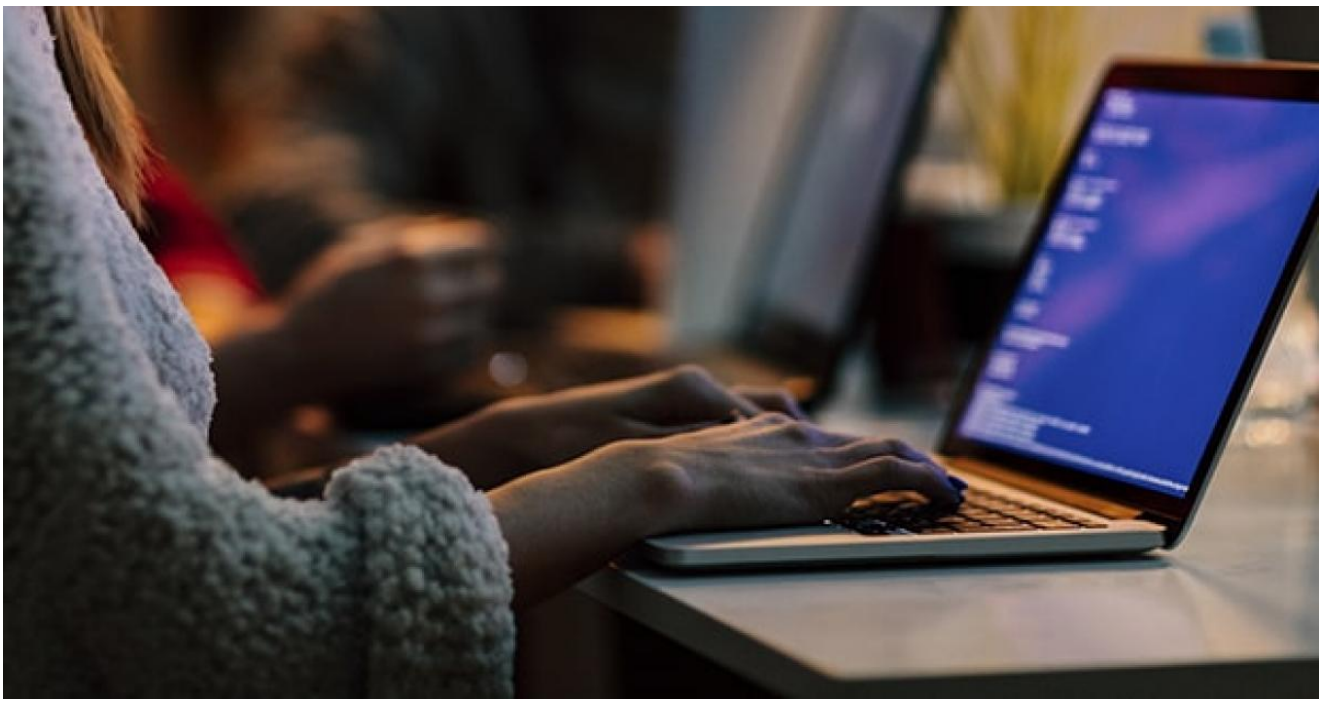
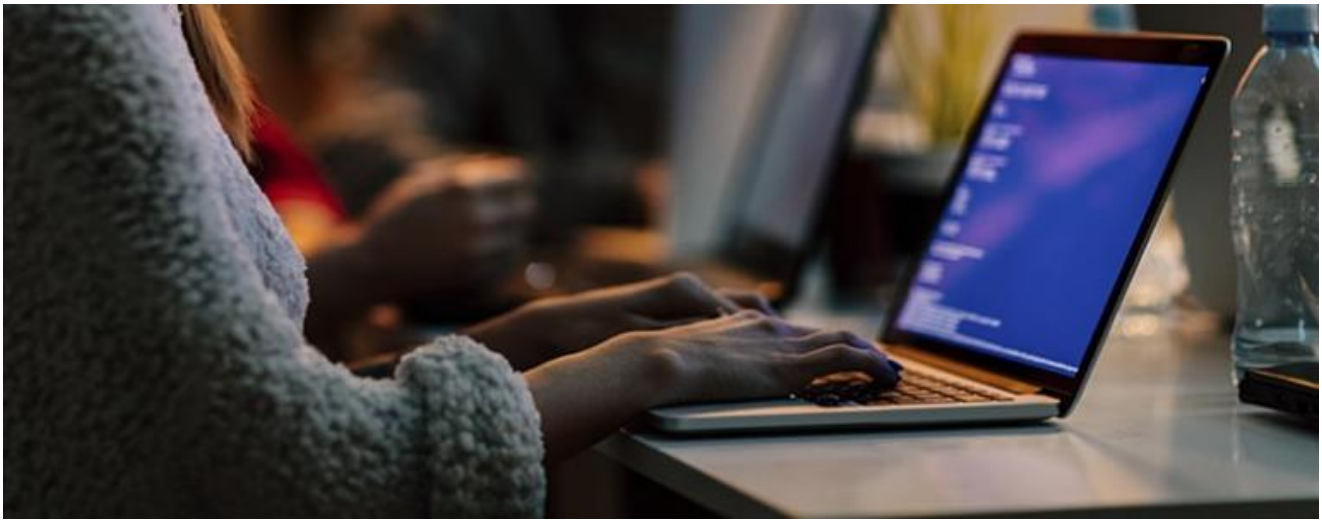
Death Comes Calling: Thanatos/Alphabot Trojan Hits the Market

