Vidar Info-Stealer Malware Distributed via Malvertising on Google

D darktrace.com/blog/vidar-info-stealer-malware-distributed-via-malvertising-on-google

31

Jan 2023

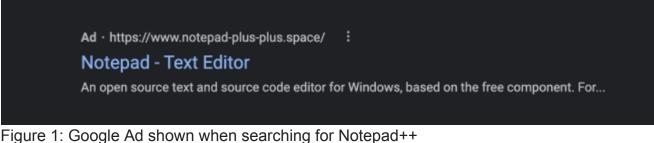
31

Jan 2023

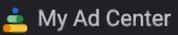
In recent weeks, security researchers and cyber security vendors have noted an increase in malvertising campaigns on Google, aimed at infiltrating info-stealer malware into the systems of unsuspecting victims, as reported in sources ^{[1] [2]}. It has been observed that when individuals search for popular tools such as Notepad++, Zoom, AnyDesk, Foxit, Photoshop, and others on Google, they may encounter ads that redirect them to malicious sites. This report aims to provide a high-level analysis of one such campaign, specifically focusing on the delivery of the Vidar Info-stealer malware.

Campaign Details

On the 25th of January 2023, Darktrace researchers observed that the advertisement depicted in Figure 1 was being displayed on Google when searching for the term "Notepad++" from within the United States.



As can be seen in Figure 2, the advertisement in question had no visible information regarding its publisher.



P Report ad

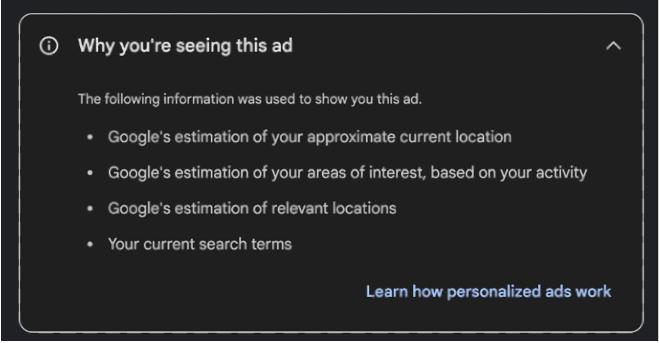
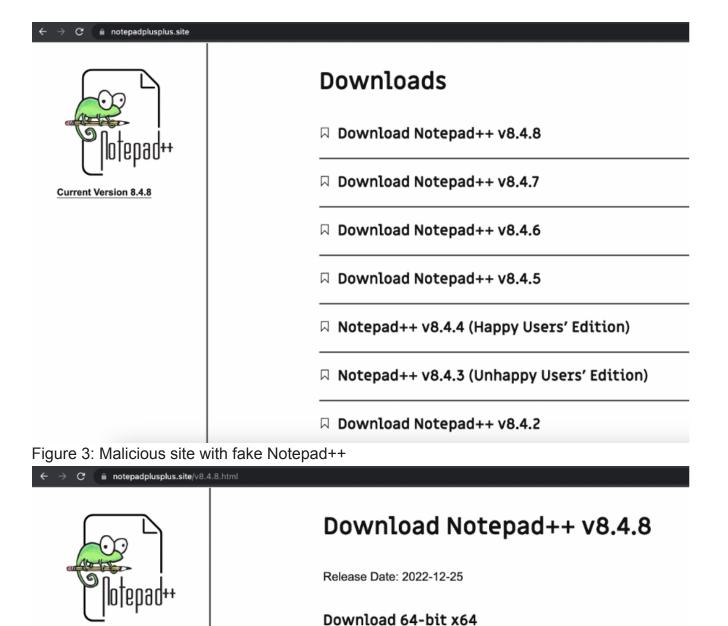


Figure 2: Advertisement information

Clicking on the advertisement would direct potential victims to the website notepadplusplus.site, which had been registered on the 4th of January and is hosted on IP address 37.140.192.11. Upon selecting the desired version of the software, a download button is presented to the visitor.

×



Current Version 8.4.8



Figure 4: Malicious site with fake Notepad++

When clicking on Download, regardless of the version selected, the traffic is then redirected to https://download-notepad-plus-plus.duckdns.org/, and a .zip file with name "npp.Installer.x64.zip" is downloaded.

