

DRIVE-BY AS A SERVICE: BLACKTDS

MARCH 13, 2018 Kafeine



Overview

Proofpoint researchers have been tracking a new Traffic Distribution System called BlackTDS implicated in the distribution of a variety of malware. BlackTDS is a privately held tool that has been advertising its services on underground markets since the end of December 2017.

BlackTDS offers a variety of services to its clients that they collectively refer to as a “Cloud TDS.” The operators claim that their Cloud TDS can handle social engineering and redirection to exploit kits (EKs) while preventing detection by bots -- namely researchers and sandboxes. Cloud TDS also includes access to fresh domains with clean reputations over HTTPS if required.

The services offered by BlackTDS are summarized in their forum advertisements, the text of which we have left unaltered:

“Cloacking antibot tds based on our non-abuse servers from \$3 per day of work. You do not need your own server to receive traffic. API for working with exploit packs and own solutions for processing traffic for obtaining installations (FakeLandings). Dark web traffic ready-made solutions. Placed in 1 click hidden code to use the injection in js on any landings, including on hacked websites.”

“Cost - \$6 per day, \$45 per 10 days, \$90 per month, FREE place on our server, FREE hosting of your file on green https:// domain. 3 DAYS FREE TEST”

** Cloud Antibot Traffic Management System on our non-abuse servers*

What we added during the holidays:

- * Built-in modes Iframe (a little morally outdated, but asked - we did).
- * fake Microsoft update (breaks the page).
- * Fake update Java and Fake update Flash (the page does not break, the original content is visible).
- * uploading a file from your personal account to our server.
- * Configure delay for the appearance of fake windows.
- * Auto-download when clicking on the window area.
- * Updating the Black and Geo databases from 13.01.18.
- * increased by breaking through the downloads from 6%-12% to 10%-30%.
- * added detailed statistics on users who downloaded the file.
- * autostart file in fakes.

And this is only on holidays! We continue to work. Cloud TDS at your service

Figure 1 shows a screen capture of the cost breakdowns and services offered by BlackTDS.

WHO WE ARE & WHAT WE CAN?



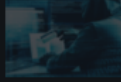
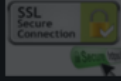

-  Cloud traffic management antibot system based on our non-abuse servers from \$2.67 per day of work. You do not need your own server to receive traffic, cloud tds - the mechanism where traffic comes from different sources, then the system broadcasts the received traffic based on the rules set by the webmaster. Accordingly, the webmaster has full and visible control over the management of his traffic.
-  API for working with exploit packs and own solutions for processing traffic for obtaining installations (Fakeupdates). Dark web traffic ready-made solutions.
-  Placed in 1 click hidden code to use the injection in js on any landings, including on hacked websites.
-  Inexpensive SSL Certificates from \$2 per domain for comfortable work with traffic.
-  Cost - \$6 per day, \$45 per 10 days, \$105 per month, \$240 per 3 month, FREE traffic on our server, FREE hosting of your file on green https:// domain. 3 DAYS
FREE TEST.

Figure 1: Portion of a BlackTDS advertisement

Threat actors drive traffic to BlackTDS via spam, malvertising, and other means, set up the malware or EK API of their choice, and then allow the service to handle all other aspects of malware distribution via drive-by.

