New Meta information stealer distributed in malspam campaign

bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/

Bill Toulas

By

<u>Bill Toulas</u>

- April 10, 2022
- 11:12 AM
- 0



A malspam campaign has been found distributing the new META malware, a new info-stealer malware that appears to be rising in popularity among cybercriminals.

META is one of the novel info-stealers, along with Mars Stealer and BlackGuard, whose operators wish to take advantage of <u>Raccoon Stealer's exit</u> from the market that left many searching for their next platform.

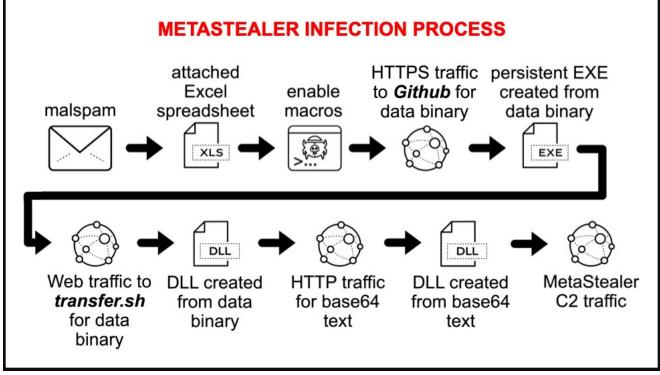
Bleeping Computer first <u>reported about META last month</u>, when analysts at KELA warned about its dynamic entrance into the <u>TwoEasy botnet marketplace</u>.

The tool is sold at \$125 for monthly subscribers or \$1,000 for unlimited lifetime use and is promoted as an improved version of RedLine.

New Meta malspam campaign

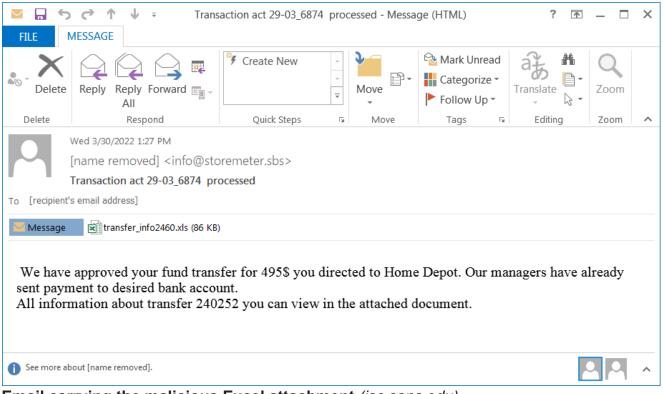
A new spam campaign seen by security researcher and ISC Handler Brad Duncan is proof that META is actively used in attacks, being deployed to steal passwords stored in Chrome, Edge, and Firefox, as well as cryptocurrency wallets.

The infection chain in the particular campaign follows the "standard" approach of a macrolaced Excel spreadsheet arriving in prospective victims' inboxes as email attachments.



META infection chain on the spotted campaign (*isc.sans.edu*)

The messages make bogus claims of fund transfers that are not particularly convincing or well-crafted but can still be effective against a significant percentage of recipients.



Email carrying the malicious Excel attachment (*isc.sans.edu*)

The spreadsheet files feature a DocuSign lure that urges the target to "enable content" required to run the malicious VBS macro in the background.

ELE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW Sign in • alibbit - 111 - A A • A • B I U - 0 - 2 - 4 - 1 • B I U - 0 - 2 - 4 - 1 • B I U - 0 - 2 - 4 - 1 • B I U - 0 - 2 - 4 - 1 • B I U - 0 - 2 - 4 - 1 • B I I U - 0 - 2 - 4 - 1005	Transfer_info2460.xls [Compatibility Mode] - Excel	? 🛧	– 🗆 🗙
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	FILE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW		Sign in
SECURITY WARNING Macros have been disabled. Enable Content × L11 • : • fx A B C D E F G H I J K L M A B C D E F G H I J K L M C D E F G H I J K L M This DOCUMENT IS PROTECTED To open the document, follow steps: This document is only available for desktop version of Microsoft Office Word Microsoft Office Word Microsoft Office Word Microsoft Office Word H H L L L L L L L L L L L L L L L L L L	Calibri VIII A A = % V Format as Table V Potete		
Introductions button from the voltave base	Clipboard 🕫 Font 🕫 Alignment 🕫 Number 🕫 Styles Cells	Editing	~
A B C D E F G H I J K L M 1 2 3 4 5 6 7 8 9 10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	SECURITY WARNING Macros have been disabled. Enable Content		×
Image: Control of the sector of Microsoft Office Word	L11 \bullet : $\times \checkmark f_x$		~
1 2 3 4 5 6 7 8 9 10 11 12 10 11 12 10 11 12 10 11 12 10 11 12 10 11 12 10 11 12 13 14 15 16 17 18 19 10 10 10 10 11 11 12 12 13 14 15 15 16 17 18 10 10 10 11 11 12 12 14	A B C D E F G H I J K	L	M
12 To open the document, follow steps: 13 14 15 16 16 17 18 19 10 10 10 11 12 13 14 15 16 17 18 19 10 10 10 10 10 10 10 10 10 10 10 10 10 10 11 12 13 14	3 4 5 5 6 10		
16 Inits document is only available for desktop version of 16 Microsoft Office Word 18 Image: State of the second secon	To open the document, follow steps:		
	16 17 Microsoft Office Word		

