

Forum:[Hack Forums](#)

Thread: [New Zeus Trojan malware is born : Pandemiya](#)

Aura - June 13, 2014, 8:33 am

Hey guys, Aura here with yet another malware alert.

This time, a more serious threat has been discovered. I'm talking about a Zeus Trojan (for more information about this type of malware, read the Wikipedia article [here](#)). Researchers from the FraudAction team of RSA Security found this new threat and code-named it "Pandemiya". This Zeus Trojan malware is sold on underground forums to cybercriminal and is said to be an alternative to the original Zeus Trojan malware, which source code has been leaked and freely distributed on the web and underground forums for the past years. However, Pandemiya appears to be far more sophisticated than the other Zeus Trojan-based malwares : Ciral, Ice IX and Gameover Zeus. This malware is coded in more than 25,000 lines of C (programming language) and with a code of an extreme quality. The researchers are quite impressed with the coding quality of the malware, mostly for the fact that it is not based on Zeus source code at all. They say that the coder might have spent close to a year to code that application. Pandemiya uses Windows "CreateProcess API" in order to inject itself in every new process that is initiated, even system/common processes like Explorer.exe and it reinjects itself when it's needed in order to maintain its persistence. This malware is being sold for around \$2,000 USD on underground forums and an extra \$500 is added to get the plugins of this malware. Because this malware is designed with a modular architecture to load external plug-ins, the users of this malware can add extra features to the original malware by writing new DLL (dynamic link libraries) and attach them to the malware. So far, Pandemiya offers features such as encrypted communication with the command and control server (to make the detection harder), open reserve proxies on infected systems, steal FTP credentials, infect executable files on the system, etc. Apparently, malware developers are already working on new features for Pandemiya, features including a RDP (Remote Desktop Protocol) connection and a Facebook attack module that can be used to spread the trojan through hijacked Facebook accounts.

Interesting fact, this malware appears quite easy to remove by following these instructions :

Quote:1. Locate the registry key

HKEY_LOCAL_USER\Software\Microsoft\Windows\CurrentVersion\Run and identify the *.EXE filename in your user's 'Application Data' folder. Note the name, and delete the registry value.

2. Locate the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDlls. Find the value with the same name as the *.EXE file in the previous step. Note the file name, and remove the value from the registry.

3. Reboot the system. At this stage Pandemiya is installed but no longer running. Delete both files noted earlier. This will remove the last traces of the Trojan. Your system is now clean.

However, this removal procedure seems far too basic and simple for me, therefore I recommend you to get checked by the [MRT](#) if you were to ever be infected with Pandemiya. Follow the instructions in [this thread](#) if you are running Windows XP, Vista or 7 and the instructions in [this thread](#) if you're running Windows 8 or Windows 8.1.

Read the original article here : [Zeus Alternative Pandemiya Banking Malware For Sale in Underground Forums](#)

New threats are discovered everyday and now more than ever is the time to protect your system against these in order to remain safe and secure. Install a good Antivirus, keep it updated, clean your system frequently and use the Web wisely. Also, more than anything else, please watch your downloads and the websites you visit.

Stay safe and secure guys.

xVSPACEVx - June 13, 2014, 9:05 am

Thanks for the Malware News Aura! :)

we r num 1 - June 13, 2014, 9:09 am

Thanks once again Aura for keeping members posted on Malware. You do a great job here on the forum for the sake of helping.

Backwoods Cigar - June 13, 2014, 9:28 am

Thanks for warning hf about this malicious tool.

Keep up the good work.

Keith Cozart - June 13, 2014, 9:29 am

Thanks for this report Aura! Always staying on top of things and helping everyone :)

Aura - June 13, 2014, 9:44 am

Thank you guys.

Hopefully you'll be more alert for this threat and the other threats that exists and are discovered everyday !

incoming - June 14, 2014, 12:58 pm

Actually, the bot has been around since the mid of April as far as I know.

It has some neat features though, especially these who cannot be discussed here, therefore I honestly

doubt a bot that powerful, compared to other common malware, can be removed by simply removing

two registry-keys and deleting the files afterwards. Glad you posted this thread, nonetheless!

Aura - June 15, 2014, 3:21 pm

(Jun 14, 2014 12:58 PM)Fake User Wrote: [\[CITE\]](#) Actually, the bot has been around since the mid of April as far as I know.

It has some neat features though, especially these who cannot be discussed here, therefore I honestly

doubt a bot that powerful, compared to other common malware, can be removed by simply removing

two registry-keys and deleting the files afterwards. Glad you posted this thread, nonetheless!