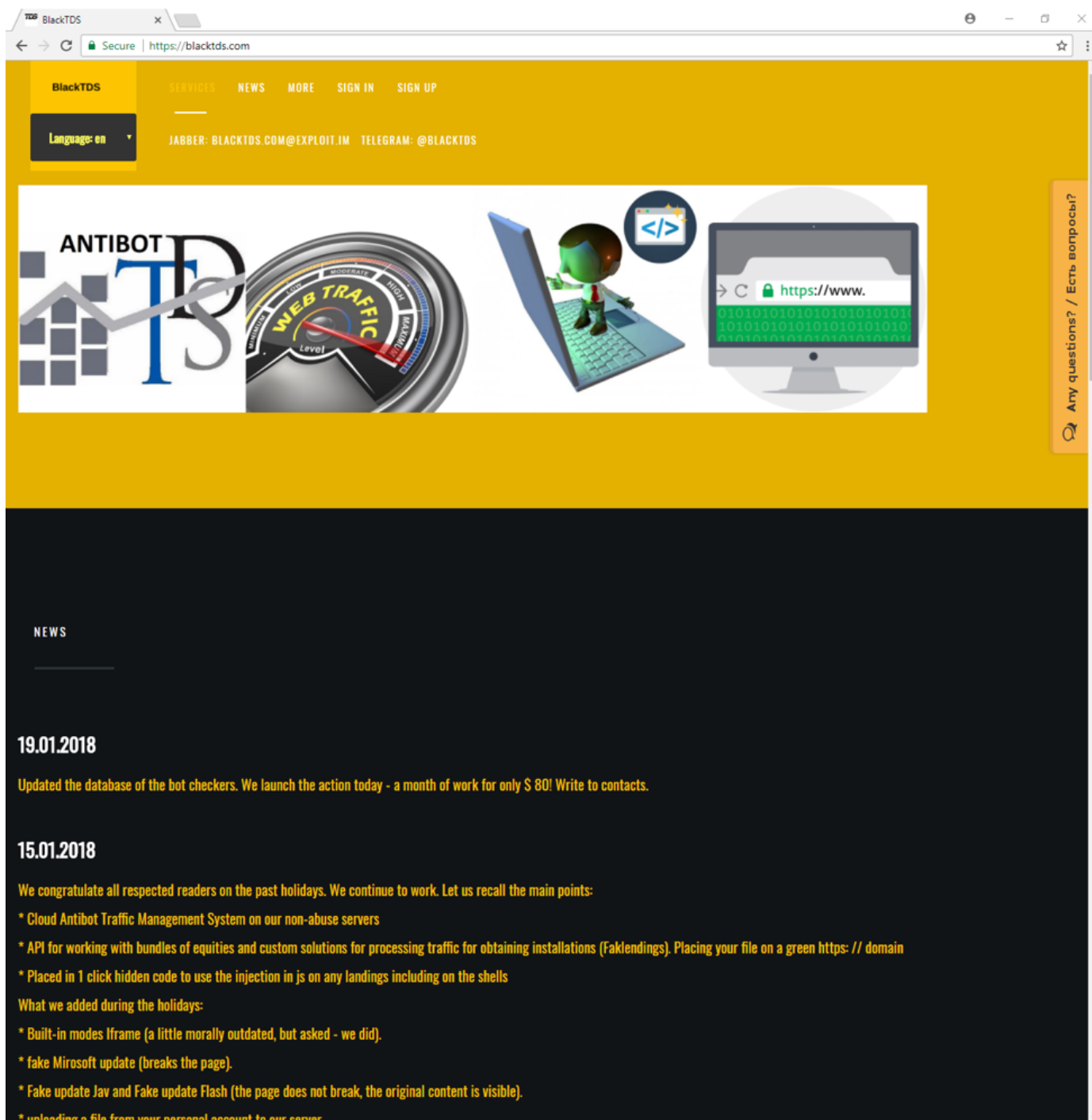


Figure 2: BlackTDS home page

We observed BlackTDS infection chains several times in the wild, distributing malware via fake software updates and other social engineering schemes (Figures 3, 6-8).