×	Headers	Preview	Response	Initiator	Timing			
▼ G	ieneral							
	Request URL: https://notepadplusplus.site/asdasdasd/asda2qwd/download.php							
	Request Method: GET							
	Status Cod	le: 😑 302						
	Remote Ad	dress: 37.	140.192.11:	443				
	Referrer Po	o <mark>licy:</mark> stric	t-origin-wh	en-cross-	-origin			
▼ R	Response Headers							
	content-ler	ngth: 0						
	content-typ	be: text/ht	tml; charset	=UTF-8				
	date: Wed,	25 Jan 20	23 11:40:04	GMT				
	location: h	ttps://dow	vnload-notep	ad-plus-	plus.duckdns.org/			
	server: ngi	inx						
	x-powered	-by: PHP/8	.0.17					

Figure 5: Traffic redirection

Upon extraction, the file "npp.Installer.x64.exe" has a file size of 684.1 megabytes. The significant size is attributed to the inclusion of an excessive number of null bytes, which serve to prevent the file from being scanned by some Antivirus and uploaded to malware analysis platforms such as VirusTotal, which has a file size limit of 650 megabytes.

🌉 npp.Installer.x64.zip		- 🗆 X
File Commands Tools Favorites Option	s Help	
Add Extract To Test View D	relete Find Wizard Info	
↑ mpp.Installer.x64.zip - ZIP archive,	unpacked size 684,134,720 bytes	~
Name	Size Packed Type Modified CRC32	
	File folder	
npp.installer.x64.exe	684,134,720 1,068,276 Application 1/24/2023 9:44 CAB230AA	
-	Total 684,134,720 bytes in 1 file	

Figure 6: npp.Installer.x64.zip

Initially, padding was incorporated at the end of the executable, enabling individuals to remove it while maintaining a fully functional file. However, in the sample analysed in this report, padding was inserted into the binary's central region. This method renders the removal of padding more challenging, as simply deleting the zeroes would compromise the integrity of the file and impede its functionality during dynamic analysis.

