KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Evolution of ChromeLoader becomes a prevalent threat

Tracker ID: TN0923 **Date:** 26/Sep/2022 **Category:** Malware **Industry:** All **Region**: All

Background

A widespread ChromeLoader malware operation that dumps malicious browser add-ons, Node-WebKit malware, and even ransomware has been discovered. Several cyberattacks on organizations in the business services, education, government, healthcare, and other critical sectors have emerged. ChromeLoader infections surged in Q1 2022, raising awareness of the browser hijacker's threat. The infection begins when a victim installs unauthorized software or is tricked into scanning a QR code on malicious websites. The malware installs a malicious extension on Chrome that redirects user traffic to advertising websites, allowing the threat actors to profit from click fraud.

ChromeLoader recently acquired an information-stealing capability and is now attempting to steal browser data while maintaining its advertising capabilities. It is allegedly being used to infect users with other malware by a threat actor identified as DEV-0796 as part of a "ongoing large click fraud operation." Malicious advertising, browser redirects, and YouTube video comments spread the infection via ISO files. Four commonly found files in ChromeLoader ISOs are an ICON file, a batch file (usually called Resources.bat) that installs malware, and a Windows shortcut that starts the batch program. When a victim opens the ISO file, it will install Node-Webkit (NW.js) or a browser extension. DMG files were also used, implying cross-platform activity.

Since the malware's initial appearance earlier this year, its developers have released multiple versions, many of which contain various dangerous features. One of these is a variant known as Bloom.exe, which originally appeared in March and has infected at least 50 VMware Carbon Black users since then. Malware is used to steal sensitive information from compromised devices. Another application imitates OpenSubtitles, a tool that connects users to subtitled TV shows and movies. In this campaign, the threat actors replaced their typical "Resources.bat" file with a file named "properties.bat," which is used to install malware and establish persistence by adding Registry keys.

The Flbmusic.exe variant, which recently mimicked the FLB Music player, included an Electron runtime and allowed the virus to load extra modules for network connection and port snooping. Some variants of the attacks take a more destructive turn, ejecting ZipBombs that overwhelm the system with a massive unpacking procedure. The ZipBomb is deployed together with the first infection when a user downloads an archive. The user must double-click to activate the ZipBomb. When the malware is triggered, it floods the user's machine with data, causing it to crash. Concerningly, recent ChromeLoader variations have been found to encrypt data with the Enigma malware. The obsolete ransomware strain Enigma may be launched directly from the browser's default browser owing to an embedded executable and a JavaScript-based installer. After encrypting the data, the ransomware appends the ".enigma" file extension and dumps a "readme.txt" file containing instructions for the victims.

Adware is often ignored or minimized by investigators since it causes little harm to victims' systems other than using bandwidth. However, because its developers may release updates that allow for more aggressive monetization, every piece of software that covertly inserts itself into systems is a potential source of bigger issues. ChromeLoader originated as adware, but it is a perfect example of how threat actors are experimenting with increasingly powerful payloads in search of more lucrative alternatives to advertising fraud.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Evolution of ChromeLoader becomes a prevalent threat

Tracker ID: TN0923 **Date:** 26/Sep/2022 **Category:** Malware **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Defense Evasion, Persistence, Execution, Exfiltration and Command and Control.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Validate the IOCs attached and implement the detection & prevention accordingly. Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Keep systems and products updated as soon as possible after the patches are released. Ensure latest patches are applied to internet-facing VMware Horizon servers.
- Identify and block extensions vulnerable to JavaScript injection. Fetch the installed extensions from devices exhibiting malicious behavior and remove them from the user's device.
- Do not download a file from an unknown website without verifying its legitimacy. Monitor time series of user activity to detect Compromised User Accounts.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically.
- Check reviews, developer information, extension permissions and anything else of note before installing a new extension to your browser. Do not launch ISO files unless they are from a trusted source.

