Local System	T1530 Data from Cloud Storage	T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information
T1003 OS Credential Dumping	T1195.002 Compromise Software Supply Chain	T1195 Supply Chain Compromise	T1036 Masquerading
T1204.002 Malicious File	T1204 User Execution		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	0a08d3601636378f0a7d64fd09e4a13b
SHA256	166d1a6ddcde4e859a89c2c825cd3c8c953a86bfa92b343de7e5bfbfb5afb8be, 089573b3a1167f387dcdad5e014a5132e998b2c89bff29bcf8b06dd497d4e63d, 915c2495e03ff7408f11a2a197f23344004c533ff87db4b807cc937f80c217a1
SHA1	8aa3877ab68ba56dabc2f2802e813dc36678aef4
URLs	hxxps[:]//update.cyberlink[.]com/Retail/Promeo/RDZCMSFY1ELY/CyberLink_Pr omeo_Downloader.exe, hxxps[:]//update.cyberlink[.]com/Retail/Patch/Promeo/DL/RDZCMSFY1ELY/Cyb erLink_Promeo_Downloader.exe, hxxps[:]//cldownloader.github[.]io/logo.png, hxxps[:]//i.stack.imgur[.]com/NDTUM.png, hxxps[:]//www.webville[.]net/images/CL202966126.png, hxxps[:]//mantis.jancom[.]pl/bluemantis/image/addon/addin.php, hxxps[:]//zeduzeventos.busqueabuse[.]com/wpadmin/js/widgets/sub/wids.php

References

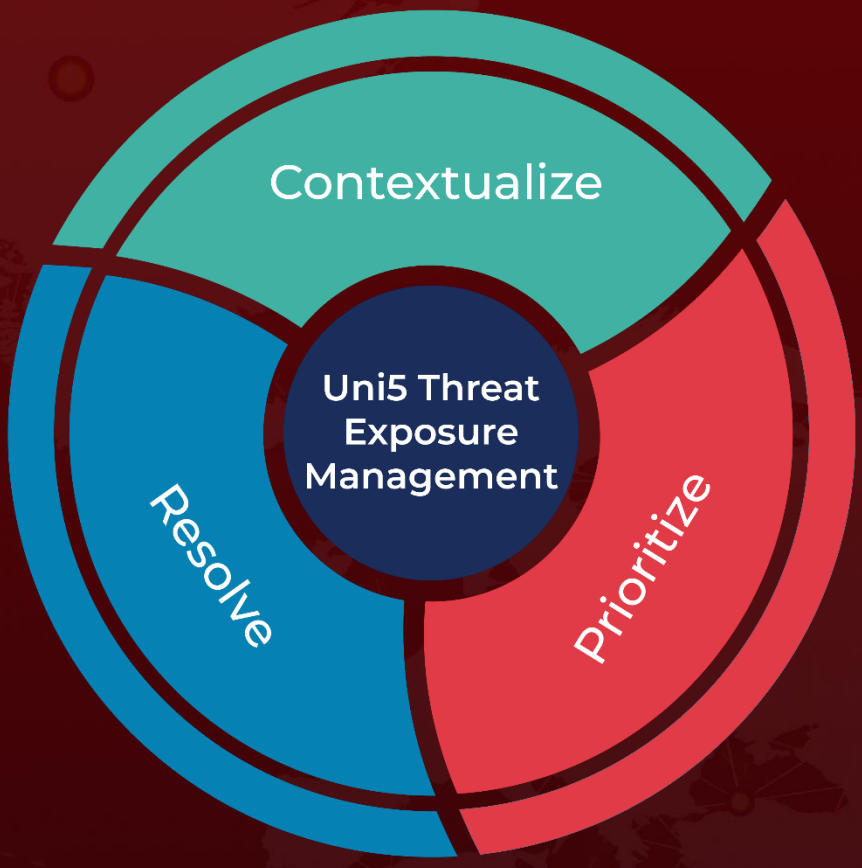
https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/

https://www.hivepro.com/threat-advisory/north-korean-actors-behind-active-exploitation-of-teamcity-vulnerability/

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 24, 2023 . 6:30 AM

More at www.hivepro.com