

Forum:[Hack Forums](#)

Thread: [How does a exploit-kit works?](#)

Theodore Evelyn Mosby - January 11, 2014, 8:55 am

Hi,
i heard about exploit-kit to spread botnets,
but i didn't understand properly how it works, i mean one time i hear that it spread with a website or something like that but im not sure that it's correct because it will be something like JDB.

PLEASE I NEED DETAILED NOOB FRIENDLY EXPLAINTION :D

BlackCodez - January 11, 2014, 8:58 am

(Jan 11, 2014 09:55 AM)??BST??C=T Wrote: [\[CITE\]](#) Hi,
i heard about exploit-kit to spread botnets,
but i didn't understand properly how it works, i mean one time i hear that it spread with a website or something like that but im not sure that it's correct because it will be something like JDB.

PLEASE I NEED DETAILED NOOB FRIENDLY EXPLAINTION :D

Well, when you visit a website with a exploit-kit iframed or installed directly on the website.
The exploit-kit will launch multiple exploits against your computer and try to send a PAYLOAD which is the "virus". If it's successful, congratulations then you recieve a bot or a slave or a zombie or whatever. If you wan't to know more just PM me. And depending on the quality of the exploits on the exploit-kit the higher success rate of infecting peoples you'll have.
Let's say that you have this super duper awesome java silent 0-day exploit that works on every version on the exploit kit that infects everyone that have java, you will get rich as fuck.
And then you have an adobe exploit that also works on every version then you'll have a success rate of 90% at least.
So let's say that you send 1 million people to the hacked website with an iframe (a little frame with a website in it on a website) on you'll have 900 infected machines.
But this is a scenario that most likeley will never happen :)

Kim Jong-Illest - January 11, 2014, 8:59 am

Like the user said above, essentially the exploit kit will attempt to use a variety of exploits on the targeted computer until one works. Generally the best way to safeguard from exploit kits is to update/update/update.

Vincenzo? - January 11, 2014, 9:08 am

Exploit kits are filled with private/public exploits to ensure maximum execution rate, you can also buy human traffic to make the process easier and faster.

Private666 - January 11, 2014, 9:49 am

With exploit packs the bots are fresh and not over used unlike most bot sellers here on HF.

Theodore Evelyn Mosby - January 11, 2014, 12:47 pm

(Jan 11, 2014 09:58 AM)BlackCodez Wrote: [\[CITE\]](#) Well, when you visit a website with a exploit-kit iframed or installed directly on the website.

The exploit-kit will launch multiple exploits against your computer and try to send a PAYLOAD which is the "virus". If it's successful, congratulations then you recieve a bot or a slave or a zombie or whatever. If you wan't to know more just PM me. And depending on the quality of the exploits on

the exploit-kit the higher success rate of infecting peoples you'll have.

Let's say that you have this super duper awesome java silent 0-day exploit that works on every version on the exploit kit that infects everyone that have java, you will get rich as fuck.

And then you have an adobe exploit that also works on every version then you'll have a success rate of 90% at least.

So let's say that you send 1 million people to the hacked website with an iframe (a little frame with a website in it on a website) on you'll have 900 infected machines.

But this is a scenario that most likeley will never happen :)So the exploit kit's are a JDB variant with more success rate?

(Jan 11, 2014 09:59 AM)Kim Jong-Illest Wrote: [\[CITE\]](#) Like the user said above, essentially the exploit kit will attempt to use a variety of exploits on the targeted computer until one works. Generally the best way to safeguard from exploit kits is to update/update/update.What you mean with "update/update/update" ?

(Jan 11, 2014 10:08 AM)CodeEcho Wrote: [\[CITE\]](#) Exploit kits are filled with private/public exploits to ensure maximum execution rate, you can also buy human traffic to make the process easier and faster.That's one of the best spread method.But how's the cost of a good exploit-kit?

(Jan 11, 2014 10:49 AM)Syncing Wrote: [\[CITE\]](#) With exploit packs the bots are fresh and not over used unlike most bot sellers here on HF.But seems, a quite famous method because it's very efficent, so which bot in commerce(obviously private botnet's are best in botkilling)has the best botkiller?

xyfir - January 11, 2014, 2:26 pm

An exploit-kit will try to infect systems through vulnerabilities in the browser or things like Flash or Java. The user above was saying the best way to avoid being infected by one is to keep everything on your system up to date so you're at least protected against known exploits.