451280 75 451264 66 451328 66 451392 65 451456 73 451520 30	069006C 0000000 06F6E3D 5726E3A	00650049 00010001 22312E30 73636865 30646570	00200820 006E0066 0000087 22206565 60617320	886F6868 88888868 636F6469	00000024 00000000	00042000 00002000	99299829 99549872 99999889	0061006E	08200028 0873006C	00200020 00510074	88288828	00200000	00000044	0000001	88568861	00729046							D	VarF
451072 00 451136 65 451200 75 451264 66 451328 67 451392 65 451456 72 451456 72 451520 30	96F6E3D 5726E3A E63793E F736F66	22312E38 73636865 3C646578	2220656E 6061732D		00000024 00000000 6E673D22		88548872 8888888	0061006E	0073006C	00610074														
451136 65 451280 75 451264 66 451328 66 451392 65 451456 73 451520 30	96F6E3D 5726E3A E63793E F736F66	22312E38 73636865 3C646578	2220656E 6061732D		6E673022		66666666				66630605	806E0008	00000000	006888400	00000000	889999668		nfo	\$	Tre				
451200 75 451264 66 451328 66 451392 65 451456 73 451456 73 451520 30	5726E3A E63793E F736F66	73636865 3C646578	60617320		6E673022					88888833			000000EF		786D6C20							3.		ml vers
451264 68 451328 68 451392 65 451456 73 451528 30	E63793E F736F66	30646578																				'yes"?> <		
451328 65 451392 65 451456 73 451520 30	F736F66							6D2E7631				7273696F			3C646570							festVersio		
451392 65 451456 73 451520 30										74697479	20141310	- COSSELLT	696E3332		60653022							ty type="w		
451456 73 451520 30	5637475	1 10001.00						73222076					2070726F		6F724172							-*6.0.0.0*		
451520 30					6C69634B			22363539				00000000	61686775									<pre>4ccf1df" l</pre>		
												6E63793E										ependency>		
451584 65												793E3C72										ecurity> <r< td=""><td></td><td></td></r<>		
												22207569										nvoker" ui		
			65644578					65717565				65733E3C										ivileges><		
												6F736F66										s-microsof		
												3435372D										(e2011457-		
												22783335			6439362D							DS Id="{35		
													49643022									portedOS		
+22200 U								3C2F7375							643D227B							dOS> <suppo< td=""><td></td><td></td></suppo<>		
		20383065			35626220					ZE737570	786F7Z74	65644F53	3E3C2F61	70706069							78}"> <td>upportedOS</td> <td>><td>ation><</td></td>	upportedOS	> <td>ation><</td>	ation><
		70617469	62696069	74793E3C	2F617373	65606260	793E0000		00000000	00000000	999999999	00000000	00000000	00000000		00000000	/compatib	Hitty><	/assent	aly>				
100.000	00005560	66666666	00000000	000000000	000000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	000009990	00000000	00000000	000000000								
452224 06	00000000	00000000	00000000	00000000	000000000	00000000	00000000	000000000	000000000	00000000	00000000	00000000	000000000	0000000	00000000	00000000								
452288 00	0000000	000000000	00000000	00000000	000000000	000000000	00000000	00000000	000000000	00000000	00000000	00000000	000000000	00000000	00000000	00000000								
	00005666	866669966	000000000	000000000	000000000	00000000	000000000		00000000	00000000	00000000		000000000	00000000	000000000	00000000								
100120 00	00000000	000000000	00000000	00000000	000066666	000000000	00000000	00000000	000000000	00000000	00000000	00000000	000000000	000000000	00000000	00000000								
452488 86	00000000	000000000	00000000	00000000	000000000	000000000	00000000	00000000	000000000	000000000	00000000	00000000	000000000	000000000	00000000	00000000								
	00000000	000000000	00000000	00000000	000000000	000000000	00000000	00000000	000000000	00000000	00000000	00000000	000000000	000000000	00000000	000000000	e x							
452688 98	0100000	000000000	00000000	000000000	000000000	000000000	000000000	000000000	000000000	000000000	00000000	000000000	000000000	00000000	000000000	000000000	é ,							
452736 00	00000000	000000000	000000000	00000000	000000000	000000000	00000000	00000000	000000000	000000000	00000000	000000000	000000000	000000000	00000000	00000000								
452888 86	00000000	000000000	00000000	000000000	000000000	000000000	00000000	000000000	000000000	000000000	00000000	000000000	000000000	00000000	000000000	000000000								
452360 00	00000000	000000000	000000000	000000000	000000000	000000000	000000000	000000000	000000000	000000000	00000000	000000000	000000000	00000000	000000000	00000000								
452928 86	00000000	000000000	000000000	000000000	993333999	000000000	000000000	00000000	999999999	000000000	000000000	000000000	000000000	000000000	00000000	999999999								
452992 00	00000000	000000000	00000000	000000000	000000000	00000000	00000000	000000000	000999000	00000000	00000000	000000000	000000000	00000000	00000066	0000000000								

