Home (https://www.bleepingcomputer.com/) > News (https://www.bleepingcomputer.com/news/)

> Security (https://www.bleepingcomputer.com/news/security/)

> New XLoader botnet uses probability theory to hide its servers

New XLoader botnet uses probability theory to hide its servers

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

May 31, 2022 11:45 AM **0**

Threat analysts have spotted a new version of the XLoader botnet malware that uses probability theory to hide its command and control servers, making it difficult to disrupt the malware's operation.

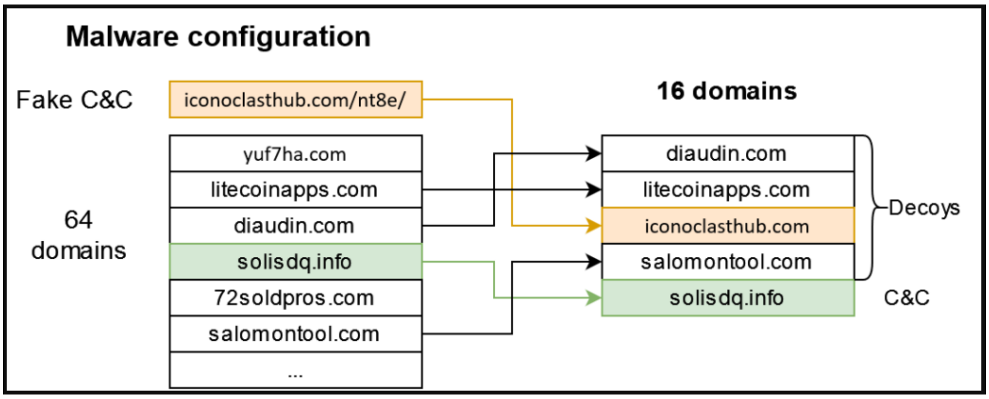
This helps the malware operators continue using the same infrastructure without the risk of losing nodes due to blocks on identified IP addresses while also reducing the chances of being tracked and identified.

XLoader is an information-stealer (https://www.bleepingcomputer.com/news/security/xloader-malware-steals-logins-from-macos-and-windows-systems/) that was originally based on Formbook, targeting Windows and macOS operating systems. It first entered widespread deployment in January 2021.

Researchers at Check Point, who have been following the evolution of the malware, have sampled and analyzed the more recent XLoader versions 2.5 and 2.6 and spotted some critical differences compared to previous versions.

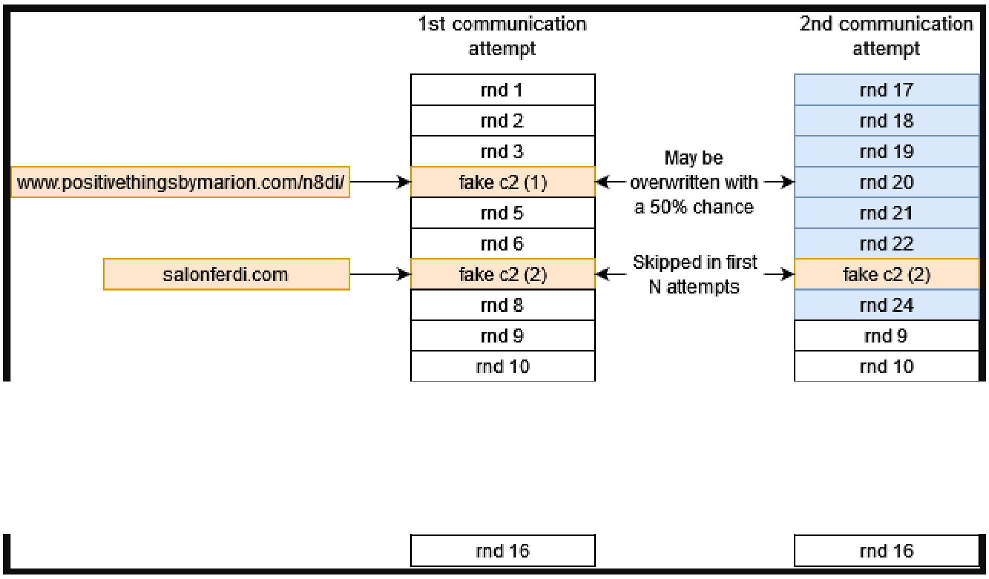
Law of large numbers

XLoader already camouflaged its actual command and control (C2) servers in version 2.3 by hiding the real domain name in a configuration that includes 63 decoys.