References

- Abe Schneider, Bethany Hardin, Lavine Oluoch, The Evolution of the Chromeloader Malware, Vmware, 19th September 2022, External Link (vmware.com)
- Bill Toulas, VMware, Microsoft warn of widespread Chromeloader malware attacks, Bleeping Computer, 19th September 2022, External Link (bleepingcomputer.com)
- Jai Vijayan, ChromeLoader Malware Evolves into Prevalent, More Dangerous Cyber Threat, Dark Reading, 21st September 2022, External Link (darkreading.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Evolution of ChromeLoader becomes a prevalent threat

Tracker ID: TN0913 **Date:** 26/Sep/2022 **Category:** Malware **Industry:** All **Region**: All

* Hash MD5	Hash SHA256	Hash SHA1	Domain	URL	IP
b5299e2413104b4b034ea8eeca0c9c74	18b8ab327177cbde47867694d3d7acb93c83237d2418271f1020fe943760c026	a5625269e2d817258ad60044f853040e95d58b47	oughsheukwa[.]autos	pontymonti[.]com/?tid=952736	104.21.70.206
d6c317db29bb1ae07393e907d85d6fc5	23f30fa4e9fe3580898be54f8762f85d5098fd526a51183c457b44822446c25a	0b4de1c09fe978152e9ec642f0d9b86ec262849a	ukizeiasnin[.]com	iminatedm[.]com/?tid=952736	172.67.139.75
e3419bc93be8f385714d0970f0175d17	276f4008ce6dcf867f3325c6b002950cbd0fdb5bf12dc3d3afb1374622820a4e	6A84FE906EBBEED933D7776731FE7118E1E028C1	yrecomemul[.]xyz	kookimookin[.]com/?tid=952736	172.67.218.221
430c83f15bb5a769dd99c094bb89460e	309c87b34966daecd05c48b787c3094eeed85b5f23ec93b20fc9cdbf8ff9b586	B7CD274E9C4036DC3F27D347A8428B40437A7AFA	tooblycars[.]com	hemicalcov[.]com/?tid=952736	104.21.51.237
c219e8b59c8c98e962d28942799902e5	47c65ef4d6b0ffe7109c588e04575dcf05fdf3afe5796078b4f335cb94c438b7		texceededon[.]autos	ernedassiu[.]com/?tid=952736	172.67.191.177
91ad76c368bc3c6c0d8c65a2a5234ac1	502a8d1e95c21b5dc283ef4877ca2fe2ba41570bd813c47527fca2fb224d5380		ymenthejuiasq[.]xyz	lamagamabanma[.]com/?tid=952736	
0a2a70d618d85067359813849dcec49d	5e6b5a9c0849db8ca0696a16c882d6945a62e419bd646f23d4d00533bbe9bca5		koooblycar[.]com	ainoutweil[.]com/?tid=952736	
02e0745a7c6a2a71d9698b67565ab2c9	6e0cb7518874437bac717ba1888991cee48dfaca4c80a4cbbbe013a5fe7b01a6		rooblimyooki[.]com	amajorinrye[.]com/?tid=952736	
0a80192cb1f31ef0a9d48932510f6956	83cf9d2244fa1fa2a35aee07093419ecc4c484bb398482eec061bcbfbf1f7fea		Yooblygoobnku[.]com	announcem[.]com/?tid=952736	
f0d2f196641475d32fc693408276bbaf	87f0416410ac5da6fd865c3398c3d9012e5488583b39edacd37f89bc9469d6a9		ringhereny.autos	ationwindon[.]com/?tid=952736	
0a18fedce42f4f3199a53351dbb516d9	c6a68fac895c0b15d5cbbba63f208e5b0a6f3c1d2382b9465375d1794f447ac5		ableawid[.]com	bamagamalama[.]com/?tid=952736//	
121300cd7050da8a1debf684f03ba05a	c7aedc8895e0b306c3a287995e071d7ff2aa09b6dac42b1f8e23a8f93eee8c7a		airplanegoobly[.]com	bambluagamgona[.]com/?tid=952736	