Figure 7: Beginning of null bytes padding

											np	p.Install	er.x64.e	xe			
	00000000														*****	000000000	
684123136 684123200															00000000	00000000	
684123288													000000000	000000000	00000000	00000000	
684123328													000000000	00000000	00000000	2000000000	
684123392												000000000	000000000	000000000	00000000	000000000	
684123456	66666666	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	66666666	00000000	00000000	00000000	00000000	00000000	
684123520	00000000	99999999	00000000	00000000	00000000	00000000	00000000	00000000	00000000	000999660	666666999	999666699	00000000	666669956	00000000	00000000	
684123584	0000000	88888888	00000000	00000000	66666666	00000000	00000000	00000000	999999999	000000000	00000000	00000000	000000000	00000000	00000000	00000000	
684123648	00000000	999999999	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	000000000	00000000	00000000	000000000	00000000	
684123712	00000000	99999999	00000000	00000000	00000000	00000000	00000000	00000000	999999999	00000000	000000000	999999999	00000000	000000000	00000000	00000000	
684123776	0000000	999999999	00000000		00000000					00000000	00000000	999999999	000000000	00000000	00000000	00000000	
684123840 684123904																00055666	
684123984		00000000	99990000	00000000						000000000		00000000	000000000	000000000	00000000	00000000	
684124832		00000000	000000000	00000000		00000000	0000000			00000000		000000000	000000000	000000000	000000000	000000000	
684124896															00000000	000000000	
684124168															00000000	00000000	
684124224	00000000	00000000	00000000	000000000	00000000	00000000	000000000	0000000	00000000	000000000	00000000	999999999	00000000	666669956	0000000	00000000	
684124288	00000000	88888888	00000000	00000000	00000000	80000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	
684124352				00000000								000000000	00000000	66666666	000000000	00000000	
684124416												999999999	00000000	00000000	00000000	00000000	
684124480				00000000								999999999	00000000	00000000	66666666	00000000	
684124544 684124688																000000000	
684124688																	₽' 9,'3 *,H,, ,,'\$8,' 1.9 `,H e 8I + ,7
684124736																	.nele + .7 e ege '.H e ePuvj<
684124890																	.)/. "SQ.I [b d.%5'!.J&Z}]00. u.
684124864	01020210	8E9B188E	F9D82DE7	EFD858E2	9848185A	30000689	24864886	F7808181	00050030	65310638	09068355	84861382	55533115	30130603	55848A13	BC446967	P. @ Z0 *.H., 8e1.0 U US1.0 U Dig
684124928	69436572	7428496E	63311938	17068355	04881310	7777772E	64696769	63657274	2E636F6D	31243822	06035584	03131844	69676943	65727428	41737375	72656428	iCert Incl @ U www.digicert.com1\$0" U DigiCert Assured
684124992	49442852	6F6F7428	4341301E	17003232	30383031	38383838	30305A17	00333131	31303932	33353935	395A3062	31083009	06035504	06130255	53311530	13060355	ID Root CA0 22080100000802 31110923595920b1 0 U US1 0 U
684125856																	DigiCert Incl 0 U www.digicert.com10 U DigiCert T
																	rusted Root G40. "0 ".H 0sh]J<0"013.
684125184																	
684125248 684125312																	N YUr.h.pu.jsZ., Dt;mq c)^Nla.4^.[
684125312																	
684125440																	.q.'09. X .\$\F.di.v.v=Y]BvizH f.tK . c
684125584																	END +~an.3K .}!p.A`c D. vb~d.3
684125568																	Cw ! .TD%.1. RQGt.8Au.z?A [. P.1r " .ILu
68412563Z	3F63EC21	SFC42051	GB6FB1AB	86884FC2	06455F90	28FCA11E	C5CR8FA2	B17E8A26	99F5E469	ZF981020	F509A982	1DE51802	83819981	A382013A	30820136	388F6683	7c.1 QkoDE~ &i/ :0. 60
684125696	551D1301	01FF0405	30030101	FF301D06	03551D0E	84168414	ECD7E382	02715064	4CDF2E67	3FE78A98	AE1C8F4F	301F0603	55102384	18301680	1445EBA2	AFF492CB	U . 0 .0 Uq]dLg? 00 U# 0.E
684125768	82312051	8BA7A721	90F360C8	0F300E05	0355100F	8181FF84	84838281	86387986	882B8581	85858781	01046030	68382486	88289681	05050730	01861868	7474703A	.1-QIm. 0 U0y + m8k8\$ + 0.http:
684125824																	//ocsp.digicert.com@C + @ .7http://cocerts.digicert.com/Dig
684125888																	iCertAssuredIDRootCA.crt@E U >0<0:.8.6.4http://crl3.digicert.
684125952																	com/DigiCertAssuredIDRootCA.crl0 U 0 0 U 0 *.H
684126816 684126888																	. pC\U.8t =W
064120889	11000315	ALF7+272	06248052	03C84ED8	2AUEFA2D	56CFF9F4	F/AC38/A	34999996	04010143	++98+321	£890/2A1	10015508	30414190	0313/727	4404E779	C655M8P8	r.\$.R .N.+V8z^CD.C!r.HO. w'DY
				~													