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

March 10, 2016



Blog
Threat Insight
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.

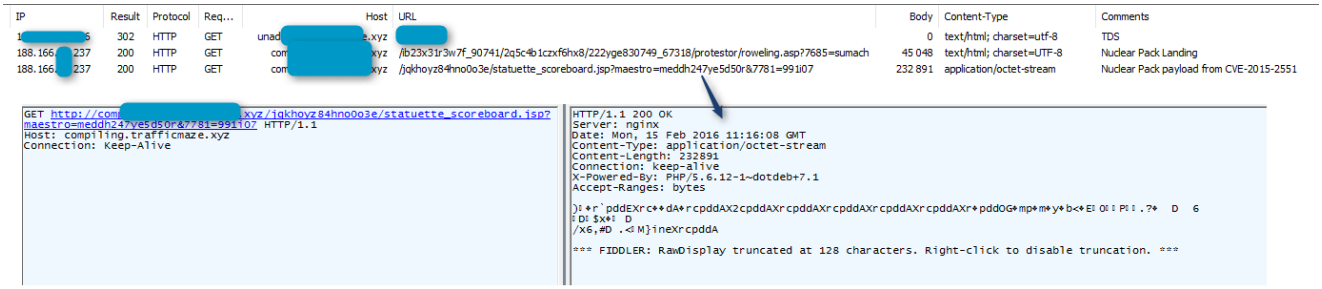


Figure 1 : Nuclear Pack dropping "Alphabot", first observed on February 15, 2016

The malware sample analyzed contains the following program database (PDB) 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.