aa87459333436eb4743e9d04ab4596b8	d374ef30aa17f8bad0fb88d0da47f4038669c340d4c7fc2ff65055b07c17fdf65		baganmalan[.]com	bookhogookhi[.]com/?tid=952736	
e0de995d9d4c395c741f9a5e00f9517f	dfc90f64139b050cf3c72d833e1a7915af1bd689ece7222b9ac2c8426a0bfd0a		balljoobly[.]com	booklilihooli[.]com/?tid=952736	
6d92ff0d3d8b71c4ab874357691f2d97	2d4454d610ae48bf9ffbb7bafcf80140a286898a7ffda39113da1820575a892f		balokyalokd[.]com	briolenpro[.]com/?tid=952736	
5ed2d89e9d05054beeebcf4a7928c4a3	8840f385340fad9dd452e243ad1a57fb44acfd6764d4bce98a936e14a7d0bfa6		boogilooki[.]com	cangomamblu[.]com/?tid=952736	
6b21699f37ff383fb76a6112f2cdd400	1c0254f0f811aadd6f1dad1cc5926f6b32fa2fb0866c35bf6a9f3dfad25fd9ca		bookimooki[.]com	cessfultrai[.]com/?tid=952736	
504dc8de41fa942ed7c174b6111c0a0d	b43767a9b780ba91cc52954aa741be1bddb0905b492e481aea992bca2a0c6a93		carfunusme[.]com	chookamookla[.]com/?tid=952736	
97f1f83a0b89078815c537bcce41988d	ad68453553a84e03c70106b7c13a483aa9ff1987621084e22067cb1344f52ab7		carmoobly[.]com	choonamoona[.]com/?tid=952736	
fd1aced8d4abc14f8b7db3d2f27260ff	cd999181de69f01ec686f39ccf9a55131a695c55075d530a44f251a8f41da7c8		chairtookli[.]com	ddenknowl[.]com/?tid=952736	
f129ba4a71ae3900bcf423ef7ed36629	3fc00a37c13ee987ec577a8fd2c9daae31ec482c5276208ddff4bc5cb518c2f3		chookiebooki[.]com	dingcounc[.]com/?tid=952736	
f90a4f01c6a411849e8a6f8ba095a79e	e132de4b3b6b6135121c809e43c0adf3ebf10cb92e7b3c989c24c68ed970a6e6		choopinookie[.]com	eavailand[.]com/?tid=952736	
01d2c774ff0e62fdc48e72d0e643bfa5	03b2f267de27dae24de14e2c258a18e6c6d11581e6caee3a6df2b7f42947d898		ckgrounda[.]com	edconside[.]com/?tid=952736	
db5dc933158fc078c4383f8b4aca40ed	e449eeade197cab542b6a11a3bcb972675a1066a88cfb07f09e7f7cbd1d32f6d		computermookili[.]com	edstever[.]com/?tid=952736	
231a5f0b8cb2c9d00cc9f0bd2abb52be	785f4ee0b26aac97429cdf99b04d2dab44798f2554b61512b49b59f834e91250		dubifunme[.]com	emblyjustin[.]com/?tid=952736	
409fa7b1056bef4b3c6dc096d583c784	e1f9968481083fc826401f775a3fe2b5aa40644b797211f235f2adbeb0a0782f		dudesurfbeachfun[.]com	eningspon[.]com/?tid=952736	
3826683a0bef0db1d05c513f75fd8f91	0ecbe333ec31a169e3bce6e9f68b310e505dedfed50fe681cfd6a6a26d1f7f41		exkcellent[.]com	erdecisesgeorg[.]info/?tid=952736	
9f561838f84712622af0fc75267fc4ed	1717de403bb77e49be41edfc398864cfa3e351d9843afc3d41a47e5d0172ca79		funbeachdude[.]com	foogimooogin[.]com/?tid=952736	
d0b0b87b68f6a93b8d1ca79afdc72e9d	18073ce19f3391f82c649a244b5555a88124fb6f496c28a914aa0f4ce139e3f2		ketobepar[.]com	ghtdecipie[.]com/?tid=952736	
9c385255dcff360d39ca1992381634b8	1b4786ecc9b34f30359b28f0f89c0af029c7efc04e52832ae8c1334ddd2b631e		koobIniplay[.]com	hoolibadullli[.]com/?tid=952736	
