مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

LummaC2 Malware Campaign Targeting Organizations

Tracking #:432317295

Date:22-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an ongoing LummaC2 infostealer malware campaigns targeting organizations to exfiltrate sensitive credentials, financial data, and personal identifiers.

TECHNICAL DETAILS:

Recent intelligence indicates active campaigns targeting organizations worldwide, with the aim of exfiltrating sensitive information such as credentials, financial data, and personal identifiers. LummaC2 is distributed primarily via phishing emails and malicious downloads, employing advanced evasion techniques to bypass detection and maximize impact.
Entities across government, energy, finance, transportation, and healthcare sectors should assume elevated risk and take immediate steps to mitigate exposure. This advisory provides technical details, actionable recommendations, and indicators of compromise (IOCs) to support detection and response.

LummaC2 Overview:

- First observed in 2022, LummaC2 is sold on cybercriminal forums and is frequently updated.
- Delivered via spearphishing emails (malicious attachments or links) and fake software downloads.
- Employs fake CAPTCHAs to trick users into executing malware via clipboard and Windows Run commands.
- Runs primarily in memory, minimizing disk artifacts and evading traditional antivirus/EDR solutions.
- Exfiltrates browser data, credentials, cryptocurrency wallets, and MFA details.
- Communicates with command-and-control (C2) servers using encrypted POST requests and JSON payloads.
- Can receive commands to steal files, download additional payloads, take screenshots, or self-delete.

MITRE ATT&CK Tactics and Techniques for LummaC2 Malware

Initial Access

- Phishing (T1566):
  Threat actors delivered LummaC2 malware through phishing emails.
- Phishing: Spearphishing Attachment (T1566.001):
  Threat actors used spearphishing attachments to deploy LummaC2 malware payloads.
- Phishing: Spearphishing Link (T1566.002):
  Threat actors used spearphishing hyperlinks to deploy LummaC2 malware payloads.

Defense Evasion

- Obfuscated Files or Information (T1027):
  Threat actors obfuscated the malware to bypass standard cybersecurity measures.
- Masquerading (T1036):
  Threat actors delivered LummaC2 malware via spoofed software.
- Deobfuscate/Decode Files or Information (T1140):
  Threat actors used LummaC2 malware to decrypt its callback C2 domains.

Discovery

- Query Registry (T1012):
  Threat actors used LummaC2 malware to query the user's name and computer name via APIs.
- Browser Information Discovery (T1217):
  Threat actors used LummaC2 malware to steal browser data.

Collection

- Automated Collection (T1119):
  LummaC2 malware has automated collection of various information including cryptocurrency wallet details.

Command and Control

- Application Layer Protocol: Web Protocols (T1071.001):
  Threat actors used LummaC2 malware to attempt POST requests.
- Ingress Tool Transfer (T1105):
  Threat actors used LummaC2 malware to transfer a remote file to compromised systems.

Exfiltration

- Exfiltration (TA0010):
  Threat actors used LummaC2 malware to exfiltrate sensitive user information, including credentials, wallets, browser extensions, and MFA details.
- Native API (T1106):
  Threat actors used LummaC2 malware to download files with native OS APIs.

Indicators of Compromise (IOCs)

Hash Type	Hash Value
MD5	4AFDC05708B8B39C82E60ABE3ACE55DB
MD5	E05DF8EE759E2C955ACC8D8A47A08F42
MD5	C7610AE28655D6C1BCE88B5D09624FEF
SHA1	1239288A5876C09D9F0A67BCFD645735168A7C80
SHA1	B66DA4280C6D72ADCC68330F6BD793DF56A853CB
TLSH	3B267FA5E1D1B18411C22E97B367258986E871E5
SHA256	19CC41A0A056E503CC2137E19E952814FBDF14F8D83F799AEA9B96ABFF11EFBB
SHA256	2F31D00FEEFE181F2D8B69033B382462FF19C35367753E6906ED80F815A7924F
SHA256	4D74F8E12FF69318BE5EB383B4E56178817E84E83D3607213160276A7328AB5D
SHA256	325daeb781f3416a383343820064c8e98f2e31753cd71d76a886fe0dbb4fe59a
SHA256	76e4962b8ccd2e6fd6972d9c3264ccb6738ddb16066588dfcb223222aaa88f3c
SHA256	7a35008a1a1ae3d093703c3a34a21993409af42eb61161aad1b6ae4afa8bbb70
SHA256	a9e9d7770ff948bb65c0db24431f75dd934a803181afa22b6b014fac9a162dab
SHA256	b287c0bc239b434b90eef01bcbd00ff48192b7cbeb540e568b8cdcdc26f90959
SHA256	ca47c8710c4ffb4908a42bd986b14cddcca39e30bb0b11ed5ca16fe8922a468b