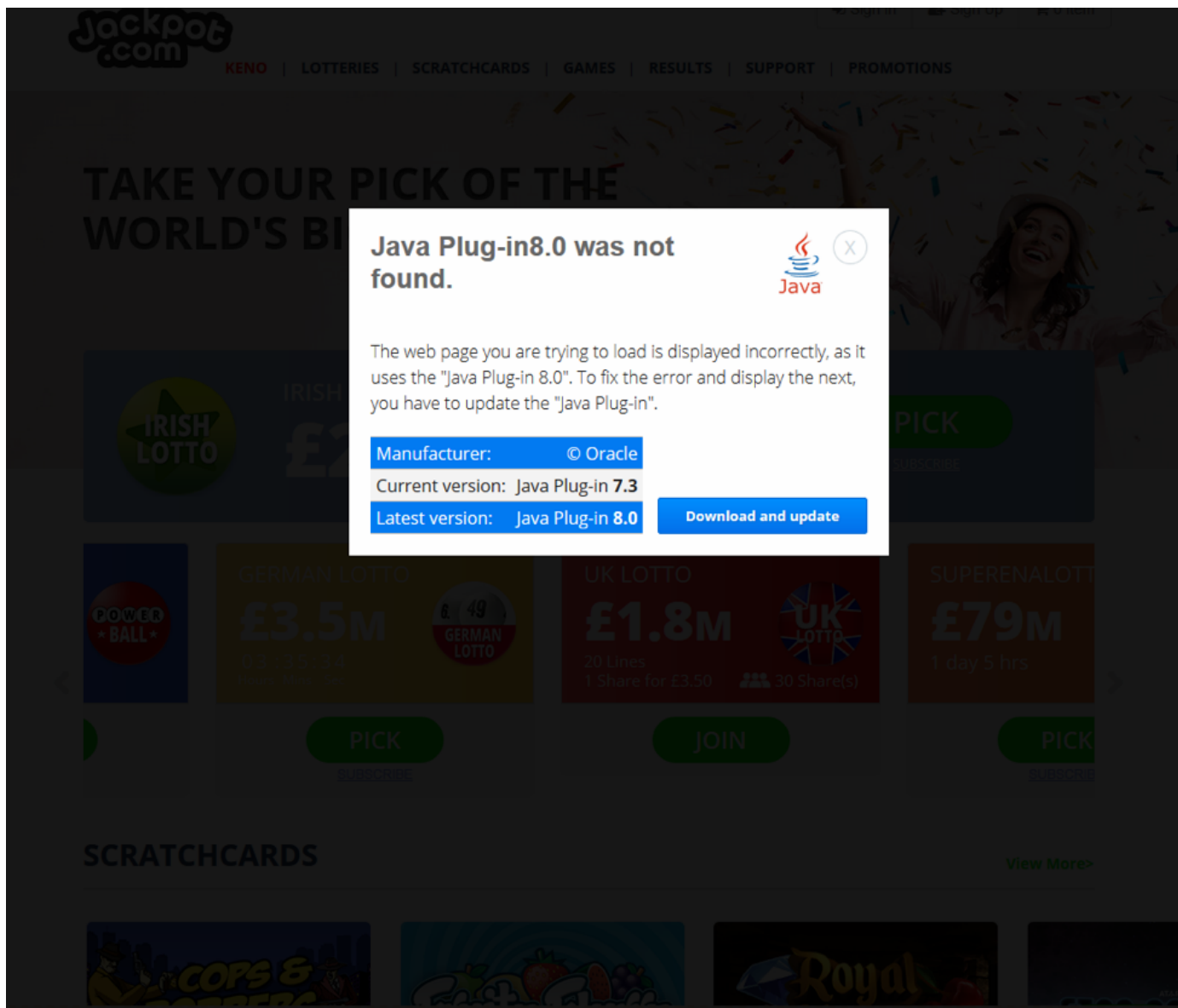


Figure 3: Fake Java Plugin download associated with a BlackTDS drive-by

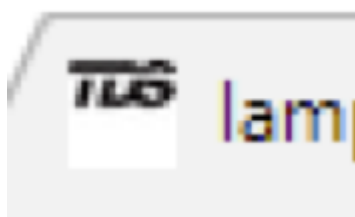


Figure 4: BlackTDS favicon that appears on all identified sites associated with the TDS

Although identifying BlackTDS sites in the wild was relatively easy based on the presence of a distinctive favicon (Figure 4), effectively associating the traffic with a known actor was difficult and, in some cases, almost impossible.