Exactly why I recommend a user that would be infected with it to go see the MRT to get it removed. This removal procedure is a joke. Even DarkComet crypted with a decent crypter would still be back after this removal procedure.

(Jun 15, 2014 03:01 PM)TheLionsDin Wrote: [\[CITE\]](#) This is obviously a prank.

The real viruses are found in programs like winRAR and Comodo

Out of my thread troll.

temfadbaba - June 15, 2014, 3:26 pm

Thanks for the update you did a nice job

Sinq - June 16, 2014, 10:01 am

Thank you for the warning Aura, another great post.

Regards, ?

Aura - June 16, 2014, 12:02 pm

No problem guys, glad that you appreciate these ! ?

Vextoray - September 29, 2014, 2:16 pm

Thank you very much for the report.

I love the dedication you put into each of your posts.

Aura - October 1, 2014, 6:36 pm

(Sep 29, 2014 02:16 PM)Vextoray Wrote: [\[CITE\]](#) Thank you very much for the report.

I love the dedication you put into each of your posts.

Thank you for the compliment.

Ill however stop posting such articles for now as I have to focus on school. But I'm glad that there's still people that appreciates them.

Ganja™ - October 3, 2014, 2:54 am

Interesting read!

I have a question.

Zeus is so known as "worst malware" but what can Zeus do that other botnet can't?

Thanks for the post!

Aura - October 3, 2014, 8:25 pm

(Oct 3, 2014 02:54 AM)Ganja™ Wrote: [\[CITE\]](#) Interesting read!

I have a question.

Zeus is so known as "worst malware" but what can Zeus do that other botnet can't?

Thanks for the post!

Zeus doesn't do anything that other botnets can't do. The thing is that Zeus Botnet was the first malware of its kind back then, hence why there was such a big deal around it and it was considered the most advanced malware, etc. Now that it had been shutdown, its source code has been leaked, so every malware developer can freely take that source code, modify it and create a new botnet with it. Hence why these botnet malware becomes "variant" of the Zeus Botnet and new features are being added to it as the variants are being created.

picmsncom - October 6, 2014, 2:52 am

Thanks for the informational post, Aura.

However, virus removal for Windows 8 & 8.1 thread doesn't exist anymore, or maybe the link is updated.

Could you please update it?

Thron - October 6, 2014, 2:58 am

Why there is not a coder by Zeus to continue programming ?

Aura - October 6, 2014, 2:40 pm

(Oct 6, 2014 02:52 AM)picmsncom Wrote: [\[CITE\]](#) Thanks for the informational post, Aura. However, virus removal for Windows 8 & 8.1 thread doesn't exist anymore, or maybe the link is updated.

Could you please update it?

This thread was deleted a while ago, now the instruction thread of the MRT also applies to Windows 8 and 8.1.

(Oct 6, 2014 02:58 AM)Thron Wrote: [\[CITE\]](#) Why there is not a coder by Zeus to continue programming ?

Wikipedia ?

[https://en.wikipedia.org/wiki/Zeus_\(Trojan_horse\)](https://en.wikipedia.org/wiki/Zeus_(Trojan_horse))

Antinormality - October 6, 2014, 2:53 pm

USD 2000\$ isn't alot for a malware like this considering that some malwares have been sold for a quarter million or more. Anyways, what is the goal of this malware? The same as Zeus being financial data or something else?

Also I've heard about pandemiya labeled virusses before...?

SIM-1984933 - October 6, 2014, 9:58 pm

[Video: <https://www.youtube.com/watch?v=zvfD5rnkTws>]

Arrandale - October 9, 2014, 7:44 am

Wew, thanks for the info!

--Still learning bro!

Aura - October 10, 2014, 5:53 pm

(Oct 6, 2014 02:53 PM)AR Wrote: [\[CITE\]](#) USD 2000\$ isn't alot for a malware like this considering that some malwares have been sold for a quarter million or more. Anyways, what is the goal of this malware? The same as Zeus being financial data or something else?

Also I've heard about pandemiya labeled virusses before...?

You can except every ZeuS variant malware to have the same primary goal as ZeuS, but with other side-plans, variations too. Also, the new is months old, hence why you heard of it. Someone "gravedigged" the thread.

sashav - January 3, 2015, 8:40 am

Very interesting piece, indeed!

these botmasters become more and more sophisticated

-Hyperion - January 3, 2015, 1:00 pm

(Jan 3, 2015 09:40 AM)sashav Wrote: [\[CITE\]](#) Very interesting piece, indeed!

these botmasters become more and more sophisticated

No need to grave dig a post that dead