Theodore Evelyn Mosby - January 11, 2014, 2:30 pm

(Jan 11, 2014 03:26 PM)xshadow Wrote: [\[CITE\]](#) An exploit-kit will try to infect systems through vulnerabilities in the browser or things like Flash or Java. The user above was saying the best way to avoid being infected by one is to keep everything on your system up to date so you're at least protected against known exploits.

Thank you very much ?

But aren't out there many private exploit-kits?Is the O.S. a significative object for this malware?I mean if i have mac os x i will have less possibilities to be infected against the windows systems for example?

SIM-1230922 - January 11, 2014, 2:32 pm

I don't really exactly know what they do.

I think they use exploits to infect you. These exploits can be through various of "programs" like flash and java.

I also know that they're really, really really expensive!

xyfir - January 11, 2014, 2:48 pm

(Jan 11, 2014 03:30 PM)??BST??C=T Wrote: [\[CITE\]](#) Thank you very much ?

But aren't out there many private exploit-kits?Is the O.S. a significative object for this malware?I mean if i have mac os x i will have less possibilities to be infected against the windows systems for example? Depends on what the kit is targeting. So if they're targeting a Windows system (like pretty much all of them do) the payload is most likely going to be an .exe. So if you're on OSX it won't do

shit to you regardless of whether you're vulnerable.

And yes, there are private exploit-kits. Those will yield you the highest infection rates, especially if they contain 0day exploits.

ZEREK - January 11, 2014, 3:54 pm

(Jan 11, 2014 09:58 AM)BlackCodez Wrote: [\[CITE\]](#) Well, when you visit a website with a exploit-kit iframed or installed directly on the website.

The exploit-kit will launch multiple exploits against your computer and try to send a PAYLOAD which is the "virus". If it's successful, congratulations then you receive a bot or a slave or a zombie or whatever. If you want to know more just PM me. And depending on the quality of the exploits on the exploit-kit the higher success rate of infecting peoples you'll have.

Let's say that you have this super duper awesome java silent 0-day exploit that works on every version on the exploit kit that infects everyone that have java, you will get rich as fuck.

And then you have an adobe exploit that also works on every version then you'll have a success rate of 90% at least.

So let's say that you send 1 million people to the hacked website with an iframe (a little frame with a website in it on a website) on you'll have 900 infected machines.

But this is a scenario that most likely will never happen :)

That was a good answer i always wanted to know how they work had a basic idea but not so much information

?Ñâzg?! - January 11, 2014, 6:16 pm

(Jan 11, 2014 03:30 PM)??BST??C=T Wrote: [\[CITE\]](#) Thank you very much ?

But aren't out there many private exploit-kits?Is the O.S. a significant object for this malware?I mean if i have mac os x i will have less possibilities to be infected against the windows systems for example?

some payloads use java instead of a native windows executable

so yes your system could get infected potentially

Tiny Hippo - January 11, 2014, 6:25 pm

Pretend Exploit Kit A has 5 exploits, let's just pretend it has 3 Java exploits, one Flash exploit and a Internet Explorer 0day. And to clarify, a 0 day is an exploit that has not been patched yet and extremely dangerous, 0days are extremely rare and hard to find.

You load the contents of Exploit Kit A onto a website. When a user visits the website, it will scan the user to see if they are running a vulnerable version of Java, Flash or Internet Explorer. For example, one of the Java exploits out of the 3 is CVE-2013-0422 (

<http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Exploit%3AJava%2FCVE-2013-0422>). If you read the description of CVE-2013-0422, every Java version under 10 is vulnerable and if the user is running 10 and under, they will be infected with the payload or the virus.

You can compare this to like pressure points on your friend. For example, you go to a website to look up pressure points and you come up with 5 different pressure points on the human body. You go up to your friend and test all of them and see if they work on him. Say you poke his wrist, and that doesn't work, you move on the next "exploit" if you will. You poke his waist, that doesn't work, you move on. Then you try to poke his neck and see if that works and it does. You successfully delivered the "virus" or in this case make him feel uncomfortable.

Theodore Evelyn Mosby - January 12, 2014, 2:40 am

(Jan 11, 2014 07:25 PM)Tiny Hippo Wrote: [\[CITE\]](#) Pretend Exploit Kit A has 5 exploits, let's just

pretend it has 3 Java exploits, one Flash exploit and a Internet Explorer 0day. And to clarify, a 0 day is an exploit that has not been patched yet and extremely dangerous, 0days are extremely rare and hard to find.