The DocuSign lure that entices users to enable content *(isc.sans.edu)* When the malicious script runs, it will download various payloads, including DLLs and executables, from multiple sites, such as GitHub.

Some of the downloaded files are base64 encoded or have their bytes reversed to bypass detection by security software. For example, below is one of the samples collected by Duncan that has its bytes reversed in the original download.

🤒 010 Ec	lito	or - C:	\Use	rs\U	ser\E)own	load	ls\W	nior	nez_l	Dabl	vtrq.	bmp	.bin				
<u>F</u> ile <u>E</u> di	it	Sear	ch	<u>V</u> iew	/ F <u>c</u>	<u>o</u> rma	t S	cr <u>i</u> pt	s T	emp	lates	<u>T</u> o	ols	<u>W</u> ir	ndov	/ <u>H</u>	elp	
🗋 🗕 💆	•	- 🔒	ð	<u>i</u>	2	2	Ъ	Þ	Ē	Ŋ	6	P	Å₿	ø	•		A	🔌 Hex 💸 🦷 🔹 »
Startup	x	Wini	orne	z_Da	blvt	rq.bn	np.bi	n 🗷										$\leftrightarrow = \mp$
₹ Edit A	s: I	lex ▼	R	in Sc	ript 🔻	R	un Te	mpla	te 🔻									
		Ó	1	2	3	4	5	Ģ	7	8	9	Ą	B	Ç	D	E	F	0123456789ABCDEF
A:EC90ł	1:	00	00	00	48	00	00	20	80	00	00	00	00	00	00	00	00	H
A:ECA0ł	1:	00	00	00	80	00	00	20	00	00	00	00	00	00	00	00	00	
A:ECB0ł	1:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
A:ECC01	1:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
A:ECD01	1:	00	00	00	00	00	00	00	00	00	00	00	0C	00	0B	40	00	
A:ECE01	1:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
A:ECF01	1:	00	00	03	7C	00	0B	20	00	00	00	00	4 B	00	0B	04	90	K
A:ED00ł	1:	00	00	00	00	00	00	00	00	00	00	00	0F	00	00	00	00	
A:ED10h	1:	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00	
A:ED20ł	1:	85	40	00	03	00	00	00	00	00	00	02	00	00	0B	60	00	@`.
A:ED30h	1:	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	04	
A:ED40ł	1:	00	00	02	00	00	00	20	00	00	40	00	00	00	0B	20	00	
A:ED50ł	1:	00	00	20	00	00	0B	04	\mathbf{DE}	00	00	00	00	00	00	06	00	Þ
A:ED60ł	1:	00	A 0	E6	00	00	06	01	0B	21	0E	00	E 0	00	00	00	00	æ!à
A:ED70ł	1:	00	00	00	00	62	3C	BE	11	00	03	01	4C	00	00	45	50	b<¾LEP
A:ED80ł	1:	00	00	00	00	00	00	00	24	A 0	0D	0D	2E	65	64	6F	6D	\$edom
A:ED90ł	1:	20	53	4 F	44	20	6E	69	20	6E	75	72	20	65	62	20	74	SOD ni nur eb t
A:EDA0ł	1:	6F	6E	6E	61	63	20	6D	61	72	67	6F	72	70	20	73	69	onnac margorp si
A:EDB01	1:	68	54	21	CD	4C	01	B8	21	CD	09	В4	00	0E	BA	1F	0E	hT!ÍL.,!Í.´°
A:EDC01	1:	00	00	00	80	00	00	00	00	00	00	00	00	00	00	00	00	€
A:EDD01	1:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
A:EDE01	1:	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	B8	
A:EDF01	1:	00	00	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	00	00	00	04	00	00	00	03	00	90	5A	4D	ÿÿZM
40033• 4																		
Opened f	ile	'C:\U	sers\	User	\Dov	vnloa	ac Po	s: 0	0h]	V	/al: 0	0h 0	0000	0000	b	Siz	e: 716	288 ANSI LIT W OVR

DLL saved in reverse byte order (*isc.sans.edu*)

Eventually, the final payload is assembled on the machine under the name

"qwveqwveqw.exe," which is likely random, and a new registry key is added for persistence.