Observed Malicious Domains- The domains below are historical in nature and may not currently be malicious

pinkipinevazzey[.]pw	fragnantbui[.]shop	medicinebuckerrysa[.]pw
musicallyageop[.]pw	stogeneratmns[.]shop	wallkedsleeoi[.]shop
tirechinecarpet[.]pw	reinforcenh[.]shop	reliabledmwqj[.]shop
musclefarelongea[.]pw	forbidstow[.]site	gutterydhowi[.]shop
fanlumpactiras[.]pw	computeryrati[.]site	contemteny[.]site
ownerbuffersuperw[.]pw	seallysl[.]site	dilemmadu[.]site
freckletropsao[.]pw	opposezmny[.]site	faulteyotk[.]site
hemispheredodnkkl[.]pw	goalyfeastz[.]site	authorizev[.]site
ghostreedmnu[.]shop	servicedny[.]site	blast-hubs[.]com
offensivedzvju[.]shop	friendseforever[.]help	blastikcn[.]com
vozmeatillu[.]shop	shiningrstars[.]help	penetratebatt[.]pw
drawzhotdog[.]shop	mercharena[.]biz	pasteflawwed[.]world
generalmills[.]pro	citywand[.]live	hoyoverse[.]blog
nestlecompany[.]pro	esccapewz[.]run	dsfljsdfjewf[.]info
naturewsounds[.]help	travewlio[.]shop	decreaserid[.]world
stormlegue[.]com	touvrlane[.]bet	governoagoal[.]pw
paleboreei[.]biz	calmingtefxtures[.]run	foresctwhispers[.]top
tracnquilforest[.]life	sighbtseeing[.]shop	advennture[.]top
collapimga[.]fun	holidamyup[.]today	pepperiop[.]digital
seizedsentec[.]online	triplooqp[.]world	easyfwdr[.]digital
strawpeasaen[.]fun	xayfarer[.]live	jrxsafer[.]top
quietswtreams[.]life	oreheatq[.]live	plantainklj[.]run
starrynsightsky[.]icu	castmaxw[.]run	puerrogfh[.]live
earthsymphzony[.]today	weldorae[.]digital	quavabvc[.]top
citydisco[.]bet	steelixr[.]live	furthert[.]run
featureccus[.]shop	smeltingt[.]run	targett[.]top
mrodularmall[.]top	ferromny[.]digital	ywmedici[.]top
jowinjoinery[.]icu	rodformi[.]run	legenassedk[.]top
htardwarehu[.]icu	metalsyo[.]digital	ironloxp[.]live
cjlaspcorne[.]icu	navstarx[.]shop	bugildbett[.]top
latchclan[.]shop	spacedbv[.]world	starcloc[.]bet
rambutanvcx[.]run	galxnetb[.]today	pomelohgj[.]top
scenarisacri[.]top	jawdedmirror[.]run	changeaie[.]top
lonfgshadow[.]live	liftally[.]top	nighetwhisper[.]top
salaccgfa[.]top	zestmodp[.]top	owlflright[.]digital
clarmodq[.]top	piratetwrath[.]run	hemispherexz[.]top
quilltayle[.]live	equatorf[.]run	latitudert[.]live
longitudde[.]digital	climatologfy[.]top	starofliught[.]top

RECOMMENDATIONS:

1. Strengthen Email and Endpoint Security
   - Deploy advanced email filtering to block phishing attempts and malicious attachments/links.
   - Ensure endpoint protection solutions are up-to-date and capable of detecting fileless malware and PowerShell-based threats.
2. User Awareness and Training
   - Conduct regular training to educate staff on phishing recognition and safe handling of email attachments and links.
   - Encourage immediate reporting of suspicious emails or system behavior.
3. Network and System Hardening
   - Monitor for anomalous outbound network traffic, especially to suspicious domains (mentioned IOCs above).
   - Restrict user privileges, limiting the ability to run unauthorized software or scripts.
   - Apply the principle of least privilege and enforce strong authentication (MFA) wherever possible.
4. Patch and Vulnerability Management
   - Ensure all operating systems and applications are fully patched, especially those commonly targeted by malware.
5. Incident Response Preparedness
   - Review and update incident response plans to ensure rapid detection, containment, and eradication of malware.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141b