

Forum:[Hack Forums](#)

Thread: [\[TUT\] Drive-By Exploits](#)

freepizza - January 1, 2016, 2:02 am

Hello again HF!!

Before i begin:

While surfing on the net, i started reading about a relatively new malware type Called a Drive-By exploit, i did a research on it - watching LinkCabins videos, reading some webpages and viewing some White hat blogs and forums, and i was scared and surprised at the same time that we are ALL unprotected - i went up to Malware domain list and blade, viewing the websites that redicts you to a website which launches the exploit itself and downloads an unwanted program on the computer, scanning the program in virus total and the website itself showed me that the ratio detection was REALLY low, meaning that some websites were not detected by "Award winning Anti Viruses" and even more threatening that some of the malware wasn't detected.

What is a drive-by download?

Well basically a Drive-By download is a download that occurs when a malicious website code exploits a vulnerability in various famous plug-ins such as: Java Script, Adobe Reader, Adobe Flash Player and uses it to download an unwanted program on your computer without your permission or of you being aware of it, most Anti-Viruses wont warn you about the download.

It would be important to mention that hackers hack legitimate websites and inject a code into them without the websites owner permission, the code should redict you to the website containing the Drive-By download.

<http://www.youtube.com/watch?v=kMGNuw9c0Ss>

Typical Black Hole Exploit kit behavior.

<http://www.youtube.com/watch?v=YAesD1TEfk0>

In this case, the user had a special program to stop the exploit, as you can see his firewall didn't start up detecting the download, this happens because the Black Hole Exploit kid code is obfuscated and polymorphic which mutates the code, generating new variants each time which makes it undetectable.

It would be important to mention that not all downloads will download the program that this guy downloaded, i have no idea why the name was given to it but its not because of this program, i saw other videos where the exploit downloaded other malware into the computer.

Exploit kit types and their behavior:

Well firstly, to build an exploit kit you have to be one rich motherfucker or either be really REALLY skilled, most hackers dont have time to look for them so they just buy them from other hackers, for example here is an advertising from the website DarCode.com(currently dead), a website which contains many famous hackers(Paunch, bx1, carberp, alexudagov), in order to get invited to website you need to apply and show your "skills" and how you could contribute the forums so its not really easy but anyway - :

[img]<http://#.com/wp-content/uploads/2013/12/JPM450K.png>[/img]

Black hole exploit kit

The exploit itself was released in 2012, in various Russian forums.

Black Hole Advertising(translated from a russian forum) -

The exploit was rather advanced, and worked like a botnet - by that i mean it would send the C&C server the details of the infected computer, and with what it was infected -

As you can see, this persons website was really wide spread, check out the hits he got. The black hole is really dangours for its polymorphic code it generates new variants the mutates the code each time and the Anti-Viruses fail to detect it.

<http://www.youtube.com/watch?v=D3NY5IBjMyM>

As you can see, that was a legit website, that was hacked.LinkCabin made a really nice presentation about the kit i would recommend watching it.

<http://www.youtube.com/watch?v=EQ4AseeBVqM>

So how to stay safe against the black hole exploit kit?

Well its pretty easy, while entering emails that you are not sure if they are so legit, put your mouse on the link and look at the website it redicts too, if the website doesn't seem legit dont enter it - most Black hole and other

Find a good host-based intrusion prevention system or HIPS but the safest thing you could do is removing the various plug ins like Java Script, Flash player and so on.

exploits websites would end int /index.html or /name.js or /name.pdf - from my research in malwaredomainslist.com.

- i know it leads to the Zeus Trojan download, but i was attempting to find various redict options.

Probably some exploit that tricks skids to think its some place where you can get various account passwords.

The Phoenix exploit that i would cover in a second.

Phoenix Exploit Kit

Introduced by the famous hacker alexudakov that was arrested and then released (Imao he got arrested because of the kit and then came back to distributing it)

Andrey Anatolevich Alexandrov didnt really bother covering his tracks, maybe because he did not gave a shit, although he was married with a wife and a child.. but well you know if your a black hat you should learn form Andrey and while making epic exploits and malware you should cover your tracks.