You load the contents of Exploit Kit A onto a website. When a user visits the website, it will scan the user to see if they are running a vulnerable version of Java, Flash or Internet Explorer. For example, one of the Java exploits out of the 3 is CVE-2013-0422 (<http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Exploit%3AJava%2FCVE-2013-0422>). If you read the description of CVE-2013-0422, every Java version under 10 is vulnerable and if the user is running 10 and under, they will be infected with the payload or the virus.

You can compare this to like pressure points on your friend. For example, you go to a website to look up pressure points and you come up with 5 different pressure points on the human body. You go up to your friend and test all of them and see if they work on him. Say you poke his wrist, and that doesn't work, you move on the next "exploit" if you will. You poke his waist, that doesn't work, you move on. Then you try to poke his neck and see if that works and it does. You successfully delivered the "virus" or in this case make him feel uncomfortable.

(Jan 11, 2014 03:48 PM)xshadow Wrote: [\[CITE\]](#) Depends on what the kit is targeting. So if they're targeting a Windows system (like pretty much all of them do) the payload is most likely going to be an .exe. So if you're on OSX it won't do shit to you regardless of whether you're vulnerable.

And yes, there are private exploit-kits. Those will yield you the highest infection rates, especially if they contain 0day exploits.

But what is a 0 day exploit?How and when it works?Why it's diffucult to find?Why microsoft or oracle didn't patch that exploit?Why it's most dangerous?

Willy Wanka - January 12, 2014, 3:33 am

(Jan 12, 2014 03:40 AM)??BST??C=T Wrote: [\[CITE\]](#)

But what is a 0 day exploit?How and when it works?Why it's diffucult to find?Why microsoft or oracle didn't patch that exploit?Why it's most dangerous?

A zero day is like a missing brick in a wall that the builder overlooked. their hard to find because they aren't usually over-looked and when the 0day get's public they patch it quickly and only because there's a limited amount of them in each update or they take awhile to find and abuse and because I'm assuming some 0days are useless which means only certain ones may be useful for certain thing's and it's dangerous because it's unknown the developer never excepted someone to use it so they probably have no defense to stop it. (This is all guess work I have a basic idea how this stuff work's considering I've never seen one or been explained them)

eddy22 - January 12, 2014, 5:01 am

If i can get good exploit kit like doc, pdf FUD i will go purchasebut i dont know how much it cost

BlackCodez - January 12, 2014, 5:05 am

(Jan 12, 2014 03:40 AM)??BST??C=T Wrote: [\[CITE\]](#)

But what is a 0 day exploit?How and when it works?Why it's diffucult to find?Why microsoft or oracle didn't patch that exploit?Why it's most dangerous?

A 0-day exploit is like all of the others exploits except one thing, the developers don't know about it yet or haven't made a patch for it yet. And the reason why it's so hard to find is because let's say you find a 0-day exploit on skype which would let you earn a shit ton of cash, would you go here on HF and say YOOO! I got a skype 0-day let's me infect anyone, even Bill Gates.

1. The developers would probably patch it in a matter of hours.
2. Obviously you wouldn't earn any money on it.

You can buy them though, mostly on "underground" forum or at least a forum that isn't as large as

HF.

They're also available sometimes on exploit-db for sale, but if you really want a quality 0-day you should look more into system penetration and how to find vulnerabilities and how to code exploits to them yourself.

I'm also going to learn that. I got the book and everything, already know pretty much but going to advance, so if you need a learning buddy just hmu bro.

Theodore Evelyn Mosby - January 12, 2014, 7:06 am

(Jan 12, 2014 06:05 AM)BlackCodez Wrote: [\[CITE\]](#) A 0-day exploit is like all of the others exploits except one thing, the developers don't know about it yet or haven't made a patch for it yet. And the reason why it's so hard to find is because let's say you find a 0-day exploit on skype which would let you earn a shit ton of cash, would you go here on HF and say YOOO! I got a skype 0-day let's me infect anyone, even Bill Gates.

1. The developers would probably patch it in a matter of hours.

2. Obviously you wouldn't earn any money on it.

You can buy them though, mostly on "underground" forum or at least a forum that isn't as large as HF.

They're also available sometimes on exploit-db for sale, but if you really want a quality 0-day you should look more into system penetration and how to find vulnerabilities and how to code exploits to them yourself.