Hiding the actual domain among 63 decoys *(CheckPoint)*

In the most recent versions, though, Check Point's analysts noticed that the malware overwrites 8 out of a list of randomly chosen domains from the 64 in its configuration list with new values in every communication attempt.



Overwriting random domains in the list *(CheckPoint)*

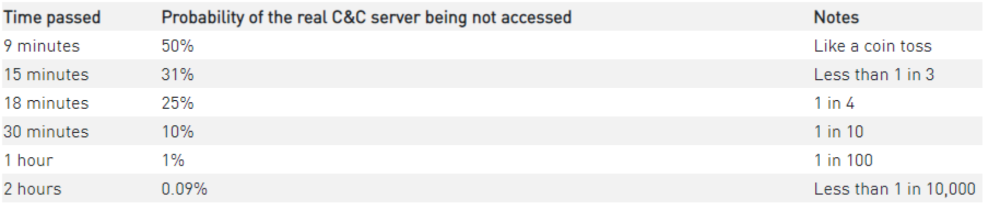
"If the real C&C domain appears in the second part of the list, it is accessed in every cycle once in approximately every 80-90 seconds. If it appears in the first part of the list, it will be overwritten by another random domain name," explains CheckPoint (https://research.checkpoint.com/2022/xloader-botnet-find-me-if-you-can/).

"The eight domains that overwrite the first part of the list are chosen randomly, and the real C&C domain might be one of them. In this case, the probability that a real C&C server will be accessed in the next cycle is 7/64 or 1/8 depending on the position of the "fake c2 (2)" domain."

This helps in disguising the real C2 servers from security analysts while keeping the impact on the malware's operations at a minimum.

Successful C2 access results from the law of large numbers (https://en.wikipedia.org/wiki/Law_of_large_numbers), which increases the probabilities of obtaining the expected outcome given enough trials.

As CheckPoint explains via the following table, threat analysts would have to perform a lengthy emulation to derive the actual C2 address, which is an atypical practice and renders all automated scripts useless.



Time passed	Probability of the real C&C server being not accessed	Notes
9 minutes	50%	Like a coin toss
15 minutes	31%	Less than 1 in 3
18 minutes	25%	1 in 4
30 minutes	10%	1 in 10
1 hour	1%	1 in 100
2 hours	0.09%	Less than 1 in 10,000

Table of probabilities *(CheckPoint)*

At the same time, for the malware operators, it would be unlikely for XLoader not to contact the genuine C2 address an hour after infection.

In version 2.6, CheckPoint noticed that XLoader removed this functionality from the 64-bit version of the payload, where the malware

new C2 obfuscation.

Related Articles:

FluBot Android malware operation shutdown by law enforcement (https://www.bleepingcomputer.com/news/security/flubot-android-malware-operation-shutdown-by-law-enforcement/)

EnemyBot malware adds exploits for critical VMware, F5 BIG-IP flaws (https://www.bleepingcomputer.com/news/security/enemybot-malware-adds-exploits-for-critical-vmware-f5-big-ip-flaws/)

Mobile trojan detections rise as malware distribution level declines (https://www.bleepingcomputer.com/news/security/mobile-trojan-detections-rise-as-malware-distribution-level-declines/)

New ChromeLoader malware surge threatens browsers worldwide (https://www.bleepingcomputer.com/news/security/new-chromeloader-malware-surge-threatens-browsers-worldwide/)

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps (https://www.bleepingcomputer.com/news/security/new-ermac-20-android-malware-steals-accounts-wallets-from-467-apps/)