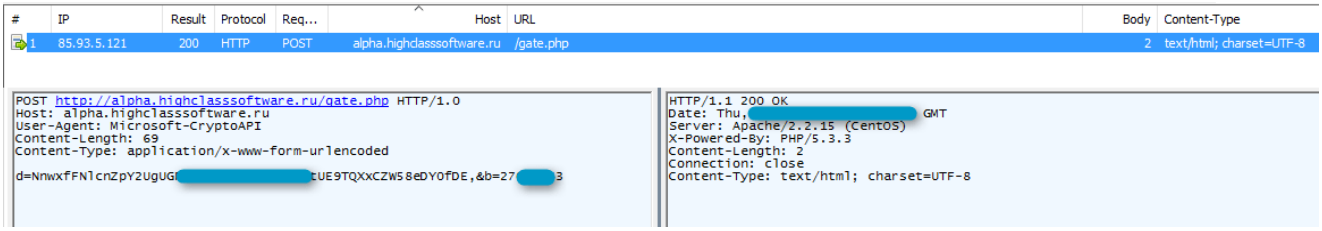


Figure 2: "Alphabot" calling home

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

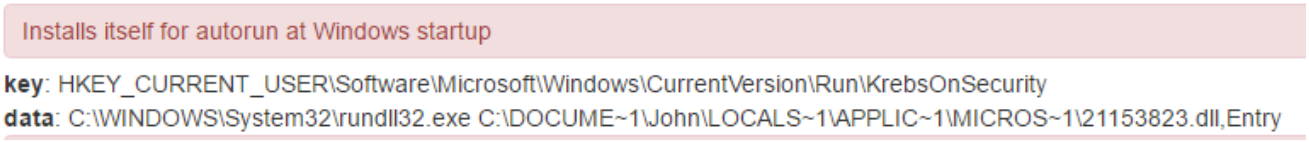


Figure 3: One more Krebs malware meme

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 Ioncube 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 (Home-made), 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 VirusTotal 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.

