Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

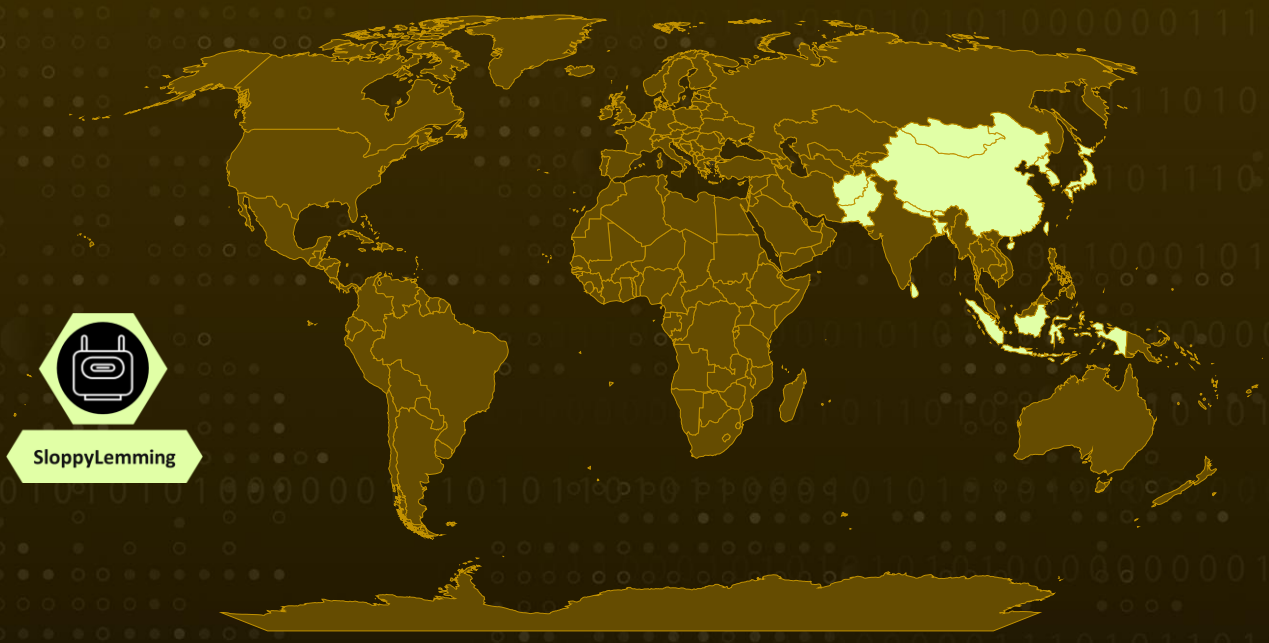
SloppyLemming's Relentless Pursuit of Asian Targets

Date of Publication	Admiralty Code	TA Number
October 4, 2024	A1	TA2024379

Summary

Attack Commenced: 2022
Threat Actor: SloppyLemming (aka Outrider Tiger, Fishing Elephant)
Targeted Countries: Afghanistan, Bangladesh, Bhutan, China, Hong Kong, Indonesia, Japan, Macau, Maldives, Mongolia, Nepal, North Korea, Pakistan, South Korea, Sri Lanka, Taiwan
Targeted Industries: Construction, Defense, Education, Energy, Equipment operators, Foreign Affairs, Government, IT providers, Law enforcement, Legislative, Logistics, Technology, Telecommunications, Textile, Transportation
Attack: SloppyLemming, an advanced threat actor likely originating from India, has been conducting a sophisticated cyberespionage campaign across South and East Asia. Leveraging Cloudflare Workers, they orchestrate a series of malicious activities, including credential theft and malware deployment.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-38831	RARLAB WinRAR Code Execution Vulnerability	WinRAR version 6.22 and older versions	✓	✓	✓

Attack Details

#1 Since late 2022, SloppyLemming, a sophisticated threat actor with origins in India, has systematically exploited Cloudflare Workers as part of a wide-reaching espionage campaign, focusing on South and East Asian nations. Their operations encompass various malicious activities, including credential harvesting, malware deployment, and command-and-control (C2) tactics.

#2 Evidence suggests that SloppyLemming has been active since at least July 2021, with previous campaigns utilizing malware strains like Ares RAT and WarHawk. The group employs advanced adversary emulation frameworks such as Cobalt Strike and Havoc.

#3 Their attack sequence often begins with a phishing email, prompting victims to engage with a malicious link that redirects to a spoofed login portal hosted via a Cloudflare Worker. In one recent campaign, SloppyLemming leveraged Dropbox to store a RAR archive that exploited the WinRAR vulnerability (CVE-2023-38831).

#4 This malicious archive included a decoy PDF, an executable disguised as a PDF, and a DLL designed for side-loading by the executable. While the decoy PDF was displayed to the victim, the executable covertly loaded CRYPTSP.dll, a downloader that retrieved a remote access trojan from Dropbox.