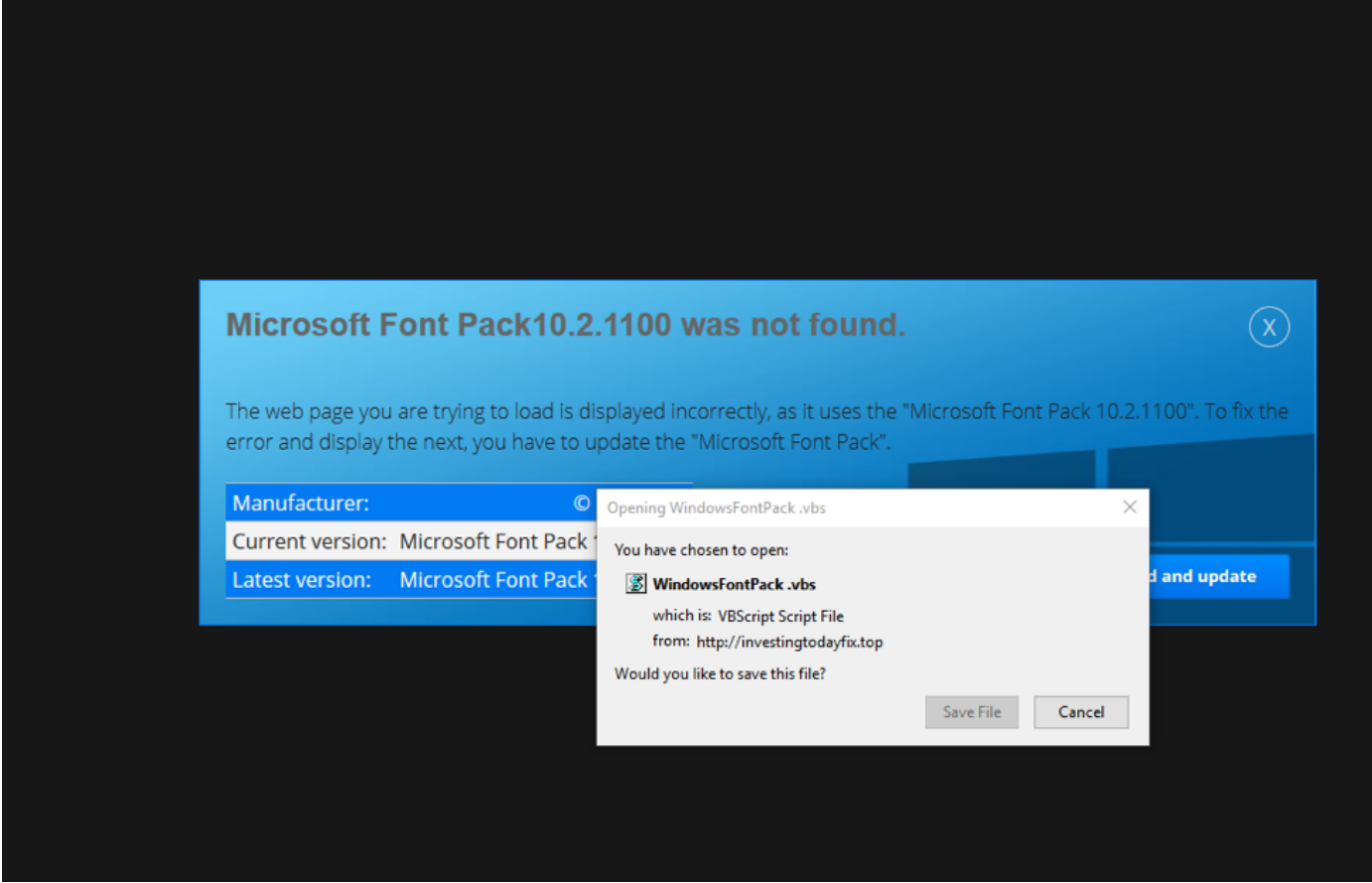


Figure 5: Fake Microsoft Font Pack download associated with a BlackTDS drive-by

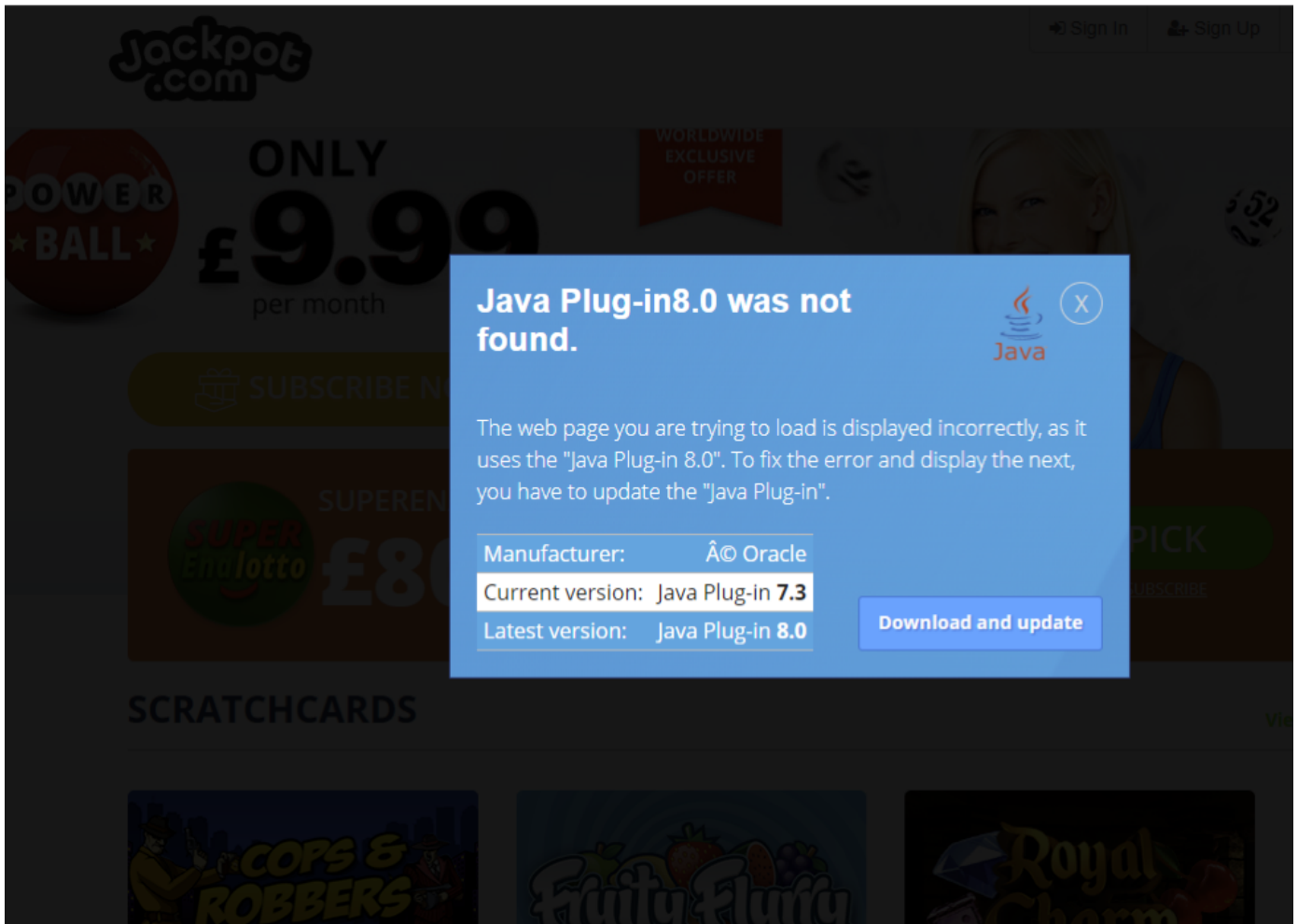
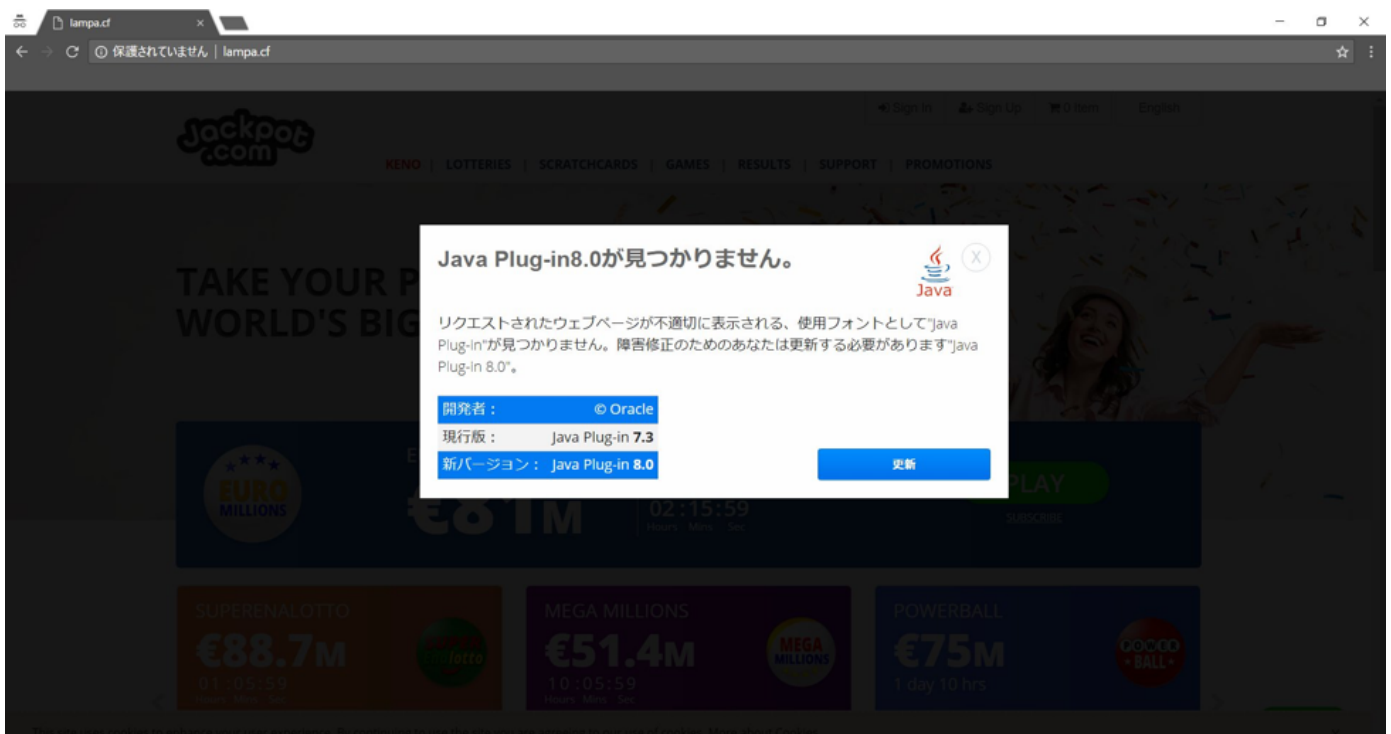