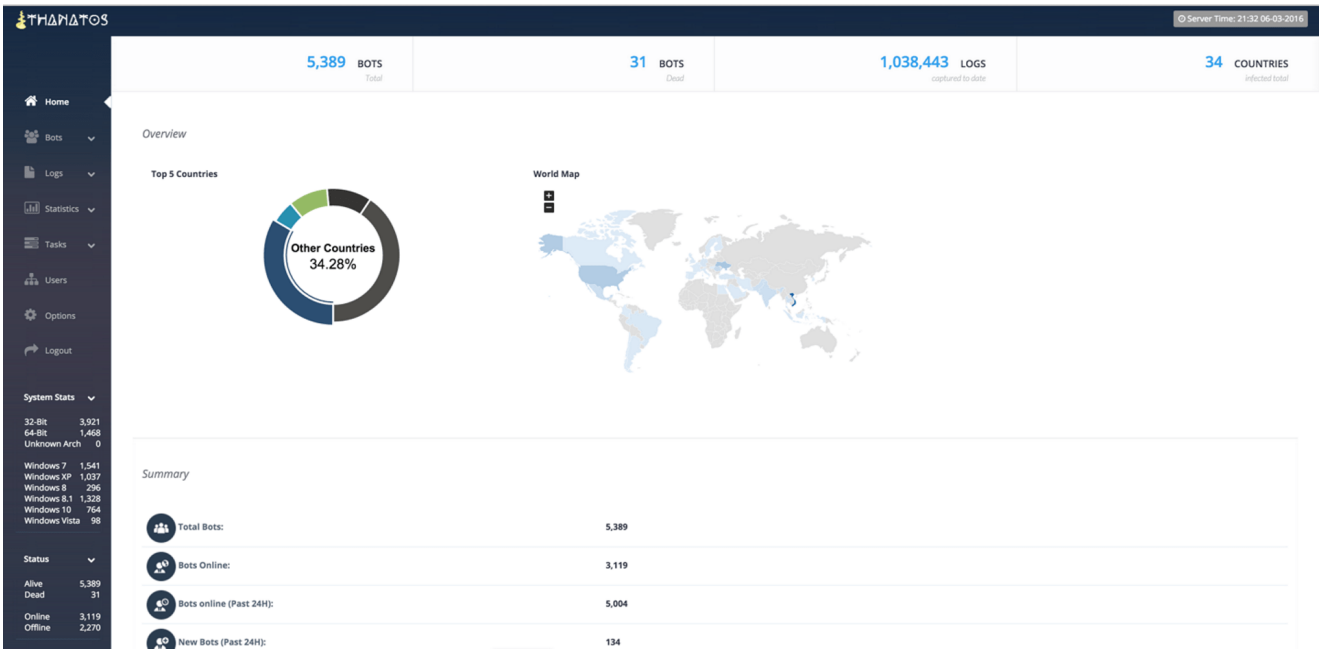


Figure 4: Thanatos C&C home page

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

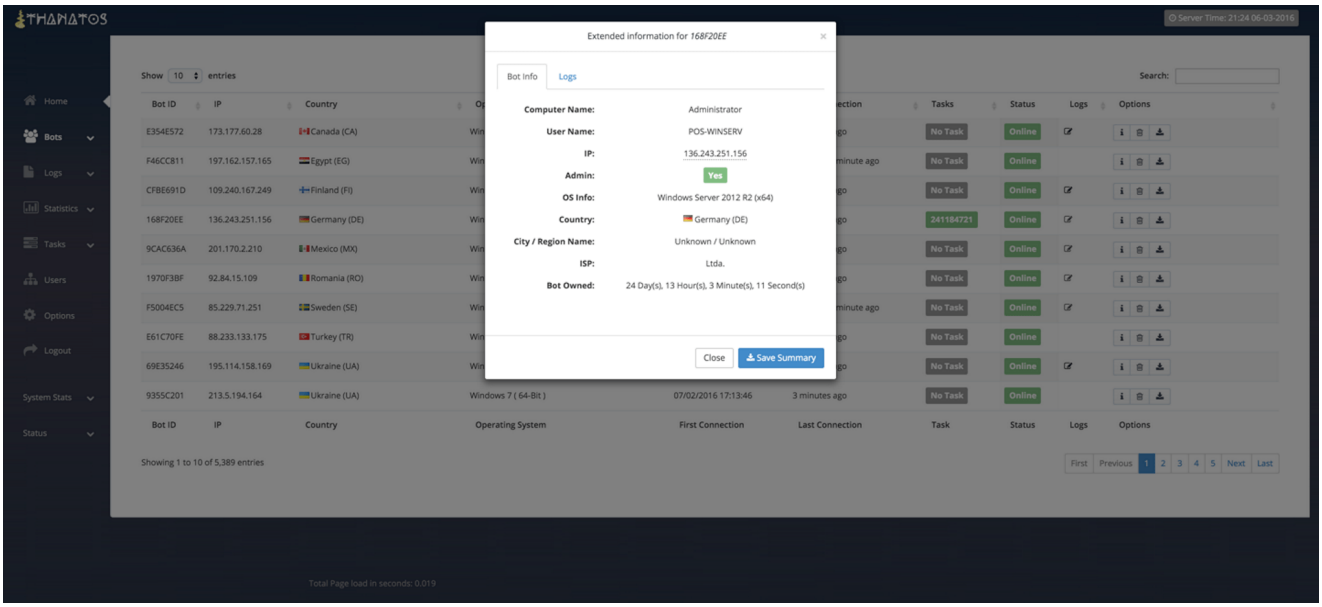