#5 Further demonstrating their technical expertise, SloppyLemming developed a custom tool called CloudPhish, which creates a rogue Cloudflare Worker to log and exfiltrate credentials. In certain attacks, they even used compromised Workers to gather Google OAuth tokens, showcasing their evolving capabilities.

Recommendations

Deploy Advanced Email Security Solutions: Utilize cloud-based email security platforms to protect against phishing attacks, business email compromise (BEC), and other email-borne threats. These solutions often include advanced threat protection features such as sandboxing, URL rewriting, and attachment scanning to detect and block malicious content before it reaches users.

Implement a Zero Trust Architecture: Adopt a Zero Trust security model that operates on the principle of "never trust, always verify." This approach requires strict identity verification for every person and device trying to access resources on your network, regardless of whether they are inside or outside the network perimeter.

Maintain Up-to-Date Software and Systems: Ensure that all systems, especially those running WinRAR and Microsoft products, have the latest security updates installed. Regularly updating software closes vulnerabilities that threat actors like SloppyLemming could exploit. Conduct regular scans to identify and remediate security weaknesses in your infrastructure.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0010** Exfiltration	**TA0011** Command and Control
TA0040 Impact	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1059** Command and Scripting Interpreter
T1204 User Execution	**T1204.002** Malicious File	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading
T1562 Impair Defenses	**T1055** Process Injection	**T1212** Exploitation for Credential Access	**T1580** Cloud Infrastructure Discovery
T1526 Cloud Service Discovery	**T1530** Data from Cloud Storage	**T1105** Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel

T1059.003	T1068	T1499	T1071
Windows Command Shell	Exploitation for Privilege Escalation	Endpoint Denial of Service	Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	storage-e13[.]sharepoint-e13[.]workers[.]dev, mailpitb-securedocs.zapto[.]org, pitb[.]gov-pkgov[.]workers[.]dev, sco.zapto[.]org, mofapak[.]info, confidential.zapto[.]org, humariweb[.]info, modp-pk[.]org, itsupport-gov[.]com, apl-org[.]online, apl-com[.]icu, maldevfudding[.]com, navybd-gov[.]info, adobefileshare[.]com, hurr.zapto[.]org, hascolgov[.]info, helpdesk-lab[.]site, crec-bd[.]site, jammycanonicalupdates[.]cloud, locaal[.]navybd-gov[.]info, openkm[.]paknavy-pk[.]org, cloud[.]adobefileshare[.]com, quran-books[.]store, redzone2[.]apl-org[.]online, hurr[.]zapto[.]org, login[.]apl-org[.]online, owa-spamcheck[.]apl-org[.]online, dawn[.]apl-org[.]online, hit-pk[.]org, blabla[.]apl-com[.]icu, acrobat[.]paknavy-pk[.]org, paknavy-pk[.]org, mail[.]pakistangov[.]com, mail[.]apl-com[.]icu, 168-gov[.]info, browser[.]apl-org[.]online,

TYPE	VALUE
Domain	docs[.]apl-com[.]icu, new[.]apl-org[.]online, mozilla[.]apl-org[.]online, m[.]opensecurity-legacy[.]com, monitor[.]opensecurity-legacy[.]com, sensors[.]opensecurity-legacy[.]com, static[.]opensecurity-legacy[.]com, bin[.]opensecurity-legacy[.]com, api[.]opensecurity-legacy[.]com, frontend-m[.]opensecurity-legacy[.]com, accounts[.]opensecurity-legacy[.]com, opensecurity-legacy[.]com, oil[.]hascolgov[.]info, hesco[.]hascolgov[.]info, locall[.]hascolgov[.]info, updpcn[.]online, update[.]apl-org[.]online, zero-berlin-covenant[.]apl-org[.]online, fonts[.]apl-org[.]online, localhost[.]apl-com[.]icu, cloud[.]cflayerprotection[.]com, secure[.]cflayerprotection[.]com, cflayerprotection[.]com, data[.]cloudlflares[.]com, secure[.]cloudlflares[.]com, cloudlflares[.]com, www[.]cloudlflares[.]com, redzone[.]apl-org[.]online
File Name	CamScanner-06-10-2024-15.29.pdf, CRYPTSP.dll, CamScanner 06-12-2024 15.29.pdf .exe, CIM and IT-Integration.pdf.url, PITB-JR5124.exe, sspicli.dll, profapi.dll, profapis.dll, Outlook.eml/ NekroWire.dll
IPv4	47[.]74[.]10[.]112, 47[.]83[.]23[.]246, 159[.]65[.]6[.]251, 139[.]59[.]109[.]136, 37[.]27[.]41[.]167, 47[.]237[.]105[.]113, 185[.]249[.]198[.]218, 8[.]222[.]235[.]145, 8[.]219[.]169[.]226,