09176b26b7e5683079d87c2ef1de757a	2e006a8e9f697d8075ba68ab5c793670145ea56028c488f1a00b29738593edfb		letfunhapeme[.]com	horticaldist[.]fun/?tid=952736	
91e5f9a599ab8078545988ecf7a93a51	31b2944fb4d13a288497e64b2c4a110127e3f685fae38860aaf68336f7804d13		lookiroobi[.]com	kookichoopi[.]com/?tid=952736	
9efee5f3f1bf4422ae1f74cc98f4fa34	3927e4832dcbfae7ea9e2622af2a37284ceaf93b86434f35878e0077aeb29e7e		lookitoogi[.]com	lidibidiredi[.]com/?tid=952736	
a2e3dd6316556f51be5dddd01fac8d58	41cc04487a80093df4ac9bb64afc44eb6492bb49fc125b4601cd53476f18d5a4		madorjabl[.]com	likomokiowoki[.]com/?tid=952736	
b67845f90fac96fe1339f890682ec572	614e2c3540cc6b410445c316d2e35f20759dd091f2f878ddf09eda6ab449f7aa		malanbagam[.]com	lookofookomooki[.]com/?tid=952736	
5f8e41b663cc77f0a364f4c57bafc7f9	66f2ade2a78843c91445f808673d6ae0fe3a13402faac2962f04544a62ffbc2d		mokkilooki[.]com	loopychoopi[.]com/?tid=952736	
f0229ff91258a5a370b9e9ae5ac92f69	6d89c1cd593c2df03cdbd7cf3f58e2106ff210eeb6f60d5a4bf3b970989dee2e		myeducatio[.]com	luublimaluulo[.]com/?tid=952736	
0a59769bf69481db464c43a3ce65d039	9ab4665f627e17377f7feda1d3ca4facb5448db587d4d22d2740585ab3fb1f54		nakasulba[.]com	luulibalulI[.]com/?tid=952736	
98e0e2863f411c6d2b7a5acabc9f234f	9dd11c756bdf612f372f3d37410bcc469f586f2fc826df5c679b3e77501c9371		ndinterper[.]com	luulibalulI[.]com/?tid=952736=3	
be81b596d84350d0d55fb5f28514a243	a9670d746610c3be342728ff3ba8d8e0680b5ac40f4ae6e292a9a616a1b643c8		ndworldwi[.]com	mambkooocango[.]com/?tid=952736	
3c8226b24f3197cbdca5b811e9627a0e	bcc6cfc82a1dc277be84f28a3b3bb037aa9ef8be4d5695fcbfb24a1033174947		nookiespooti[.]com	mamblubamblua[.]com/?tid=952736	
90195a912807bd27e413001755210998	dd2da35d1b94513f124e8b27caff10a98e6318c553da7f50206b0bfded3b52c9		oempafnyfi[.]com	mesucces[.]top/?tid=952736	
8724955c260a3b6aa61ca52a2e9a1fc4	fb9cce7a3fed63c0722f8171e8167a5e7220d6f8d89456854c239976ce7bb5d6		saveifmad[.]com	miookilOogif[.]com/?tid=952736	
3b6c81eac226274ca6fdd98b688a9d15	9eca0cd45c00182736467ae18da21162d0715bd3d53b8df8d92a74a76a89c4a0		siwoulukdli[.]com	moekyepkd[.]com/?tid=952736	
239d5148370fb74a2e6afb276e2438b6	564e913a22cf90ede114c94db8a62457a86bc408bc834fa0e12e85146110c89b		slootnI[.]com	mokklachookla[.]com/?tid=952736	
89867c4e2243faddb8e4004dcb8aee2d	c56139ea4ccc766687b743ca7e2baa27b9c4c14940f63c7568fc06495214307		sonalskills[.]com	montikolti[.]com/?tid=952736	
746cf2d6f71aa8ed5405abf2ba8b82bf	53347d3121764469e186d2fb243f5c33b1d768bf612cc923174cd54979314dd3		tabletoobly[.]com	mooogInnumit[.]com/?tid=952736	
979381a3df54ea9db90308cde4ba4aca	44464fb09d7b4242249bb159446b4cf4c884d3dd7a433a72184cdbdc2a83f5e5		toogimoogi[.]com	motoriesml[.]com/?tid=952736	