Figure 5: Bots Page

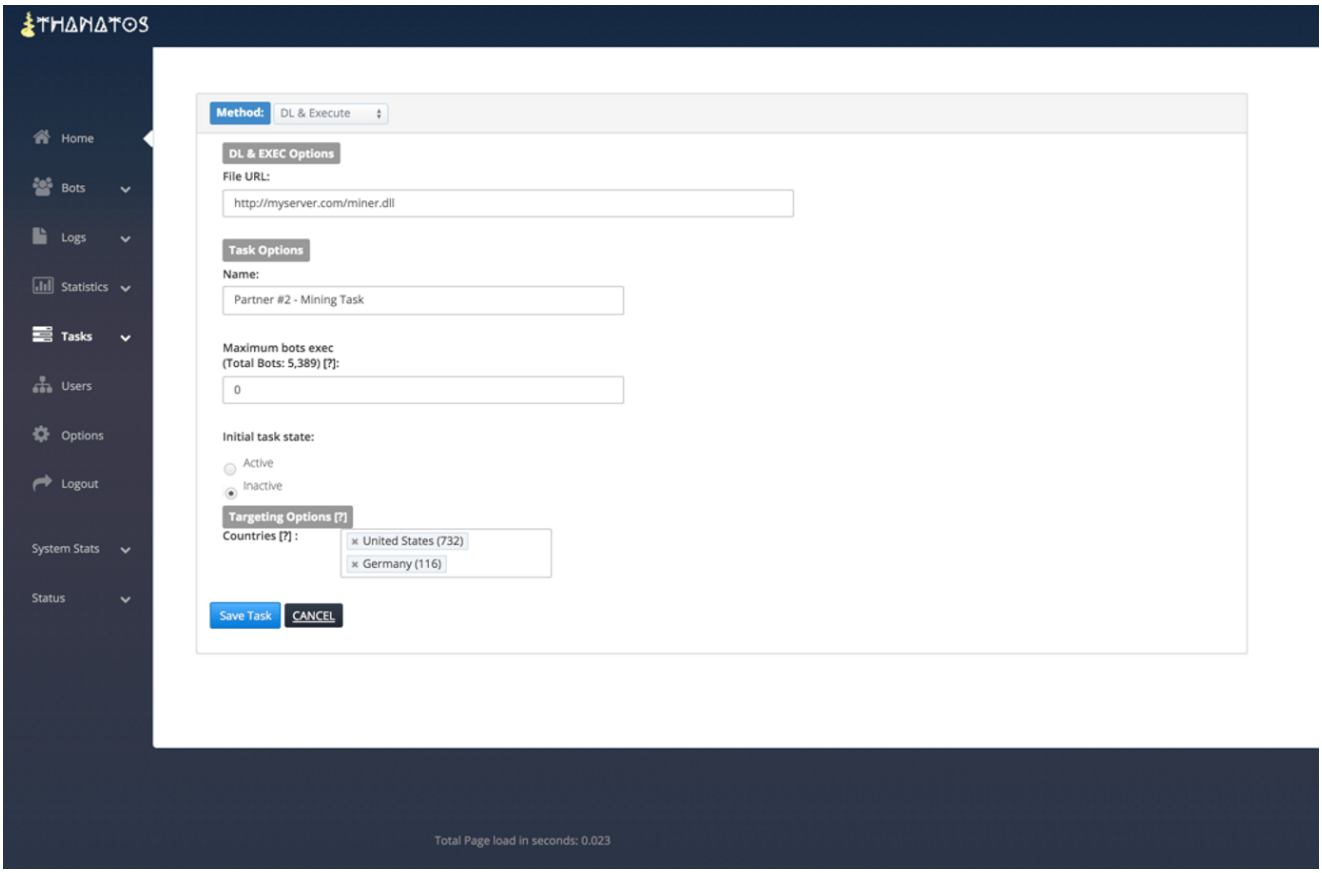


Figure 6: Create a Task

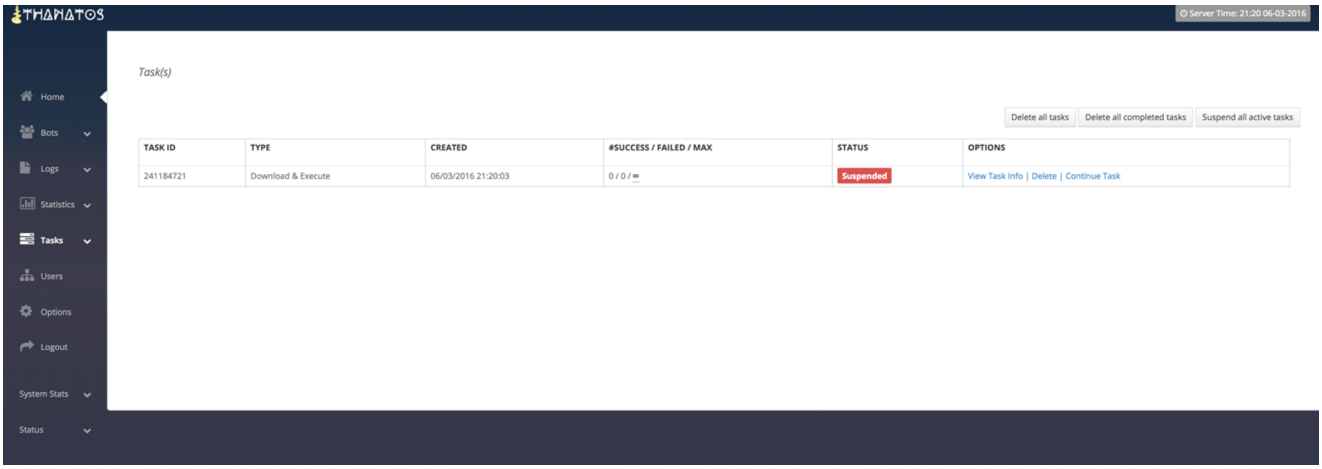


Figure 7: Viewing a Task