TYPE	VALUE
IPv4	47[.]237[.]20[.]135, 47[.]245[.]56[.]29, 47[.]237[.]20[.]201, 47[.]237[.]25[.]198, 47[.]245[.]2[.]77, 208[.]85[.]22[.]252, 8[.]219[.]114[.]124, 47[.]236[.]65[.]190, 47[.]245[.]114[.]11, 47[.]76[.]61[.]241, 149[.]28[.]153[.]250, 47[.]245[.]42[.]208, 47[.]74[.]84[.]168, 47[.]74[.]87[.]155, 159[.]253[.]120[.]25, 207[.]148[.]73[.]145, 47[.]254[.]229[.]56, 47[.]76[.]181[.]76, 47[.]245[.]126[.]218, 142[.]93[.]139[.]164, 45[.]137[.]116[.]8
SHA256	fb4397c837c7e401712764f953723153d5bb462bc944518959288ea47dec6446, 95cf90b2610c6f0ec67c1d669cd252468f6c3b8eaeea588f342d2bd74d90e093, 337ca61e23bcb86f26dc40a36316621b74ec6f29a55820899ed30b03b69a6025, b6ae5b714f18ca40a111498d0991e1e30cd95317b4904d2ef0d49937f0552000, e3bc0246ab95b527aa86e52e62f554ab8db04523f35aee50b508d0fa48ab49f7, b53c7b13a4af47c3976bfad63fe9c5fd988dc0807dd040e8d63d790b65394afb, 06f82a8d80ec911498e3493ebefa8ad45e102dd887ce2edc11f8f51bafab2e80, ac3dff91982709f575cfbc6954b61130b4eeab5d3759772db220f1b76836be4d, 3dfb8d198de95090e2ad3ffc9d9846af5c3074563acb0ce5b0ef62b20e4bf432, 82e99ceea9e6d31555b0f2bf637318fd97e5609e3d4d1341aec39db2e26cf211
URL	hxxps[:]//mail-na-gov-pk[.]na-gov-pk[.]workers[.]dev/api/login, hxxps[:]//zoom[.]osutuga7[.]workers[.]dev/authenticate

Patch Details

Upgrading to WinRAR version 6.23 or later is highly recommended.

References

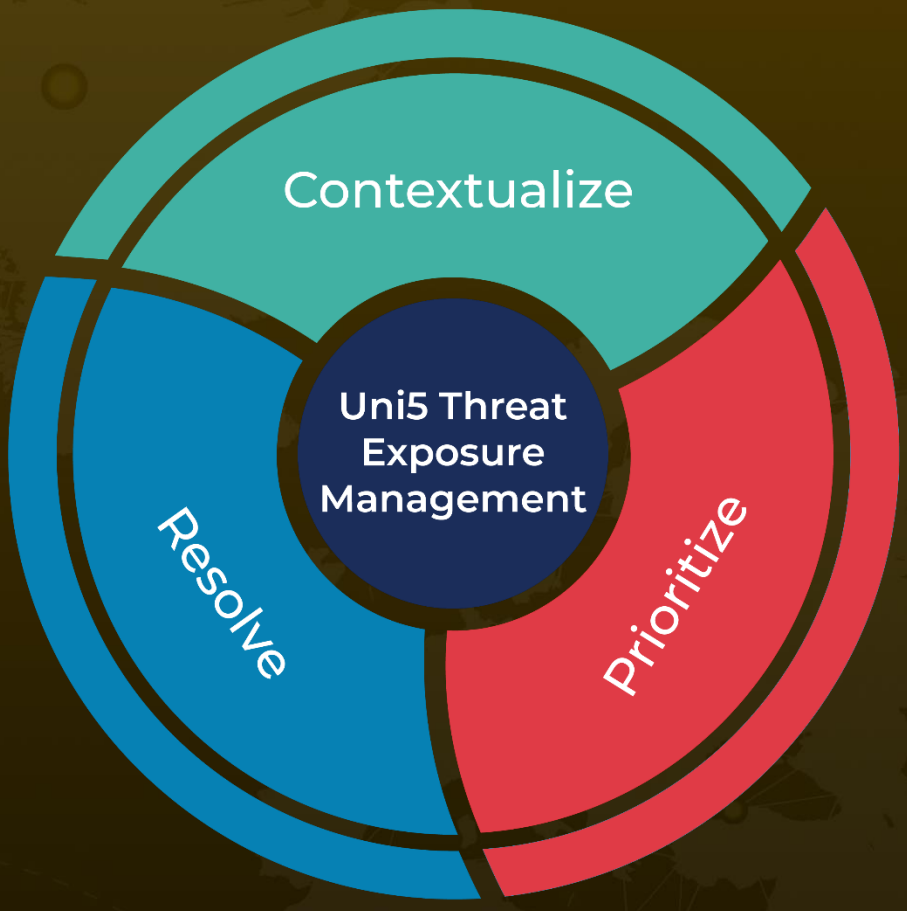
https://www.cloudflare.com/en-in/threat-intelligence/research/report/unraveling-sloppylemmings-operations-across-south-asia/

https://hivepro.com/threat-advisory/winrar-zero-day-exploit-targeting-traders-since-april/

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 4, 2024 . 8:00 AM

More at www.hivepro.com