I'm also going to learn that. I got the book and everything, already know pretty much but going to advance, so if you need a learning buddy just hmu bro.LOL, simply the best, thanks a lot man now i understand it completely, but what means "hmu"?

Can you pm me the path of studies to go in advance in this kind of things?

Thanks a lot to everyone :D

Tiny Hippo - January 12, 2014, 10:21 am

HMU means hit me up. Exploit.in is a more exclusive forum than HF, not as public and you have to be accepted but it is not as hard to be accepted into it as other super underground forums. Exploit.in holds a good majority of the bots and exploit kits, true underground forums like LCP are extremely hard to get into and you need vouches from other members to get in and have simply stunning bots and EK's.

0 day are dangerous because they exploit a piece of software and the developer of the software is not aware of it yet, which makes it extremely dangerous. If anyone finds a 0 day will probably keep it private as if you go on a public forum and talk about it, it'll be patched really quickly. 0 day's can sell on underground forums for tens of thousands even hundreds of thousands. Exploit kit owners will be the ones that will buy these and therefore can raise the price of their exploit kits and make profit. Paunch, the owner of the Blackhole (arrested now) spent hundreds of thousands buying exploits and 0 day's and put them on his own EK and sell them.

Theodore Evelyn Mosby - January 12, 2014, 11:22 am

(Jan 12, 2014 11:21 AM)Tiny Hippo Wrote: [\[CITE\]](#) HMU means hit me up. Exploit.in is a more exclusive forum than HF, not as public and you have to be accepted but it is not as hard to be accepted into it as other super underground forums. Exploit.in holds a good majority of the bots and exploit kits, true underground forums like LCP are extremely hard to get into and you need vouches from other members to get in and have simply stunning bots and EK's.

0 day are dangerous because they exploit a piece of software and the developer of the software is not aware of it yet, which makes it extremely dangerous. If anyone finds a 0 day will probably keep it private as if you go on a public forum and talk about it, it'll be patched really quickly. 0 day's can sell on underground forums for tens of thousands even hundreds of thousands. Exploit kit owners will be

the ones that will buy these and therefore can raise the price of their exploit kits and make profit. Paunch, the owner of the Blackhole (arrested now) spent hundreds of thousands buying exploits and 0 day's and put them on his own EK and sell them.LOL, reading you're post i understand that i know about botnet like a monkey know about wikipedia.

Hmmm, is there any way to start for serious botting for me?

And i heard that now exploit[.]im don't accept more new members, is it true?

Tiny Hippo - January 12, 2014, 2:28 pm

(Jan 12, 2014 12:22 PM)??BST??C=T Wrote: [\[CITE\]](#) LOL, reading you're post i understand that i know about botnet like a monkey know about wikipedia.

Hmmm, is there any way to start for serious botting for me?

And i heard that now exploit[.]im don't accept more new members, is it true?

They closed free instant registrations, but you have to apply in a sense to get in, but it's still easy to get in.

Theodore Evelyn Mosby - January 13, 2014, 4:43 am

Ok, but what's LCP?

And to learn more about exploit which basic thing i have to know?(example:html language... and other things)

Tiny Hippo - January 13, 2014, 3:31 pm

(Jan 13, 2014 05:43 AM)??BST??C=T Wrote: [\[CITE\]](#) Ok, but what's LCP?

And to learn more about exploit which basic thing i have to know?(example:html language... and other things)

LCP is an underground hacking forum. You'll need the direct URL, you won't find it on Google.

pillion - January 14, 2014, 1:37 am

BlackCodez..please Pm me your skype id...want to get information from u..and do u sell exploit kits also

Theodore Evelyn Mosby - January 14, 2014, 5:18 am

(Jan 13, 2014 04:31 PM)Tiny Hippo Wrote: [\[CITE\]](#) LCP is an underground hacking forum. You'll need the direct URL, you won't find it on Google.Ok, it's underground, but how the hell it can't be found by the BigG?I mean there must be a ranking,even if the admin didn't wan, right?

Tiny Hippo - January 14, 2014, 11:52 am

(Jan 14, 2014 06:18 AM)??BST??C=T Wrote: [\[CITE\]](#) Ok, it's underground, but how the hell it can't be found by the BigG?I mean there must be a ranking,even if the admin didn't wan, right?

The first precaution they would take is making a robots.txt so that it blocks every bot and spider. Another step it takes is verifying if you're a bot or something, it won't let you even see the site.