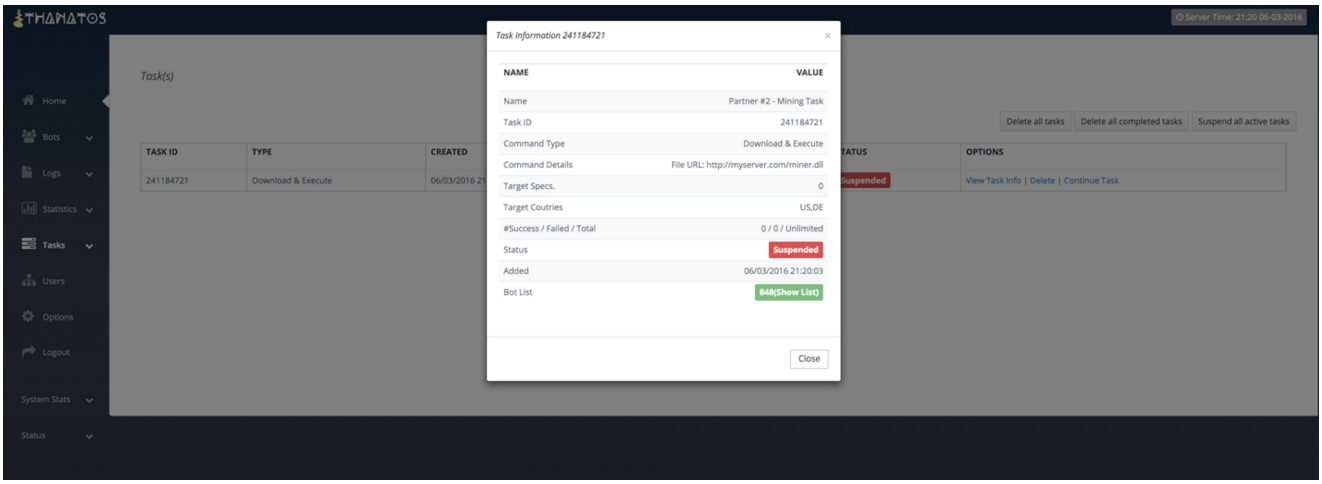


Figure 8: Task Information

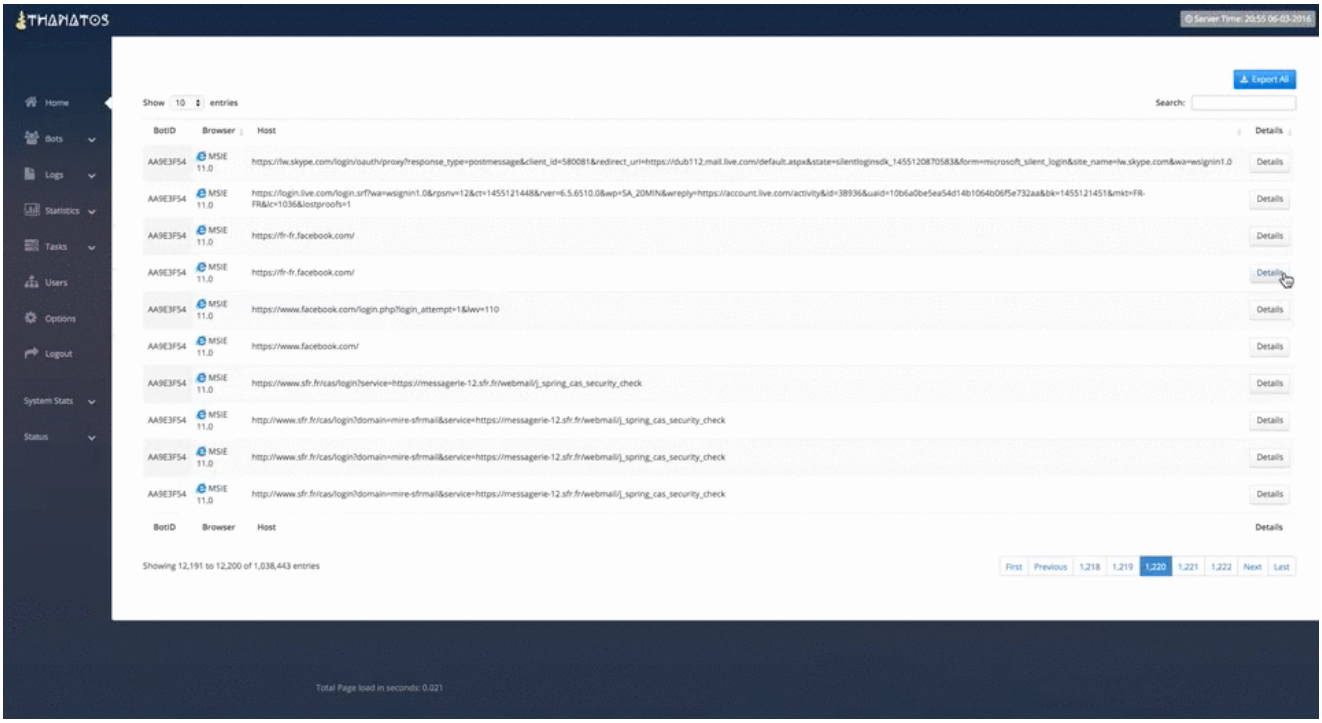


Figure 9: Viewing Logs

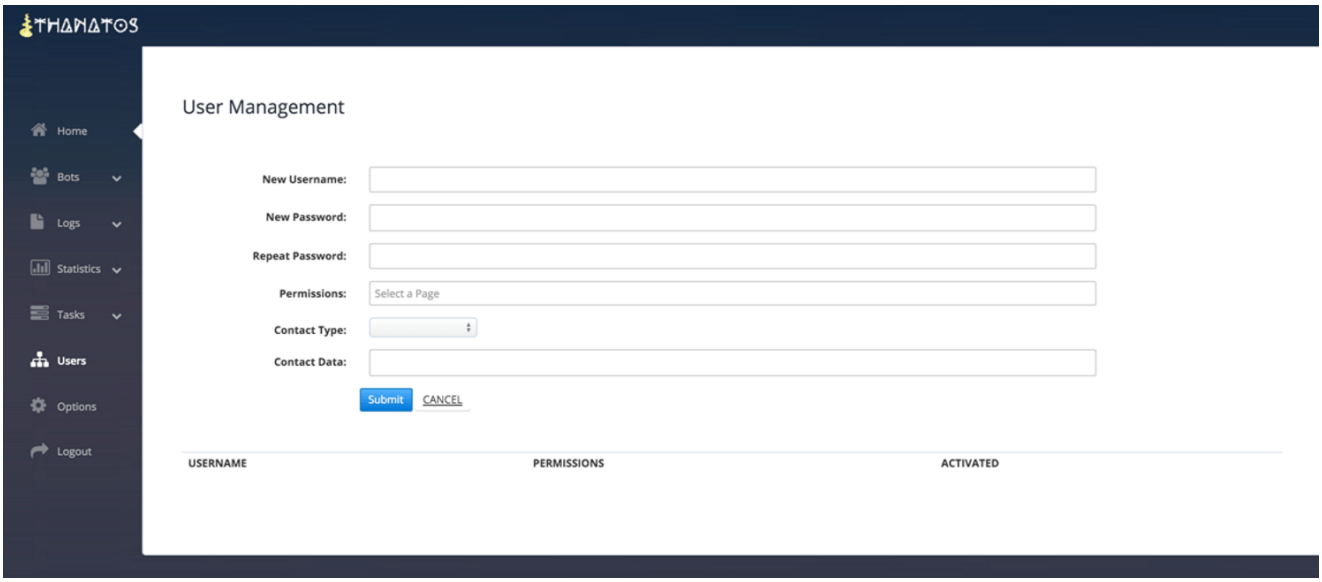