	9									
ile Edit View Favori			60.147							
Computer\HKEY_CURR				dows NI\Currer	ntVersio	n\Winlogor	n			
TokenBroker 🔨	Name	Туре	Data							
Vindows	ab (Defa		(value not							
Winlogon	👪 Build	REG_DWORD REG_BINARY								
Windows Script	NP DP	6b 57 6	7 55 4b (00 00 .						
Windows Script He	ab Exclud	REG_SZ	AppData\l	Local;AppData\	LocalLo	w;\$Recycle.l	Bin;Onel	Drive;Wo	rk Fol.	
Windows Search	👪 FirstL	REG_DWORD	0x000000	00 (0)						
Windows Security	arse	-	1							
Nisp	BUUA REG_BINARY 23 e8 6b 57 01 00 00 00 10 00 14 00 81 35 00 00 ed 35 00 0									
	-661.001.00									
(boxLive	ور دور الله الله الله الله الله الله الله الله	REG_SZ		ke,"C:\Users\	\Ap	pData\Roan	ning\qw	veqwveo		
KboxLive	ab Shell ming			ke, "C:\Users\	\Ap		ning\qw	×		
KboxLive	Shell ming Share Vi	REG_SZ		ke, "C:\Users\	\Ap	oData\Roan —		×	ąw.exe	
KboxLive	Shell ming Share Vi	REG_SZ	explorer.ex	ke, "C:\Users\ V Type		oData\Roan —		×	ąw.exe	
KboxLive KboxLive	Shell ming Share Vi	REG_SZ	explorer.ex	~		Data\Roan — P Sea		×	ąw.exe	
KboxLive KboxLive	Shell ming Share Vi	REG_SZ	explorer.ex	✓ Type File folder		Data\Roan — P Sea		×	ąw.exe	
KboxLive KboxLive	Shell ming Share Vi	REG_SZ	explorer.ex	Type File folder File folder		Data\Roan — P Sea		×	ąw.exe	
KboxLive KboxLive	et Shell ming Share Vi AppData	REG_SZ	explorer.ex	✓ Type File folder	U	Data\Roan — P Sea	rch Roa	×	ąw.exe	

New registry key and the malicious executable (*isc.sans.edu*)

A clear and persistent sign of the infection is the EXE file generating traffic to a command and control server at 193.106.191[.]162, even after the system reboots, restarting the infection process on the compromised machine.

Time		Host	Info	
2022-04-05	23:24:21	github.com	Client Hello	
2022-04-05	23:24:21	raw.githubusercontent	Client Hello	
2022-04-05	23:25:19	transfer.sh	GET /get/qT523D/Wlniornez_Dablvtrq.	bmp
2022-04-05	23:25:19	transfer.sh	Client Hello	
2022-04-05	23:25:37	193.106.191.162:1775	GET /avast_update HTTP/1.1	
2022-04-05	23:25:39	193.106.191.162:1775	GET /api/client/new HTTP/1.1	
2022-04-05	23:25:40	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:27:40	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:29:41	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:31:41	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:33:43	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:35:44	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:37:45	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:39:46	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:41:48	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:43:49	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:45:50	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:47:51	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:49:52	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:51:52	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:53:53	193.106.191.162:1775	<pre>POST /tasks/get_worker HTTP/1.1 , Jage</pre>	ava
2022-04-05	23:55:53	193.106.191.162:1775	POST /tasks/det worker HTTP/1.1 , J	ava

Malicious traffic captured in Wireshark (isc.sans.edu)

One thing to note is that META modifies Windows Defender via PowerShell to exclude .exe files from scanning, to protect its files from detection.

If you'd like to dive deeper into the malicious traffic details for detection purposes or curiosity, Duncan has published the PCAP of the infection traffic <u>here</u>.

Related Articles:

German automakers targeted in year-long malware campaign

Ukraine warns of "chemical attack" phishing pushing stealer malware

Pixiv, DeviantArt artists hit by NFT job offers pushing malware

New powerful Prynt Stealer malware sells for just \$100 per month

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.