

Forum:[Hack Forums](#)

Thread: [\[BHCPU\] Gameover Zeus Botnet being revived !](#)

Aura - July 11, 2014, 9:01 am

[img]http://#.com/wp-content/uploads/2014/07/gameover.png[/img]

Hey guys, Aura here with yet another [WARNING] thread and from now on, they'll be under the name of The Brotherhood Computer Sector, White Hat Help subsector ! ?

You guys all remember the Gameover Zeus Botnet that was taken down around a month ago right ? If not, read these articles to be up to date on the subject :[Gameover ZeuS](#) on Wikipedia

[Gameover Zeus P2P Malware](#) on the US-CERT

[GameOver Zeus botnet seized; Two week window to protect yourself, say authorities](#) via ZDNET

[US disrupts \\$100M GameOver Zeus malware cybercrime ring](#) via CNET

Well apparently, someone or some people are attempting to revive the downed botnet to put it back online again, starting from scratch.

Researchers at Malcovery noticed that a spam campaign was currently in progress and that contains phishing lure that include a .zip archive trapped with a malware. While analyzing the malware, Malcovery discovered that the malware shares around 90% of it's code with the code of the Gameover Zeus botnet malware. What made GOZ so hard to shutdown was his advanced P2P spreading mechanism in order to control and update the zombies that were part of it's botnet. However, this new malware is completely stripped from that P2P code and relies instead on a mechanism known as "fast-flux hosting". This mechanism is a "round-robin technique that lets botnets hide phishing and malware delivery sites behind an ever-changing network of compromised systems acting as proxies, in a bid to make the botnet more resilient to takedowns." (quoted from the article linked below) This new malware also include a DGA (Domain name Generation Algorithm) which is a failsafe mechanism on which the malware can rely on if it's normal communication ways/system fails. This DGA constantly creates a list of domain names (gibberish ones, in the form of "fkejfopwefiJKLHajsjsds") that changes every week. Therefore, if the malware on a computer can't reach the fast-flux servers (Command and Control servers) to receive updates and instructions, the malware will attempt to connect to the domains listed by the DGA in order to connect to an active one and receive updates. It's a security used by botmasters in case that an infected computer cannot use his stand communication method to connect back to the server.

According to Gary Warner, the original Gameover Zeus botnet that was closed/shutdown last month is STILL locked down, which means that whoever is launching this new campaign is planning on rebuilding the botnet from scratch. Warner also says that ""This discovery indicates that the criminals responsible for Gameover's distribution do not intend to give up on this botnet even after suffering one of the most expansive botnet takeovers and takedowns in history". The crooks that were responsible behind the Gameover Zeus botnet kept a low profile in the last month which

surprised the researchers at Malcovery. But it seems that they are now back on the scene and are ready to fight back to retake control of their botnet, even after suffering one of the hardest botnet shutdown and takeover in history.

According to the Justice Department, the Gameover Zeus botnet is the responsible of account takeovers worth over \$100 millions and the author of this botnet is presumably a Russian citizen named Evgeniy Mikhailovich Bogachev.

More information can be found on Malcovery's blog post [here](#) if you want to receive the latest updates on this situation.

It looks like that takedown was too good to be true. Someone or some organization is now attempting to bring back the Gameover Zeus botnet back in the game and we should all be on our guards since this is one of the most advanced botnet there is.

I would like to recommend you all once again to be careful on what you do on the web, what you download, etc. and to ALWAYS keep your OS updated and protected with an Antivirus and other protection softwares in order to stay as secure as possible.

I'll update this thread whenever new development comes out.

Stay safe and secure guys !

This thread was inspired by the current Gameover Zeus botnet article on # that can be found here below :

[Crooks Seek Revival of 'Gameover Zeus' Botnet](#)

Update : New article on TheHackerNews [After Takedown, GameOver Zeus Branking Trojan Returns Again](#)

Aceman - July 11, 2014, 10:44 am

That was an interesting read. I love reading about the intricate ways in which these massive botnets work. The coders behind them are nothing short of impressive and could surely do a lot of great things if they were white hat. It's just a shame that blackhat pays so much better if you're Russian and won't get extradited to the US.

Aura - July 12, 2014, 4:11 pm

(Jul 11, 2014 10:44 AM)Aceman Wrote: [\[CITE\]](#) That was an interesting read. I love reading about the intricate ways in which these massive botnets work. The coders behind them are nothing short of impressive and could surely do a lot of great things if they were white hat. It's just a shame that blackhat pays so much better if you're Russian and won't get extradited to the US.

That's the biggest issue. China and Russian hackers are hyperactive because most of their targets are in the US and they don't have any extradition accord when it, which means that they are safe to do "whatever" they want on the web and face little to no consequences at all. However, someone will have to put a real end to this in a way or another.