Unlike the Black Hole Exploit the Phoenix Exploit targets mostly outdated plug ins, while the black hole almost each time updates to the new versions to remain undetected, the kit was selling for 2200 dollars a pop.. not really cheap.

-

Phoenix Kit Advertising in exploits.

if you want to read about Andrey, there is some interesting information about him over here - <http://#.com/2013/04/phoenix-exploit-kit-author-arrested-in-russia/>

Well back to the exploit kit:

<http://www.youtube.com/watch?v=KLUI0sUWUjo>

The best video i could find, showing the Drive-By in action, as you can see it acts like the Black Hole, but what i found scary about the kit from looking at malwaredomainslist.com that MOST websites that redict to a Drive-By download are infected with the Phoenix Exploit kit.

-Statistics, there is a picture that shows the country statistics but i think the thread has enough pictures.

How to stay safe against he Phoenix Exploit Kit:

Well i was searching through out the web and found a program that could deal with some Drive-By Downloads, i didn't test it out my self but be my guest its called ExploitShield.

<http://www.youtube.com/watch?v=cN2CErkoiks>

But it looks like the java.exe still downloaded itself into the computer so i don't really know if this is effective, but since the Phoenix Exploit Kit targets ONLY outdated versions of Flash player, java, and reader you should just update them and your safe.

Exploits in General and Summary

There are WAAAAAY more exploit kits than you think, i was looking through blade statistics page to only find out there are shit ton of free exploit kits that were used:

While the detection ratio was the following:

This picture shows that there is a chance of more than 50% than your AV wont detect the exploit kit.

Well thank you for your time, now you are safer on the internet, brian krebs is a great information ressource and his blog helped me gather those amazing information about the Black Exploit kit and The Phoenix Exploit kit,

And remember be safe, dont be stupid its always better to be safe than sorry...please don't forget to rate the thread and post your comments and feedbacks here :)

Regards.
freepizza

Neptuna - January 1, 2016, 6:24 am

Thank you for your post.

Very interesting!

rapidfire08 - January 1, 2016, 6:28 am

Great article. Puts things in perspective for learners.

freepizza - January 1, 2016, 7:01 am

Thank you guys ,glad you like it ,
A little thanks really make me happy and keep me going.

Armada - January 1, 2016, 9:20 am

Why Have you not cited any sources for this?

- I know for a fact I have read majority of this in another article, nearly IDENTICAL.

Plagiarism is not allowed here.

cyberb0b - January 1, 2016, 2:40 pm

Thanks.....!!!!!!!!!!!!!!!!!!!!!!

freepizza - January 2, 2016, 3:10 am

(Jan 1, 2016 10:20 AM)Armada Wrote: [\[CITE\]](#) Why Have you not cited any sources for this?

- I know for a fact I have read majority of this in another article, nearly IDENTICAL.

Plagiarism is not allowed here.

If you pay attention you will see my source...btw a little thanks won't hurt !

(Jan 1, 2016 03:40 PM)cyberb0b Wrote: [\[CITE\]](#) Thanks.....!!!!!!!!!!!!!!!!!!!!!!

Thanks glad u like it!!!!!!

ov3rf10w. - January 26, 2016, 3:59 am

This is Nice HQ shit... GJ! ^^

Un0hex - January 26, 2016, 5:18 am

great article, interesting to read

kmz22222 - January 26, 2016, 9:41 am

GOTCHA BITCH,The tutorial is copy pasted <3

<https://evilzone.org/tutorials/%28tut%29-what-are-drive-by-exploits/?wap> :)

Edit: I reported the thread to the staff,he is going to deal with it.

Next time don't steal someone's effort and add some images and call it your tutorial.

I who make my tutorials and threads and i got negative rep

You copy paste threads and you get positive rep

HACK FORUMS LOGIC.