Figure 8: End of null bytes padding

After execution, the malware promptly establishes a connection to a Telegram channel to acquire its command and control (C2) address, specifically http://95.217.16.127. If Telegram is not available, the malware will then attempt to connect to a profile on video game platform Steam, in which case the C2 address was http://157.90.148.112/ at the time of initial analysis and http://116.203.6.107 later. It then proceeds to check-in and obtain its configuration file and subsequently downloads get.zip, an archive containing several legitimate DLL libraries, which are utilized to extract information and saved passwords from various applications and browsers. Through traffic analysis, the method by which the malware obtains its Command and Control (C2) location, and analysis of the configuration obtained, it can be assessed with high confidence that the malware in question is the info-stealer known as Vidar. Vidar has been extensively covered by various cybersecurity organizations. Further information regarding this info-stealer and its origins can be found here^[3].

	l Time	Source	Destination	Protocol	Length	Info												
	110 101110	- ISTITUGITUGITUS	14011041101100			011 7		,	7111			1.01/1					453	
	217 23.97435		149.154.167.99	TCP												61888 Len	=157	
	218 23.97453		192.168.100.223	TCP					Seq=225			1=64128	Len=0 S	LE=265	SRE=422			
	278 28.28935		192.168.100.223	TLSv1					reassem									
	279 28.28962		149.154.167.99	TCP					Seq=422									
	280 28.28978		192.168.100.223	TCP													assembled	
	281 28.28979		192.168.100.223	TCP										0 [TCP	segment	of a rea	assembled	PDU
	282 28.28997	8 192.168.100.223	149.154.167.99	TCP					Seq=422									
	283 28.29007		192.168.100.223	TCP	1514	443 →	58588	[ACK]	Seq=572	0 Ack=4	122 Wi	1=64128	Len=146	60 [TCP	segment	of a rea	assembled	PDU
	284 28.29008	3 149.154.167.99	192.168.100.223	TCP	1514	443 →	58588	[ACK]	Seq=718	0 Ack=4	22 Wi	1=64128	Len=146	0 [TCP	segment	of a rea	assembled	PDU
	285 28.29008	4 149.154.167.99	192.168.100.223	TCP	1514	443 →	58588	[ACK]	Seq=864	0 Ack=4	122 Win	1=64128	Len=146	0 [TCP	segment	of a rea	assembled	PDU
	286 28.29022	9 192.168.100.223	149.154.167.99	TCP	54	58588	→ 443	[ACK]	Seq=422	Ack=97	44 Wi	=26214	4 Len=0					
	287 28.29027	5 192.168.100.223	149.154.167.99	TCP	54	58588	→ 443	[ACK]	Seq=422	Ack=10	100 W	in=2616	32 Len=@)				
	288 28.29264	0 149.154.167.99	192.168.100.223	TCP	1514	443 →	58588	[ACK]	Seq=101	00 Ack	422 W	in=6412	8 Len=14	60 [TC	P segmen	nt of a re	eassembled	d PD
	289 28.29277	0 192.168.100.223	149.154.167.99	TCP	54	58588	→ 443	[ACK]	Seq=422	Ack=13	560 W	in=2621	44 Len=€	,				
	290 28.29423	4 149.154.167.99	192.168.100.223	TCP	1514	443 →	58588	[ACK]	Seq=115	60 Ack	422 W	in=6412	8 Len=14	60 [TC	P segmen	nt of a re	eassembled	d PD
	291 28.29423	9 149.154.167.99	192.168.100.223	TCP	1514	443 →	58588	[ACK]	Seq=130	20 Ack:	422 W	in=6412	8 Len=14	60 [TC	P segmen	nt of a re	eassembled	d PD
	292 28.29424	1 149.154.167.99	192.168.100.223	HTTP	745	HTTP/1	1.1 200) OK	(text/ht	ml)					-			1
	<head>\n</head>						07	10 61	1 6d 22 3				1 20 70	70.04	70 65	and a sea	ta prope	
	<meta charse<="" td=""/> <td>="utf-8">\n</td> <td></td> <td></td> <td></td> <td></td> <td>07</td> <td></td> <td>2 74 79 3</td> <td></td> <td></td> <td></td> <td>55 73 63</td> <td></td> <td></td> <td></td> <td>descript</td> <td></td>	="utf-8">\n					07		2 74 79 3				55 73 63				descript	
		ram: Contact @litlebey<	/title>\n				079		9 6f 6e 2				55 6e 74				tent="ho	
		/iewport" content="widt		al-scale=1.0	Ø">\n				1 6f 73 2	20 68 7	4 74 7		2f 2f 39				://95.21	
		if(window.parent!=null&				nastMes	071			36 2e 3			38 30 7c				:80 ">	
	\n	er (willdowipar en et-ind e da		., (azildowip	ur en en en	posicies	SE 070			74 61 2 74 74 6	0 70 7		70 65 72 59 74 6c		3d 22		operty="	
~		g:title" content="litt	lebe">\n				07			/4 /4 0 55 6e 7			59 74 6C 59 74 74				littlebe	
		a property="og:image" c		well hace6	A DHN2	ZVR3aWD			2 3e 0a 3				70 72 6f				propert	
		g:site_name" content="		, xareyoaseo	·,···	Lyosan	080	00 79	3d 22 1	74 77 6	9 74 7		72 3a 69				er:image	
		g:description" content		46 407-001	lle Ver			10 22	2 20 63 6	5f 6e 7	4 65 6	e 74 3	3d 22 64	61 74	61 3a	<pre>" conten image/sv</pre>	t="data:	