Sacred Symmetry - July 12, 2014, 4:17 pm

This is very interesting.

Amazing actually.

Regards

Agent Shark - July 12, 2014, 4:19 pm

It makes you wonder when the white hat field will become the more dominate. It seems white hats are always on edge with these malicious coders.

Aura - July 12, 2014, 8:11 pm

(Jul 12, 2014 04:19 PM)Sh?rk Wrote: [\[CITE\]](#) It makes you wonder when the white hat field will become the more dominate. It seems white hats are always on edge with these malicious coders. Exactly.

But fear not Shark. Once you and me gets in the game one day when we graduate, we'll bring a good hand to the IT Security World ?

Updated the OP with an article from TheHackerNews.

nextbeats12 - July 26, 2014, 6:28 am

nice one :) this is really helpful i will try it out

Aura - July 26, 2014, 8:40 am

(Jul 26, 2014 06:28 AM)nextbeats12 Wrote: [\[CITE\]](#) nice one :) this is really helpful i will try it out What do you mean you'll try it out ? ...

Black Hats out of this section.

VirusTotal - July 26, 2014, 8:42 am

Thanks for the warning Aura ;)

Good job as usual!

HIGH PAID FELLA - July 26, 2014, 11:28 am

(Jul 12, 2014 04:11 PM)Aur? Wrote: [\[CITE\]](#) That's the biggest issue. China and Russian hackers are hyperactive because most of their targets are in the US and they don't have any extradition accord when it, which means that they are safe to do "whatever" they want on the web and face little to no consequences at all. However, someone will have to put a real end to this in a way or another.

Putin does, he will make you a millionaire if you crack down Tor.

Only thing, all the exit nodes are getting killed already so yeah.

Aura - July 26, 2014, 11:36 am

(Jul 26, 2014 11:28 AM)Asterea Wrote: [\[CITE\]](#) Putin does, he will make you a millionaire if you crack down Tor.

Only thing, all the exit nodes are getting killed already so yeah.

Putin is ready to pay you to do whatever you can that would piss off the US or put them in a bad situation.

HIGH PAID FELLA - July 26, 2014, 11:38 am

(Jul 26, 2014 11:36 AM)Aur? Wrote: [\[CITE\]](#) Putin is ready to pay you to do whatever you can that would piss off the US or put them in a bad situation.

That is bad for the Russians isn't it? Plz care to explain?

Aura - July 28, 2014, 5:06 am

(Jul 26, 2014 11:38 AM)Asterea Wrote: [\[CITE\]](#) That is bad for the Russians isn't it? Plz care to explain?

It's bad for everyone to be honest. We all know that the TOR network is being used by people that wants to hide from the government, and some of them use it to prepare "attacks" or "releases" against it. So if a government was to break the TOR anonymosity and manage to see who's using it, from where and for what, well these people would be in big trouble. Also, we all know how Russia is, law-sided, and that would be very bad for them ...

onyeoga - August 23, 2014, 8:50 am

very interesting post learnt a lot from it..would put into prsctice soon

Aura - October 4, 2014, 5:48 pm

(Aug 23, 2014 08:50 AM)onyeoga Wrote: [\[CITE\]](#) very interesting post learnt a lot from it..would put into prsctice soon

What do you mean ? Don't put that into practice ... actually equip yourself to defend against that comeback.

hyp3ri0n - October 9, 2014, 3:48 pm

I had to deal with a Gameover Zeus variant on a laptop at work last week. It was dropped by worm then the worm deleted itself and then the Trojan ran. The only way we caught it was because we caught the traffic being sent to a CC server. ?

Aura - October 10, 2014, 5:52 pm

(Oct 9, 2014 03:48 PM)hyp3ri0n Wrote: [\[CITE\]](#) I had to deal with a Gameover Zeus variant on a laptop at work last week. It was dropped by worm then the worm deleted itself and then the Trojan ran. The only way we caught it was because we caught the traffic being sent to a CC server. ?

Did you keep or wrote down the address of that C&C server ?

hyp3ri0n - October 10, 2014, 7:30 pm

(Oct 10, 2014 05:52 PM)Aur? Wrote: [\[CITE\]](#) Did you keep or wrote down the address of that C&C server ?

Yes, I have it documented in the incident response report I wrote up. I will post the address for the C&C it was communicating with on Monday so I can get the report from work.

Aura - October 11, 2014, 7:03 am

(Oct 10, 2014 07:30 PM)hyp3ri0n Wrote: [\[CITE\]](#) Yes, I have it documented in the incident response report I wrote up. I will post the address for the C&C it was communicating with on Monday so I can get the report from work.

Are you going to try to take it down or it's just because you have to report it ?