Figure 10: User Management

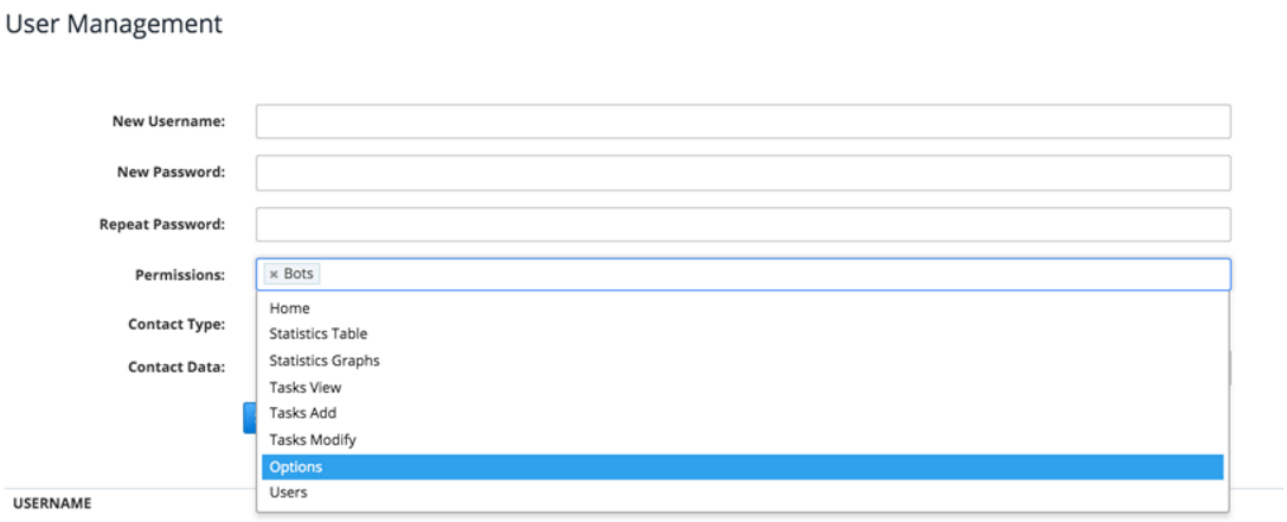


Figure 11: User Permissions

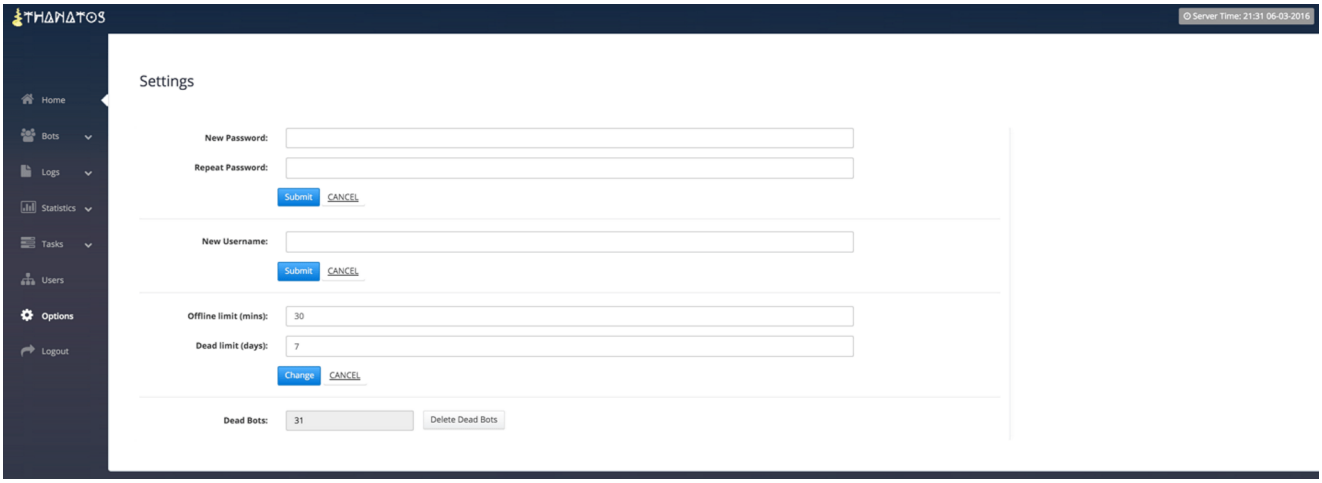


Figure 12: Panel Settings

Conclusion

Although we have yet to see widespread use of Thanatos, it appears to be a robust, full-featured 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