Figure 6: Fake Java Plugin download associated with a BlackTDS drive-by on a typosquatted domain



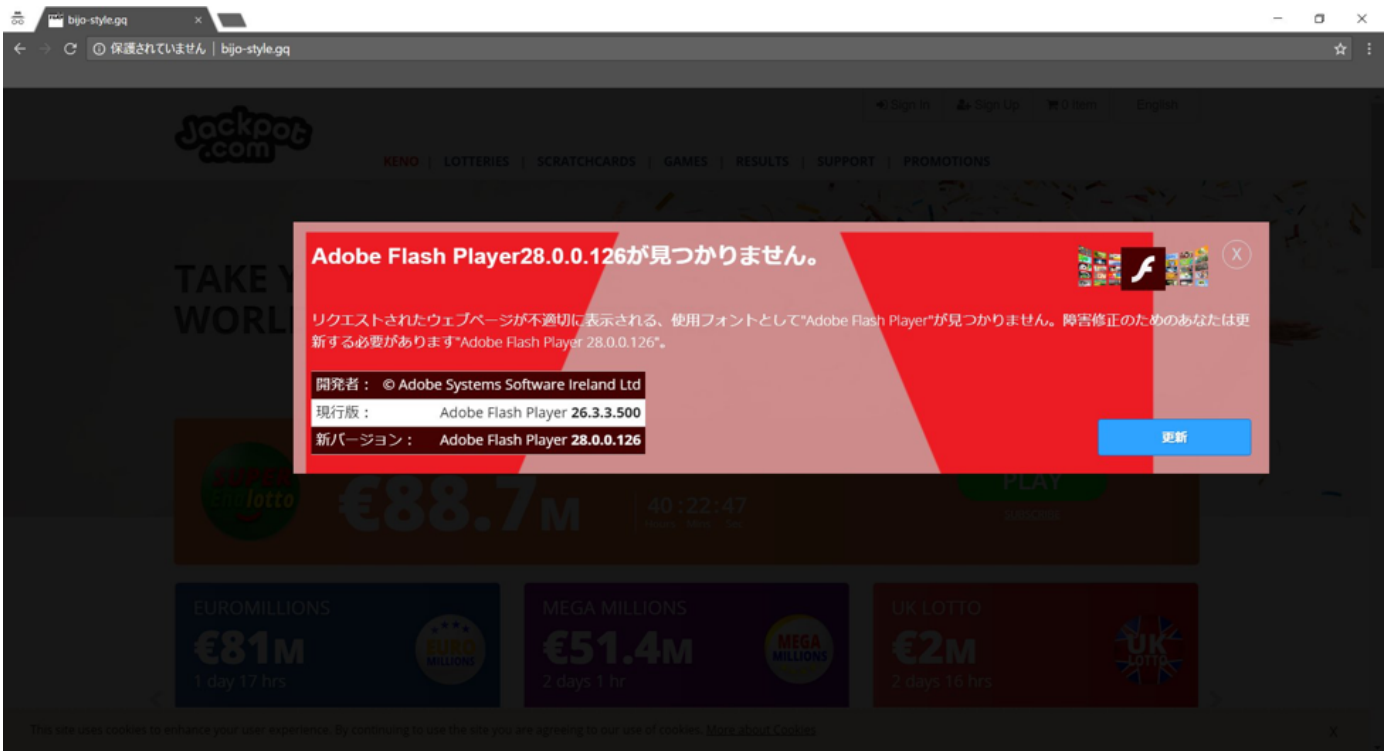


Figure 8: Fake Adobe Flash Player updated associated with a BlackTDS drive-by (source: @Nao_sec)