Figure 9: Telegram traffic

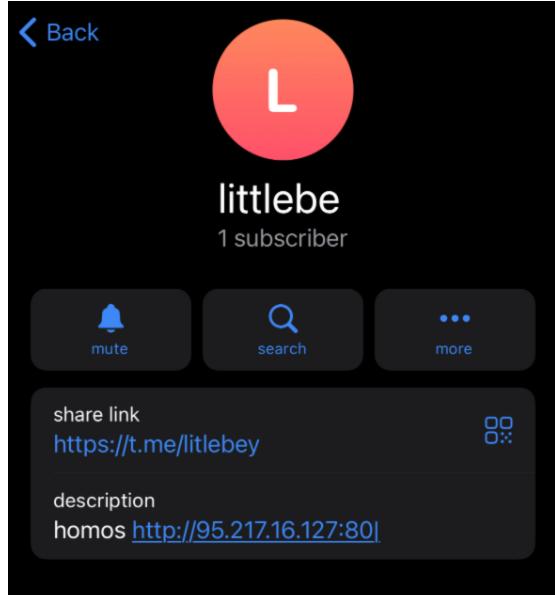


Figure 10: Telegram channel containing the location of Vidar's C2 address

steamcommunity.com/profiles/76561199472399815 ①											
STEAM	STORE COMMUNITY ABOUT SUPPORT	🧟 Install Steam Iogin language 🛩									
?	homos http://116.203.6.107 +	Level 💿									
		Currently Offline									

Figure 11: Steam profile containing the location of Vidar's C2 address

•	н	TTP Requests 40	Connections 47	DNS Requests	23	Threats	21	http://95.217.16.127/	🛨 PCAP	生 SSL Keys
(hift	Headers	Rep PID	Process name	C	CN URL			Con	ntent
	ms		👌 4836	npp.Installer.x64.exe		http	://95.2	17.16.127/827	109 b -	∔ text
	ms	GET 200: OK	6 4836	npp.Installer.x64.exe	E	http	://95.2	:17.16.127/get.zip	1.49 Mb	↓ compressed
Ť	ms	POST 200: OK	e 4836	npp.Installer.x64.exe		http	://95.2	17.16.127/	86.4 Kb · 2 b ·	† text ∔ text

Figure 12: Vidar C2 traffic

1,1,1,1,0,5cf324caa7f3102f9da9c12d59f2d187,1,1,1,0,Default;%DOCUMENTS%\;*.txt;50;true;movies:music:mp3:exe; Figure 13: Vidar configuration obtained from the C2

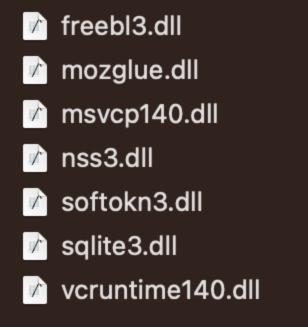


Figure 14: Libraries downloaded by Vidar

Campaign ID 827

The domain download-notepad-plus-plus.duckdns.org, from which the malware is distributed, resolves to the IP address 185.163.204.10. Using passive DNS, it has been determined that multiple domains also resolve to this IP address. This information suggests that the threat group responsible for this campaign is also utilizing advertising to target individuals searching for specific applications besides Notepad++, including:

- OBS Studio
- Davinci Resolve
- Sqlite
- Rufus
- Krita

Furthermore, it has been observed that all the malware samples obtained in this investigation connect to the same Telegram channel, utilize the same two Command and Control IP addresses, and share the same campaign ID of "827".

