Hive Pro

THREAT ADVISORY

North Korean state-sponsored threat actor Lazarus Group exploiting Chrome Zero-day vulnerability	TA2022077
Threat Level RED	**Publish Date –** Mar 25, 2022

For more than a month before a fix was available, North Korean state hackers known as Lazarus group exploited a zero-day, remote code execution vulnerability (CVE-2022-0609) in Google Chrome's web browser. The attack mainly targets firms situated in the United States, particularly those in the industries of news media, information technology, cryptocurrency, and finance. However, other organizations and countries are also on the list of attackers.

The campaign begins by sending them phishing emails purporting to be from recruiters at Disney, Google, and Oracle, offering them false employment opportunities. The emails included links to bogus job-search websites such as Indeed and ZipRecruiter. Targets who clicked on the included malicious URLs were infected with drive-by browser malware downloads. The North Korean groups were utilizing an exploit kit (CVE-2022-0609) with hidden iframes embedded into a variety of websites. The attack kit may fingerprint target devices by collecting details like user-agent and screen resolution. After that the exploit kit executes a Chrome remote code execution hack capable of bypassing the lauded Chrome sandbox to move out onto the system.

The Mitre TTPs commonly used by Lazarus Group are:
TA0001: Initial Access
TA0007: Discovery
TA0040: Impact
TA0009: Collection
TA0005: Defense Evasion
TA0003: Persistence
TA0011: Command and Control
TA0042: Resource Development
TA0002: Execution
TA0008: Lateral Movement
TA0006: Credential Access
TA0029: Privilege Escalation
TA0010: Exfiltration
T1134.002: Access Token Manipulation: Create Process with Token
T1098: Account Manipulation
T1583.001: Acquire Infrastructure: Domains
T1583.006: Acquire Infrastructure: Web Services
T1071.001: Application Layer Protocol: Web Protocols
T1010: Application Window Discovery
T1560: Archive Collected Data
T1560.002: Archive via Library
T1560.003: Archive via Custom Method
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1547.009: Boot or Logon Autostart Execution: Shortcut Modification
T1110.003: Brute Force: Password Spraying
T1059.003: Command and Scripting Interpreter: Windows Command Shell
T1543.003: Create or Modify System Process: Windows Service
T1485: Data Destruction
T1132.001: Data Encoding: Standard Encoding
T1005: Data from Local System

T1001.003: Data Obfuscation: Protocol Impersonation
T1074.001: Data Staged: Local Data Staging
T1491.001: Defacement: Internal Defacement
T1587.001: Develop Capabilities: Malware
T1561.001: Disk Wipe: Disk Content Wipe
T1561.002: Disk Wipe: Disk Structure Wipe
T1189: Drive-by Compromise
T1573.001: Encrypted Channel: Symmetric Cryptography
T1048.003: Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
T1041: Exfiltration Over C2 Channel
T1203: Exploitation for Client Execution
T1008: Fallback Channels
T1083: File and Directory Discovery
T1564.001: Hide Artifacts: Hidden Files and Directories
T1562.001: Impair Defenses: Disable or Modify Tools
T1562.004: Impair Defenses: Disable or Modify System Firewall
T1070.004: Indicator Removal on Host: File Deletion
T1070.006: Indicator Removal on Host: Timestomp
T1105: Ingress Tool Transfer
T1056.001: Input Capture: Keylogging
T1036.005: Masquerading: Match Legitimate Name or Location
T1571: Non-Standard Port
T1027: Obfuscated Files or Information
T1588.004: Obtain Capabilities: Digital Certificates
T1566.001: Phishing: Spearphishing Attachment
T1542.003: Pre-OS Boot: Bootkit
T1057: Process Discovery
T1055.001: Process Injection: Dynamic-link Library Injection
T1090.002: Proxy: External Proxy
T1012: Query Registry
T1021.001: Remote Services: Remote Desktop Protocol
T1021.002: Remote Services: SMB/Windows Admin Shares
T1489: Service Stop
T1218.001: Signed Binary Proxy Execution: Compiled HTML File
T1082: System Information Discovery
T1016: System Network Configuration Discovery
T1033: System Owner/User Discovery
T1529: System Shutdown/Reboot
T1124: System Time Discovery
T1204.002: User Execution: Malicious File
T1047: Windows Management Instrumentation

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
Lazarus Group (Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra , Appleworm , APT-C-26 , ATK 3 , SectorA01, ITG03)	North-Korea	Australia, Bangladesh, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam	Aerospace, Defense, Engineering, Financial, Government, Media, Shipping and Logistics, Technology	Information theft and espionage, Sabotage and destruction, Financial crime

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0609	Google Chrome prior to Chrome 98.0.4758.80	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in Animation	CWE-416

Indicators of Compromise (IoCs)

Type	Value
SHA-256	03a41d29e3c9763093aca13f1cc8bcc41b201a6839c381aaaccf891204335685
Domain	disneycareers[.]net, find-dreamjob[.]com, indeedus[.]org, varietyjob[.]com, ziprecruiters[.]org, blockchainnews[.]vip, chainnews-star[.]com, financialtimes365[.]com, fireblocks[.]vip, gatexpiring[.]com, gbclabs[.]com, giantblock[.]org, humingbot[.]io, onlynova[.]org, teenbeanjs[.]com
URLs	https[:]//colasprint[.]com/about/about.asp, https[:]//varietyjob[.]com/sitemap/sitemap.asp, https[:]//financialtimes365[.]com/user/finance.asp, https[:]//gatexpiring[.]com/gate/index.asp, https[:]//humingbot[.]io/cdn/js.asp, https[:]//teenbeanjs[.]com/cloud/javascript.asp,

Patch

https://www.google.com/intl/en/chrome/?standalone=1

References

https://blog.google/threat-analysis-group/countering-threats-north-korea/