Clusters	Tags	#Attr.	Date ↓
RIG	exploit-kit, RIG-v, bbsindex, BlackTDS, Malvertising, PrimusAd, AUS, Smokebot, XMRig Variant, CoinMiner, mineXMR	28	2018-01-11
RIG	exploit-kit, RIG-v, get2median, Keitaro, BlackTDS, Malvertising, PopCash, USA, Ramnit, fenquyidh	20	2018-01-21
	soceng-dl, JavaUpdate, url-to-mz, SysStorm, BlackTDS, Undefined, Malvertising, PopCash, USA, Atmos	22	2018-01-23
	soceng-dl, JavaUpdate, url-to-mz, Undefined, BlackTDS, Malvertising, Neutrino Bot	6	2018-01-29
RIG	blog-post, mta, exploit-kit, RIG-v, Undefined, BlackTDS, Malvertising, Ramnit, fenquyidh, AZORult	15	2018-01-30
RIG	exploit-kit, RIG-v, Undefined, BlackTDS, Malvertising, Neutrino Bot	8	2018-01-31
	soceng-dl, MissingFont, url-to-vbs, Expless, BlackTDS, DreamSmasher, No Or Legit Payload	12	2018-02-01
	soceng-dl, FlashUpdate, JavaUpdate, url-to-mz, Undefined, BlackTDS, Bitty, Googl, GoogleDrive, UndefinedDrop	21	2018-02-06
RIG	exploit-kit, RIG-v, Undefined, BlackTDS, Malvertising, PopCash, MIX, No Or Legit Payload	10	2018-02-18
GrandSoft	exploit-kit, GrandSoft, get2median, BlackTDS, Keitaro, Malvertising, PopCash, POL, Quant, Zeus Panda, Thawte	81	2018-03-03

Figure 9: Selection of events we documented involving BlackTDS

Result	X-HostIP	Proto...	Host	URL	Body	Content-Type	Comments
200	54.236.93.2	HTTP	popcash.net	/world/go/9041/174802/aHR0cDovL3BvcG9wcy5jb20...	321	text/html	Popcash Malvertising
303	54.236.93.2	HTTP	popcash.net	/world/sgo/ad?p=9041&w=174802&t=7e34404c9485...	44	text/html; charset=utf-8	Popcash Malvertising
200	46.30.45.78	HTTP	trythat.ga	/	290	text/html; charset=utf-8	BlackTDS
302	185.203.242.228	HTTP	gamjoi.cf	/?gmj	0	text/html; charset=utf-8	get2median (aka "Slots") Keitaro
200	62.109.4.135	HTTP	guardian.julyzssimilarxpm.xyz	/wicks-barr-marque.php	18,517	text/html; charset=utf-8	Grandsoft Landing
200	62.109.4.135	HTTP	guardian.julyzssimilarxpm.xyz	/getversionpd/null/16A0A0A305/null/9A3A0A0	6,498	text/html; charset=utf-8	GrandSoft IE Exploit
200	62.109.4.135	HTTP	guardian.julyzssimilarxpm.xyz	/dwie.hta	6,511	application/octet-stream	Grandsoft soceng HTA
200	62.109.4.135	HTTP	guardian.julyzssimilarxpm.xyz	/2/603656	401,255	application/octet-stream	Grandsoft Payload: Quant
200	87.236.16.224	HTTP	ohyeah.party	/customer/index.php?id=10825902&c=18mk=6c5bb2...	205	text/html	Quant Callback
200	212.237.12.113	HTTP	212.237.12.113	/wp-content/uploads/1hyfyevsaseonebinibi.exe	282,624	application/octet-stream	Quant Task: Load Zeus Panda
200	87.236.16.224	HTTP	ohyeah.party	/customer/index.php?id=10825902&c=28mk=6c5bb2...	0	text/html	Quant Callback
200	87.236.16.224	HTTP	ohyeah.party	/customer/index.php?id=10825902&c=38mk=6c5bb2...	0	text/html	Quant Callback

On February 19, we also observed a massive spam campaign from the actor **TA505** with PDF attachments containing links to a chain involving BlackTDS before ending on a website purporting to sell discount pharmaceuticals. TA505 has typically distributed ransomware and banking Trojans at enormous scale, making this particular campaign unusual.

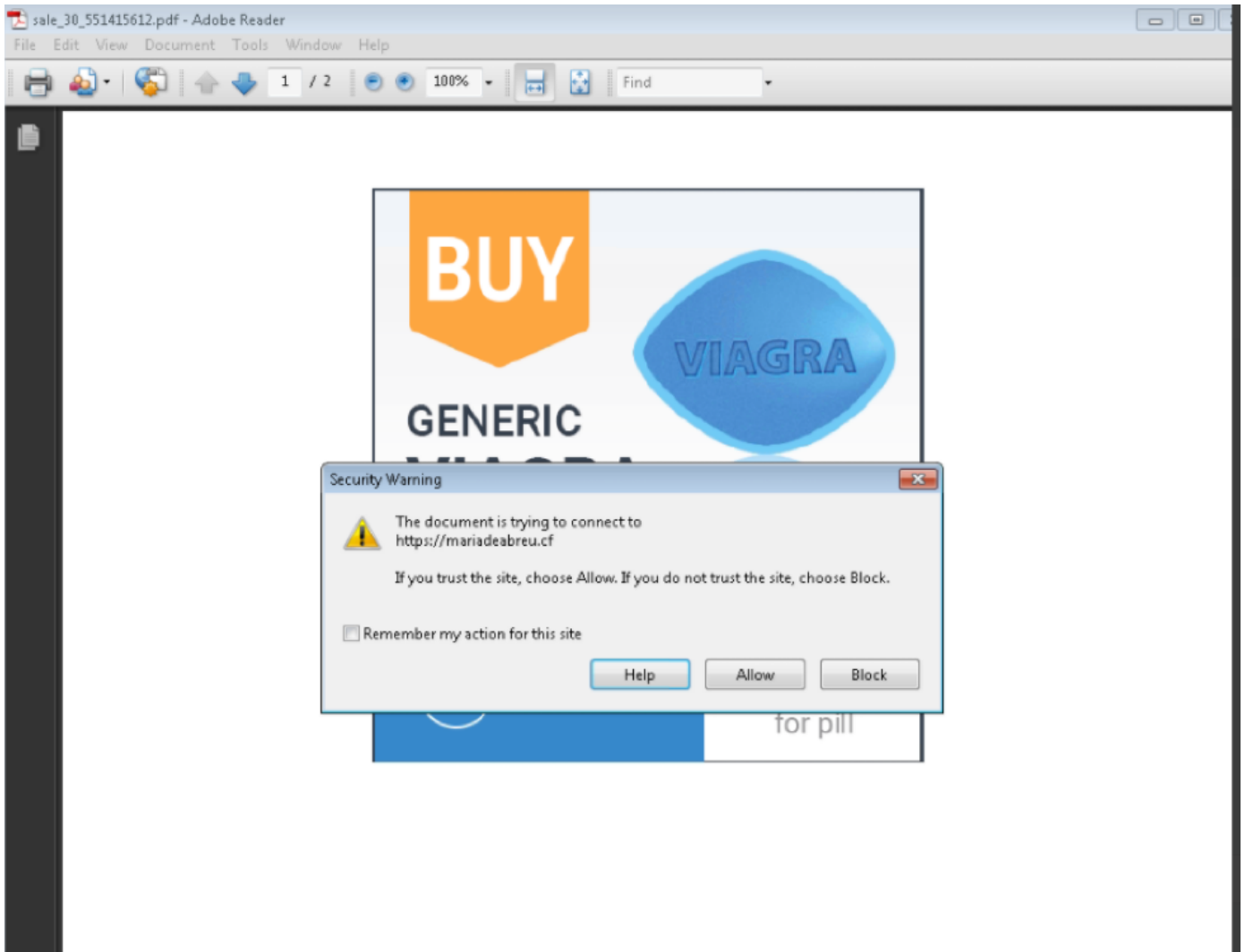


Figure 11: HTTPS URL to BlackTDS in malspam - February 19, 2018

The screenshot shows the Pharmacy Express website interface. At the top, it displays "WE SHIP WORLDWIDE", "\$ USD", "English", and "\$0.00 (0 items)". The main header features the Pharmacy Express logo with a maple leaf and the tagline "#1 ONLINE WORLDWIDE STORE" next to a female pharmacist. A "FAST DELIVERY WORLDWIDE" banner with a male pharmacist is also present. Below the header is a search bar and a "CATEGORIES MENU" button. A navigation bar includes "Browse all by letter" with a grid of letters from A to Z. The main content area is divided into several product sections:

- ED PACKS**: A list of four packs with prices: Super Discount Pack (\$0.68), Active Discount Pack (\$0.68), Super Active Discount Pack (\$1.12), and Classic Discount Pack (\$1.13). A "View all packs" link is provided.
- VIAGRA**: A product card for Viagra showing market prices of \$13.36 - \$39.14 and a special offer starting from \$0.72 per pill. It includes "AIR MAIL" and "EMS" shipping options and a "Select pack" button.
- SUPER DISCOUNT PACK**: A product card showing market prices of \$2.12 - \$6.21 and a special offer starting from an unspecified amount.
- CIALIS**: A product card for Cialis showing market prices of \$11.52 - \$33.77 and a special offer starting from an unspecified amount.

Figure 12: Pharma website receiving the traffic after BlackTDS filtering

It is worth noting that we determined which actor was operating the service itself based on an artefact of this TDS since at least February 2017. We associate the artefact with a trafter we track under the name "BBSindex".

Figure 13 shows infection activity we associate with both BBSindex and BlackTDS:

Sundown	exploit-kit	Sundown	bbsindex	Malvertising	TrafficHolder	USA	Smokebot		2017-01-29				
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	USA	Chthonic	CAN		2017-02-07				
Sundown	exploit-kit	Sundown	bbsindex	USA	Chthonic				2017-02-08				
RIG	exploit-kit	RIG-v	bbsindex	USA	Yebot				2017-02-12				
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	MIX	Smokebot	zloader	Globe	Ransomware	Kelihos	TDS		
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	MIX	Dreambot/ISFB	87694321POIRYTRI	1032		2017-02-16			
RIG	exploit-kit	RIG-v	bbsindex	USA	Dreambot/ISFB	87694321POIRYTRI	1032		2017-02-19				
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	USA	Chthonic			2017-02-27				
RIG	exploit-kit	RIG-v	SweetGarrety	bbsindex	Keitaro	DriveByBot	USA	Smokebot	Kelihos	Dreambot/ISFB	87694321POIRYTRI	1030	
RIG	exploit-kit	RIG-v	SweetGarrety	DriveByBot	bbsindex	Smokebot	Kelihos	Satan	Ransomware	UndefinedDrop	Dreambot/ISFB	87694321POIRYTRI	1030
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	ExoClick	POL	Smokebot	Kelihos	Undefined	CoinMiner	ESP	DiamondFox	
RIG	exploit-kit	RIG-v	bbsindex	Keitaro	Malvertising	MIX	Smokebot	Kelihos	Umbald	Hiloti	CoinMiner	Pushdo	
RIG	exploit-kit	RIG-v	OnlinerBot										
RIG	exploit-kit	RIG-v	Ebates	Malvertising	MIX	Smokebot	bbsindex	Kelihos	Proxyback	Quant			
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	PopCash	AUS	Dreambot/ISFB	87694321POIRYTRI	1030				
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	PopCash	AUS	Madness						
RIG	exploit-kit	RIG-v	bbsindex	Keitaro	ESP	Dreambot/ISFB	87694321POIRYTRI	1033					
RIG	exploit-kit	RIG-v	bbsindex	Keitaro	Malvertising	PopCash	USA	Smokebot	Kelihos				
RIG	exploit-kit	RIG-v	bbsindex	Keitaro	Malvertising	PopCash	CAN	Neutrino Bot					
	soceng-dl		bbsindex	Keitaro	Smokebot								
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	Traffic Shop	POL	Chthonic						
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	PopUnder	CAN	Quant	zloader					
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	USA	Quant							
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	USA	Kovter	885						
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	USA	Dreambot/ISFB	s4Sc9mDb35Ayj8oO	9999	Pushdo				
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	USA	Pushdo							
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	EroAdvertising	USA	Dreambot/ISFB	s4Sc9mDb35Ayj8oO	9999	Pushdo			
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	EroAdvertising	MIX	Dreambot/ISFB	s4Sc9mDb35Ayj8oO	9999				
RIG	exploit-kit	RIG-v	bbsindex	CAN	Chthonic								
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	URLZone								
	soceng-dl		bbsindex	Malvertising	Nymaim								
	soceng-dl		bbsindex	Undefined	CoinMiner	CoinMiner	DwarfPool						
RIG	exploit-kit	RIG-v	bbsindex	Malvertising	adcash	NDL	Ramnit						
RIG	exploit-kit	RIG-v	bbsindex	BlackTDS	Malvertising	PrimusAd	AUS	Smokebot	XMRig Variant	CoinMiner	mineXMR		

Figure 13: Overview of “bbsindex” traffic activity. We believe the artefact tied to BlackTDS appeared between February 12-19, 2017

BlackTDS runs on a single IP address that proved simple to track. However, at the end of



Figure 14: New BlackTDS home page, retrieved March 4, 2018

Conclusion

Like so many legitimate services, we are increasingly observing malicious services offered “as a Service.” In this case services include hosting and configuration of the components of a sophisticated drive-by. The low cost, ease of access, and relatively anonymity of BlackTDS reduce the barriers to entry to web-based malware distribution. With full support for social engineering and the flexibility to either distribute malware directly or simply redirect victims to exploit kit landing pages, BlackTDS demonstrates the continued maturation of crimeware as a service. Moreover, it demonstrates that, despite their steady decline, EKs and web-based attacks are not a thing of the past. On the contrary, web-based attack chains are increasingly incorporating **social engineering**, taking advantage of both existing underlying infrastructure and human fallibility rather than short-lived exploits.

Acknowledgement:

Thanks to @nao_sec for sharing the Japanese regionalized version of the Social Engineering templates.

blacktds[.]com	Domain	Customer facing domain from middle of december 2017 to end of february 2018
blacktds[.]cf	Domain	Customer facing domain starting 2018-03-04
88.99.48[.]65	IP	Both Victim and Customer facing IP from middle of december 2017 to end of february 2018
46.30.45[.]78	IP	Both Victim and Customer facing IP starting 2018-03-04
en.sundayloop[.]com 193.70.73[.]251	domain/IP	BBSindex redirector from 2017-02-06 till 2017-09-18 (earlier version of BlackTDS in private mode)
6a207ea9d9e60a9bc9de7b1c2b87e06fa85ac31cbbf8c69e1627408c8f3d2b7f	SHA256	PDF attachment with link to blackTDS - 2018-02-19

MOST RECENT



6 DAYS AGO

Leaked source code for Ammyy Admin turned into FlawedAmmyy RAT



1 MONTH AGO



1 MONTH AGO

Proofpoint Q4 2017 Threat Report: Coin miners and ransomware are front and center



2 MONTHS AGO

Holiday lull? Not so much

RELATED LINKS

- [Ransomware Survival Guide >](#)
- [Threat Reference >](#)
- [Proofpoint Blog >](#)
- [Threat Insight Blog >](#)
- [Events >](#)
- [Media Contacts >](#)

COMPANY INFORMATION

- [> About Proofpoint](#)
- [> Board of Directors](#)
- [> Careers](#)
- [> Corporate Blog](#)
- [> Investors Center](#)
- [> Leadership Team](#)
- [> News Center](#)

QUICK LINKS

- [> Daily Ruleset Summary](#)
 - [> IP Address Blocked?](#)
 - [> Threat Insight \(blog\)](#)
-

 SEE ALL CONTACTS



REGIONS

United States United Kingdom France Germany Spain Japan Australia

© 2018. All rights reserved. [Privacy Policy.](#)