859b78f3b7c1a6888eed6e63f3d081e4	afc8a5f5f8016a5ce30e1d447c156bc9af5f438b7126203cd59d6b1621756d90		toukfarep[.]com	mworkhovd[.]com/?tid=952736	
ce163bd544fc7bbf1ccaf9ff80c0a21f	2d4454d610ae48bf9ffbb7bafcf80140a286898a7ffda39113da1820575a892f		uiremukent[.]com	nkingwitheа[.]com/?tid=952736	
5b46680db17ff396e7250307964c9969	ded20df574b843aaa3c8e977c2040e1498ae17c12924a19868df5b12dee6dfdd		ukrawinrusyes[.]com	ntconcert[.]com/?tid=952736	
8c3e85a06704767fc7f47b1f9efe41c7	5f57a4495b9ab853b9d2ab7d960734645ebe5765e8df3b778d08f86119e1695c		utfeablea[.]com	nuumitgooblI[.]com/?tid=952736	
2129c5e739575951c33c8f69a3418815	187e08fca3ea9edd8340aaf335bd809a9de7a10b2ac14651ba292f478b56d180		voobmijump[.]com	opositeass[.]com/?tid=952736	
c6b952b2410ab86c126216d302bc3e5a	5c07178b0c44ae71310571b78dde5bbc7dc8ff4675c20d44d5b386dfb4725558		xoomitsleep[.]com	redibidilidi[.]com/?tid=952736	
aa1a0458653a0fd5621267109bcc5d6e	42afb7100d3924915fde289716def039cd14d8116757061df503874217d9b047		yalfnbagan[.]com	rokitokijokI[.]com/?tid=952736	
c105df325566c8b374649c74d35908d4	2df0cf38c80397450f0341fc679d1dd7a066ec0d2e687c6914d2a2256f945d96d		yalokmalos2[.]com	sopertyvalua[.]com/?tid=952736	
6986f8348b7fab32560198704510f8a6	aed9351ff414ddf1ecbfeb747b0bc6d650fcf026290cb670cbbaaad02fdf3dcd		yescoolservmate[.]com	tokijokoloki[.]com/?tid=952736	
1305ee449cc0230c98e4e1301da81698	dca529c6ec9ea1f638567d5b6c34af4f47a80c0519178c4829becc337db5be02		yourretyeq[.]com	undencesc[.]com/?tid=952736	
08dc5ad1b6cc00e129526b9054a06e4e	860c1f6f3393014fd84bd29359b4200027274eb6d97ee1a49b61e038d3336372		hxxps[://learnataloukt[.]xyz	undencesc[.]com/?tid=952736/	
31d63653666646a46742257004229203	0fb038258bbbc61d4f43cac585ec92c79a9a231bcd265758c23c78f96ac1dbb2		hxxps[://brokenna[.]work	vehavings[.]biz/?tid=952736	
421b03d5b3f8136c7b959c560c074767	1dbe5c2feca1706fafc6f767cc16427a2237ab05d95f94b84c287421ec97c224		hxxps[://yflexibilituky[.]co	vementalc[.]xyz/?tid=952736	
	8193040c9da90dc7c22cf84b227c147cf0c92e7eecbc7f4a890e7ca6fd680ca3		hxxps[://ktyouexpec[.]xyz	yabloomambloo[.]com/?tid=952736	
	2f00d7cd954bcb1fffdc3f14fde7f239b4eb3aecc9f6ac24540ed25856969f33		hxxps[://withyourret[.]xyz	ystemgthr[.]com/?tid=952736	
			hxxps[://]bosscast[.]net	hxxps://$d/e?iver=$iv&u=$u&is=$is&ed=$di	
			hxxps[://soap2day[.]ac	hxxps://$d/e?iver=$iv&did=$dd&ver=$ver&ed=$di	
			hxxps[://wallpaperaccess[.]com	hxxps://$d/err?iver=$iv&did=$dd&ver=$ver	
			hxxps[://uploadhaven[.]com	hxxps://$dl/err?iver=$iv&u=$u&is=$is	
			hxxps[://steamunlocked[.]net	hxxps://$d/x?u=$u&is=$is&lv=$lv&rv=$v	
			hxxps[://]etterismype[.]co		

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia