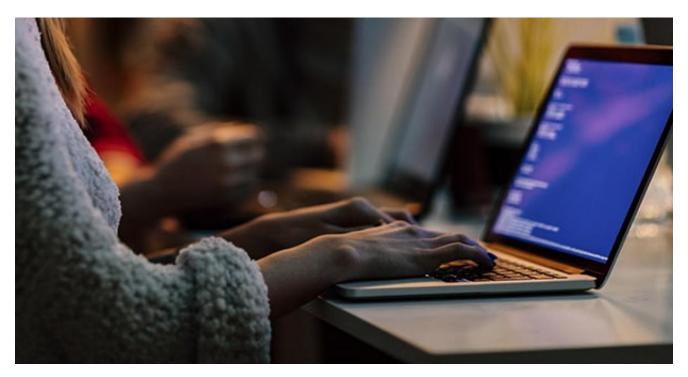
Death Comes Calling: Thanatos/Alphabot Trojan Hits the Market

proofpoint.com//us/threat-insight/post/Death-Comes-Calling-Thanatos-Alphabot-Trojan-Hits-Market

March 10, 2016





<u>Threat Insight</u> Death Comes Calling: Thanatos/Alphabot Trojan Hits the Market



March 10, 2016 Proofpoint Staff

Proofpoint researchers discovered a never-before-documented malware strain on February 15. Dropped by the Nuclear exploit kit, further investigation showed that the malware was a new Trojan called Thanatos by its developers and that we refer to internally as "Alphabot".

Thanatos is being marketed as a service with both short and long-term subscriptions and support and the authors claim it is under ongoing development with new plugins and functionality being actively added.

The following analysis details what we have observed and uncovered so far.



Figure 1 : Nuclear Pack dropping "Alphabot", first observed on February 15, 2016

The malware sample analyzed contains the following program database (<u>PDB</u>) path, on which we based the bot's name:

H:\Alpha\Bot\Release\Loader.pdb

The malware performs HTTP requests to its command and control (C&C) server, for example *alpha[.]highclasssoftware[.]ru/gate.php*, as shown in Figure 2. Proofpoint currently detects this malware based on this C&C communication.

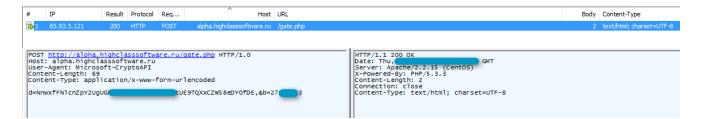


Figure 2: "Alphabot" calling home

Further examination of the malware shows that it modifies the Windows Registry to start the malicious binary during startup (Fig. 3). Like <u>a number of other malware authors</u>, the registry key invokes Brian Krebs in the naming convention:

```
Installs itself for autorun at Windows startup
```

```
key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\KrebsOnSecurity
data: C:\WINDOWS\System32\rundll32.exe C:\DOCUME~1\John\LOCALS~1\APPLIC~1\MICROS~1\21153823.dll,Entry
```

Figure 3: One more Krebs malware meme

Malware For Sale

On March 6, we found an underground advertisement for a new Trojan. While we cannot publicly disclose how we connected the dots, the following advertisement is describing "Alphabot." The description underscores features such as Download/Execute, Form Grabber, Update and future plugins such as HiddenVNC, HiddenFTP, SOCKS and WebInjects.

Thanatos Bot [IE/FF/Chrome/MSE]

Greetings users of [REDACTED] - I would like to introduce to you trojan "Thanatos".

Important aspects of Thanatos?

Programming Languages: C++, Masm, Delphi

OS: Windows XP/2003, Vista/2008, 7, 8, 8.1/2012, 10

Admin Rights Required: No, Thanatos runs in user-mode

Unicode Supported: Yes, Thanatos can run on any system language Size of stub: 150 - 350 kb, it varies depending on your build expectation

Run-time FUD Support: Yes, i will provide updates to bypass most heuristics & proactive of AV

Scan-time FUD Support: No, this part is on you (use any crypter that you wish)

Cross-architecture Support: Yes, Thanatos is able to inject code into both x86 & x64 processes, it is important to take note that x64 code injection on Windows 10 will not work (I am working on patch to re-open Heavens Gate)

What is functionality inside Thanatos?

Formgrabber Support: Yes, form grabber will inject both x86 & x64 browsers on either x86 or x64 versions of Windows. Currently there is support for

IE (Internet Explorer), IE7/8/9/10/11, hooks will bypass Protected Mode too!

FF (Firefox/Mozilla), FF, all versions are supported (both nss3/nspr)

GC (Chrome/Chromium), GC30-46,48+ (working on fixing an issue in 47)

MSE (Microsoft Edge), Hook into explorer.exe waits for RuntimeBroker.exe, followed by injection into MicrosoftEdgeCP.exe to hook HttpSendRequestW/A (same as IE)

To-be added: Opera, Safari

Download/Execute (EXE, JAR, SCR, COM, etc) OR Inject (DLL, .PLUG = Plugins)

Update (If you receive an update build, make an update task so your bots will live longer)

Anti-hook: Removes hooks in target processes from other bots so that no one (other bots on same victim) will have your logs

Bot-killer: AV-Module will scan for other bots on the system, and will remove them once detected (scans task scheduler, registry, services (if admin), and environment variable paths). If the process is considered malicious (from 3-8 hardcoded flags), it will upload file to virustotal.com and parse results from page, if detection on > 3 AV's then malicious file will be removed from system!

Watermark: All builds are watermarked with a unique customer-id, if you leak, then your license will be terminated

What do I get with purchase of my license?

Infinite rebuilds for the duration of your term

Panel (web component, if you're hosting on your own servers loncube loader is required)

Updates of your stub whenever a change is made (by my team)

Runtime patches to evade heuristic or proactive detection engines

Full support (my team is located in various countries, support can be around the clock, 24/7)

Important Notes

If you are in need of an Exploit Kit (Private), Traffic (From our affiliate), or Crypt (Homemade), Bulletproof Hosting (feedback from previous customers available) then you should not worry as we can offer it as well.

What are the plans for the future?

We will be working on improving this trojan for as long as there is interest in our product. We can make anything that you request, and if you have any suggestions you can always let us know, and we will try our best to meet your standards to the highest degree possible!

We also have plans to write additional plugins to help you make money. In the coming months, along with everything stated above we plan to make the follows unique plugins (from scratch):

HiddenVNC

- This will not be a rip-off of Zeus like everyone before us
- We plan to make ours much more stable in terms of connection speed & encoding quality
- This plugin will not require admin permissions and but will require a back-connect server

HiddenFTP

- This will be a plugin similar to that of the Ramnit bonnet
- You will be able remotely download/upload files from the victim you choose
- This plugin will not require admin permissions and but will require a back-connect server

SOCKS4b/5

- This plugin will bypass NAT/Network Firewall
- It will work with a back-connect server and not through SSH

WebInjects

- This will be the first plugin to be added
- This plugin will be much faster than Zeus Web Injects
- It will not stress the loading time of webpages and will be affective with both HTTP/HTTPS

- Web Injects will have the option to be grabbed remotely (can affect loading time of webpage) or they can be stored locally (will not affect the loading time of webpage)

- There will also be an option to update the web injects locally from the panel (web server) when a web browser is not opened

Rootkit

- We have already written a rootkit for Ring-3, it works on both x86/x64

- We are deciding whether to make a Ring-0 rootkit or stick with the current one

- It is important to take note that in our own tests some of our bots with AVs have lived greater than 1 month without an update and the core component of or 4-stage dropper still remains FUD

What is the price for a license?

The price for Thanatos depends on the term which you wish to purchase it for, the schematic is as follows (each term comes with everything stated above):

1 month rent = \$1,700 USD 3 month rent = \$4,800 USD 6 month rent = \$9,200 USD

Lifetime License = \$12,000 USD

If you wish to talk about the pricing/license/more-info you can contact me in jabber, please note ONLY the jabbers below are used by me, every other jabber that is NOT listed below should be assumed a ripper.

ESCROW IS ACCEPTED

Jabber (XMPP):

- #1 [redacted]@sj.ms
- #2 [redacted]@null.pm
- #3 [redacted]@exploit.im

The author of the advertisement is also showing images of the C&C panel which are included below. Here are a few important takeaways from the advertisement:

- The authors appear to be well-embedded in the cybercrime underground and are ready to make life as easy as possible for future customers. Offering private exploit kits, affiliate traffic, packing (crypt services), and hosting makes this something of a one-stop shop for cyber criminals.
- The malware makes use of <u>VirusTotal</u> to scan for other suspected malware on infected machines. While the "bot killer" functionality isn't new, the conditional upload to VirusTotal is unusual, helping to ensure that other malware doesn't have access to the data on the infected PC.
- Ongoing updates make this "malware as a service" even more attractive to prospective customers.
- The malware supports all major versions of Microsoft Windows, and they specifically mention support for Microsoft's 8-month-old Edge browser.

Thanatos in action

The following screenshot is the Thanatos home page, according to the ad.

\$THANATOS				O Server Time: 21:32 06-03-201
	5,389 BOTS Total	31 BOTS	1,038,443 LOGS	34 COUNTRIES
📸 Home 🔸				
🐸 Bots 🗸 Overview				
Logs 🗸 Top 5 Countries		World Map		
📶 Statistics 🗸				
📰 Tasks 🗸	Other Countries			
击 Users	34.28%			
Options			3	
Cogout				
System Stats 🗸				
32-Bit 3,921 64-Bit 1,468 Unknown Arch 0				
Windows 7 1,541 Windows XP 1,037 Summary				
Windows 8 296 Windows 8.1 1,328 Windows 10 764				
Windows Vista 98 Total Bots:		5,389		
Status Bots Online:		3,119		
Alive 5,389 Dead 31 Online 3,119	ast 24H):	5,004		
Offline 2,270 New Bots (Past	t 24H):	134		

Figure 4: Thanatos C&C home page

The remaining panel pages from the advertisement are self explanatory and we present them with captions only.

ana†⊙s					Exten	ded information for 168F20EE	×				O Server Tir	ne: 21:24 06-03-201
	Show 10 \$	entries			Bot Info Logs						Search:	
ome ┥	Bot ID	IP	Country	0 OF	Computer Name:	Administrator	ection) Tasks) Status	Logs	Options	
ots 🗸	E354E572	173.177.60.28	i+I Canada (CA)	Win	User Name:	POS-WINSERV	go	No Task	Online	œ	i 😑 🔺	
şs 🗸	F46CC811	197.162.157.165	Egypt (EG)	Win	IP:	136.243.251.156	minute ago	No Task	Online		i 🔒 🔺	
Ť	CFBE691D	109.240.167.249	+ Finland (Fi)	Win	Admin: OS Info:	Yes Windows Server 2012 R2 (x64)	go	No Task	Online	œ	i g ±	
rtics 🤝	168F20EE	136.243.251.156	Germany (DE)	Win	Country:	Windows Server 2012 R2 (X64)	go	241184721	Online	æ	i e 🔺	
s 🗸	0/4/6264	201.170.2.210	I-I Mexico (MX)	Win	City / Region Name:	Unknown / Unknown		No Task	Online	æ	i e ±	
					ISP:	Ltda.	gu					
rs	1970F3BF	92.84.15.109	Romania (RO)	Win	Bot Owned:	24 Day(s), 13 Hour(s), 3 Minute(s), 11 Secon		No Task	Online	œ	i 🔒 📥	
ons	F5004EC5	85.229.71.251	E Sweden (SE)	Win			minute ago	No Task	Online	ß	i 😑 🔺	
ut	E61C70FE	88.233.133.175	🖾 Turkey (TR)	Win			go	No Task	Online		i 🔒 🔺	
_	69E35246	195.114.158.169	Ukraine (UA)	Win		Close 📥 Save Sur	go	No Task	Online	œ	i 😫 📥	
its 🗸	9355C201	213.5.194.164	Ukraine (UA)	Windo	ows 7 (64-Bit)	07/02/2016 17:13:46	3 minutes ago	No Task	Online		i 8 🔺	
.	Bot ID	IP	Country	Ope	rating System	First Connection	Last Connection	Task	Status	Logs	Options	
_	Showing 1 to 1	0 of 5,389 entries									Previous 1 2 3 4 5	
_												

Figure 5: Bots Page

≜ тнанат⊙s	a de la construction de la constru En la construction de la constructio
	Method: DL & Execute \$
倄 Home	DL & EXEC Options
🐸 Bots 🗸	File URL: http://myserver.com/miner.dll
🔓 Logs 🗸	
III Statistics 🗸	Task Options Name:
Tasks 🗸	Partner #2 - Mining Task
	Maximum bots exec (Total Bots: 5,389) [7]:
Users	0
Options	Initial task state:
P Logout	Inactive Targeting Options [7]
System Stats 🗸 🗸	Countries [7]: × United States (732) × Germany (116)
Status 🗸	
	Save Task CANCEL
	Total Page load in seconds: 0.023

Figure 6: Create a Task

<u></u> етнан/	∆ ≭ ⊙\$								0	Gerver Time: 21:20 06-03-2016
		Task(s)								
倄 Home		1038(3)								
🐮 Bots	~	TASK ID	туре	CREATED	#SUCCESS / FAILED / MAX	STATUS	OPTION		Delete all completed tasks	Suspend all active tasks
Logs	~									
		241184721	Download & Execute	06/03/2016 21:20:03	0/0/	Suspended	View Tas	k Info Delete Co	ntinue Task	
III Statistic	cs 🗸									
Tasks	~									
🖶 Users										
Option:	s									
r Logout										
System Stats	×									
Status										

Figure 7: Viewing a Task

етнанат о	૭ઙ									0	erver Time: 21:20 06-03-20	16
					Task Information 241184721	×						
		Task(s)			NAME	VALUE						
😤 Home					Name	Partner #2 - Mining Task						
Aut .					Task ID	241184721			Delete all tasks	Delete all completed tasks	Suspend all active tasks	
🕍 Bots 🗸	´	TASK ID	TYPE	CREATED	Command Type	Download & Execute	TATUS	OPTION	s			
🔓 Logs 🗸					Command Details	File URL: http://myserver.com/miner.dll						
		241184721	Download & Execute	06/03/2016 21	Target Specs.	0	Suspended	View Tas	k Info Delete Co	ontinue Task		
📶 Statistics 🗸					Target Coutries	US,DE						
					#Success / Failed / Total	0 / 0 / Unlimited						
📰 Tasks 🗸	·				Status	Suspended						
🖶 Users					Added	06/03/2016 21:20:03						
See Oscis					Bot List	848(Show List)						
Options												
r Logout						Close						
System Stats 🗸												
Status 🗸												



&THANATOS			© Saver The	e: 20,55 06-03-2016
			1	A Export All
19 Home	Show 10	1 entries	Search:	
철 Bots 🗸	BotiD	Browser	Most	Details
🖺 Logs 🗸		MSIE 11.0	https://w.skype.com/login/oauth/prosy/tresponse_type+pontmessage&client_id=580081&redirect_uri+https://dub112.mail.live.com/default.aspx&state=silentiogineds_14551208705838&/orm=microsoft_silent_login&site_name=hx.skype.com&wa=wsignin1.0	Details
🗐 Statistics 🗸		MSIE 11.0	https://login.live.com/login.srf/bwarwsignin1.0&rponv=12&ct=1455121448&rver=6.5.6510.0℘=54_20MIN&wreply=https://account.live.com/activ/ty&id=38936&waid=1066a0be5ea54d14b10640685e732aa&bi=1455121451&mit=FR- FR⁣=108&lostproofs=1	Details
🎬 Tasks 🗸		MSIE 11.0	https://h-fs-facebook.com/	Details
atta Users	AASE3F54	MSIE 11.0	https://r-fs.facebook.com/	Details
Coptions	AA9E3F54	MSIE 11.0	https://www.facebook.com/login_php?login_attempt=1&wv=110	Details
r Logout	AA9E3F54	MSIE 11.0	https://www.facebook.com/	Details
System Stats 🗸	AA9E3F54	MSIE 11.0	https://www.sh.fricad/ogin/ban/co-https://messagerio=12.shr.frivebmail/j.spring_cas_security_check	Details
Status v	AASE3F54	C MSIE	http://www.sfr.fz/cas/login/domain-mire-sfrmalikaen/ce-https://messagerie=12.sfr.fz/webmail/j_spring_cas_security_check	Details
	AA9E3F54	MSIE 11.0	http://www.sfr.fr/zas/ogin/doarnaiovmine-sfrmail&cenvice=https://messagerie=12.sfr.fr/webmail/j_spring_cas_security_check	Details
	AASE3F54	MSIE 11.0	http://www.sfr.fr/cas/togin/doinain-mine-sfrmali8.service-https://messagerie-12.sfr.fr/webmalif_spring_cas_security_theck	Details
	BotiD	Browser	Host	Details
	Showing 12,	191 to 12,200	0 of 1,038,443 entries	Next Last

Figure 9: Viewing Logs

≜ тнанат⊙s			
😤 Home 🖣	User Management		
🐮 Bots 🗸	New Username:		
🔓 Logs 🗸 🗸	New Password:		
III Statistics 🗸	Repeat Password:		
📰 Tasks 🗸	Permissions:	Select a Page	
	Contact Type:	1	
users	Contact Data:		
Options		Submit CANCEL	
r Logout	USERNAME	PERMISSIONS ACTIVATED	

Figure 10: User Management

User Management	
New Username:	
New Password:	
Repeat Password:	
Permissions:	× Bots
Contact Type:	Home Statistics Table
Contact Data:	Statistics Graphs
	Tasks View Tasks Add Tasks Modify
	Options
USERNAME	Users

Figure 11: User Permissions

ЕТНАНАТО S			Ø Server Time: 21:31 06-03-2016
僧 Home	Settings		
📸 Bots 🗸	New Password: Repeat Password:		
📶 Statistics 🗸	I	Submit CANCE	
📰 Tasks 🗸	New Username:	Submit CANCEL	
Options	Offline limit (mins):	30	
r Logout	Dead limit (days):	7 Ownye: <u>CANCE</u>	
	Dead Bots:	31 Delete Dead Bots	

Figure 12: Panel Settings

Conclusion

Although we have yet to see widespread use of Thanatos, it appears to be a robust, fullfeatured new Trojan. Based on the author's description in the ad, Thanatos will be a flexible tool for threat actors. The comparisons to Zeus give hints about expected uses. For Thanatos/Alphabot, the authors appear to be ready to provide access to a complete ecosystem of underground tools, making this new Trojan attractive to malicious actors and worthy of attention from organizations and security vendors.

We will be actively watching for new developments and appearances in the wild and updating protection as needed.

IOCs

Thanatos :

6b6978726960c090479ab6a67b05eb62d1d4894b89fa6d094be31b7f71c3913a 2085db7e7764e0693fe128fa7530338af8c8c598d1f3a85a2299991248ec553a 6043a9d69eee2994d330b891d29115e95d5466fb0673932e85c16a4c0232b81b

C&C : alpha[.]highclasssoftware[.]ru 85.93.5.121

Rules :

2816233 ETPRO TROJAN Thanatos CnC Post

Subscribe to the Proofpoint Blog