

Forum:[Hack Forums](#)

Thread: [What are the most used spreading techniques for Linux malware?](#)

legouser02303035 - October 17, 2024, 10:51 am

The title says it all, I want to know the most common spreading techniques for malware on Linux.

Bastille - October 17, 2024, 11:00 am

I guess Github and fake tutorials on YT, like "hacking" videos with "cracked" software to "become a h4ck3r"

legouser02303035 - October 17, 2024, 11:06 am

(Oct 17, 2024 11:00 AM)Bastille Wrote: [\[CITE\]](#) I guess Github and fake tutorials on YT, like "hacking" videos with "cracked" software to "become a h4ck3r"

Thanks, but that was not my question tho I mean like literally what protocols are used like SSH network scanning or Telnet maybe

Bastille - October 17, 2024, 11:13 am

(Oct 17, 2024 11:06 AM)legouser02303035 Wrote: [\[CITE\]](#) Thanks, but that was not my question tho I mean like literally what protocols are used like SSH network scanning or Telnet maybe

You asked for the most common spreading method, that's a spreading method. Like, people do this to spread their malware on the web ...

I don't understand the second question, tools such as nmap (which is a network scanner) don't spread malware, it helps conducting penetration/hacking on networks/targets.

Protocols such as SSH or Telnet allow to send or get data / remote access to connected devices, such as firewalls, computers, servers, and so on. There are many applications of these protocols (you can remotely access a victim's computer, you can make your loader download a payload through SSH, even if this protocol is not often enabled by default).

Could you develop a little bit please ? More context would be helpful I think

legouser02303035 - October 17, 2024, 11:27 am

(Oct 17, 2024 11:13 AM)Bastille Wrote: [\[CITE\]](#) You asked for the most common spreading method, that's a spreading method. Like, people do this to spread their malware on the web ...

I don't understand the second question, tools such as nmap (which is a network scanner) don't spread malware, it helps conducting penetration/hacking on networks/targets.

Protocols such as SSH or Telnet allow to send or get data / remote access to connected devices, such as firewalls, computers, servers, and so on. There are many applications of these protocols (you can remotely access a victim's computer, you can make your loader download a payload through SSH, even if this protocol is not often enabled by default).

Could you develop a little bit please ? More context would be helpful I think

Oh okay I am sorry I didn't understand your answer. To explain a little bit more I want to target Linux IoT devices, like the mirai botnet. I know I need to build a loader that will be send to a unsafe devices that was bruteforced via telnet, atleast that is how mirai does it. I was just wondering if that technique of network scanning and using telnet is outdated, and if there are new better techniques

to spread it. I hope I made it more clear.

Bastille - October 17, 2024, 11:55 am

(Oct 17, 2024 11:27 AM)legouser02303035 Wrote: [\[CITE\]](#) Oh okay I am sorry I didn't understand your answer. To explain a little bit more I want to target Linux IoT devices, like the mirai botnet. I know I need to build a loader that will be send to a unsafe devices that was bruteforced via telnet, atleast that is how mirai does it. I was just wondering if that technique of network scanning and using telnet is outdated, and if there are new better techniques to spread it. I hope I made it more clear.

Network scanning and exploiting open ports of outdated / vulnerable services is still used. Mirai was effective because IoT was quite new and not well secured back in the days, by default many devices were exposed on the WAN with default or weak passwords.

Mirai exploited these weakneeses mainly on Telnet, but also on Alternative Telenet (2323), HTTP and HTTPS. It seems that the hacker didn't use nmap, but instead a custom tool, however it could work with nmap to find open and vulnerable ports.

If you don't use nmap it the good way your IP could be flagged as malicious and blacklisted tho.

What the Mirai hacker did was to include in the malware a code so the infected devices also ran scan with the custom tool. Doing this, he didn't conduct the attack / scan from a single or a couple of IPs but from plenty.

However, regarding the impact of Mirai, nowadays IoT manufacturer had improve the security of their devices, you'll find vulnerable devices but it will not be as easy as it was with Mirai

legouser02303035 - October 17, 2024, 12:28 pm

(Oct 17, 2024 11:55 AM)Bastille Wrote: [\[CITE\]](#) Network scanning and exploiting open ports of outdated / vulnerable services is still used. Mirai was effective because IoT was quite new and not well secured back in the days, by default many devices were exposed on the WAN with default or weak passwords.

Mirai exploited these weakneeses mainly on Telnet, but also on Alternative Telenet (2323), HTTP and HTTPS. It seems that the hacker didn't use nmap, but instead a custom tool, however it could work with nmap to find open and vulnerable ports.

If you don't use nmap it the good way your IP could be flagged as malicious and blacklisted tho.

What the Mirai hacker did was to include in the malware a code so the infected devices also ran scan with the custom tool. Doing this, he didn't conduct the attack / scan from a single or a couple of IPs but from plenty.

However, regarding the impact of Mirai, nowadays IoT manufacturer had improve the security of their devices, you'll find vulnerable devices but it will not be as easy as it was with Mirai

What would be good alternative ways to get loaders onto linux systems. I know you said github and youtube tutorials, I think however that that would work more for windows users and not so much for linux iot devices and linux servers.

Bastille - October 17, 2024, 12:34 pm

(Oct 17, 2024 12:28 PM)legouser02303035 Wrote: [\[CITE\]](#) What would be good alternative ways to get loaders onto linux systems. I know you said github and youtube tutorials, I think however that that would work more for windows users and not so much for linux iot devices and linux servers. Github / YT tutorial was a good way for Linux users especially beginners as you said "Linux" in your

first post, but for IoT and servers it's different.

Can't help more tho

evilginx - *October 26, 2024, 2:42 am*

make youtube video where you use wget on your file :D

Infinity. - *October 31, 2024, 10:20 am*

(Oct 17, 2024 11:00 AM) Bastille Wrote: [\[CITE\]](#) I guess Github and fake tutorials on YT, like "hacking" videos with "cracked" software to "become a h4ck3r"

I doubt this works for most linux users.

777extremegamer - *December 12, 2024, 6:03 pm*

This is awesome wow ?