Conclusion

The recent proliferation of malvertising campaigns, which are employed by cyber-criminals to distribute malware, has become a significant cause for concern. Unlike more traditional infection vectors, such as email, malvertising is harder to protect against. Furthermore, the use of padding techniques to inflate the size of malware payloads can make detection and analysis more challenging.

To mitigate the risk of falling victim to such attacks, it is recommended to exercise caution when interacting with online advertisements. Specifically, it is advisable to avoid clicking on any advertisements while searching for free software on search engines and to instead download programs directly from official sources. This approach can reduce the likelihood of inadvertently downloading malware from untrusted sources.

Another effective measure to counteract the threat of malicious ads is the utilization of adblocker software. The implementation of an ad-blocker can provide an additional layer of protection against malvertising campaigns and enhance overall cybersecurity.

Appendices

Indicators of Compromise

Filename npp.Installer.x64.zip

SHA256 Hash

7DFD1D4FE925F802513FEA5556DE53706D9D8172BFA207D0F8AAB3CEF46424E8

Filename npp.Installer.x64.exe

SHA256 Hash

368008b450397c837f0b9c260093935c5cef56646e16a375ba7c47fea5562bfd

Filename rufus-3.21.zip

SHA256 Hash

75db4f8187abf49376a6ff3de0163b2d708d72948ea4b3d5645b86a0e41af084

Filename rufus-3.21.exe

SHA256 Hash

169603a5b5d23dc2f02dc0f88a73dcdd08a5c62d12203fb53a3f43998c04bb41

Filename DaVinci_Resolve_18.1.2_Windows.zip

SHA256 Hash 73f00e3b3ab01f4d5de42790f9ab12474114abe10cd5104f623aef9029c15b1e

Filename DaVinci_Resolve_18.1.2_Windows.exe

SHA256 Hash

169603a5b5d23dc2f02dc0f88a73dcdd08a5c62d12203fb53a3f43998c04bb41

Filename krita-x64-5.1.5-setup.zip

SHA256 Hash

85eb4b0e3922312d88ca046d89909fba078943aea3b469d82655a253e0d3ac67

Filename krita-x64-5.1.5-setup.exe

SHA256 Hash

169603a5b5d23dc2f02dc0f88a73dcdd08a5c62d12203fb53a3f43998c04bb41

- **URL** http://95.217.16.127/827
- URL http://95.217.16.127/get.zip
- URL http://95.217.16.127/
- URL http://157.90.148.112/827
- URL http://157.90.148.112/
- URL http://157.90.148.112/get.zip
- URL http://116.203.6.107/
- Domain notepadplusplus.site

Domain	download-notepad-plus-plus.duckdns.org
Domain	download-obsstudio.duckdns.org
Domain	dowbload-notepadd.duckdns.org
Domain	dowbload-notepad1.duckdns.org
Domain	download-davinci-resolve.duckdns.org
Domain	download-davinci.duckdns.org
Domain	download-sqlite.duckdns.org
Domain	download-davinci17.duckdns.org
Domain	download-rufus.duckdns.org
Domain	download-kritapaint.duckdns.org
IP Address	37.140.192.11
IP Address	185.163.204.10
IP Address	95.217.16.127
IP Address	157.90.148.112
IP Address	116.203.6.107
URL https:/	/t.me/litlebey

URL https://steamcommunity.com/profiles/76561199472399815

References

[1] https://www.bleepingcomputer.com/news/security/hackers-push-malware-via-google-search-ads-for-vlc-7-zip-ccleaner/

[2] https://www.bleepingcomputer.com/news/security/ransomware-access-brokers-use-google-ads-to-breach-your-network/

[3] https://www.team-cymru.com/post/darth-vidar-the-dark-side-of-evolving-threatinfrastructure

More in this series:

No items found.