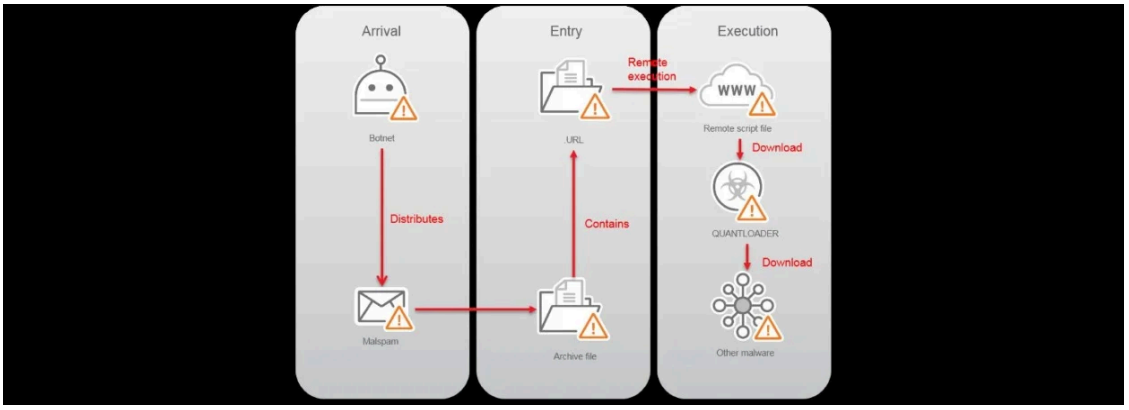
World's Largest Spam Botnet Finds a New Way to Avoid Detection... For Now

By Catalin Cimpanu

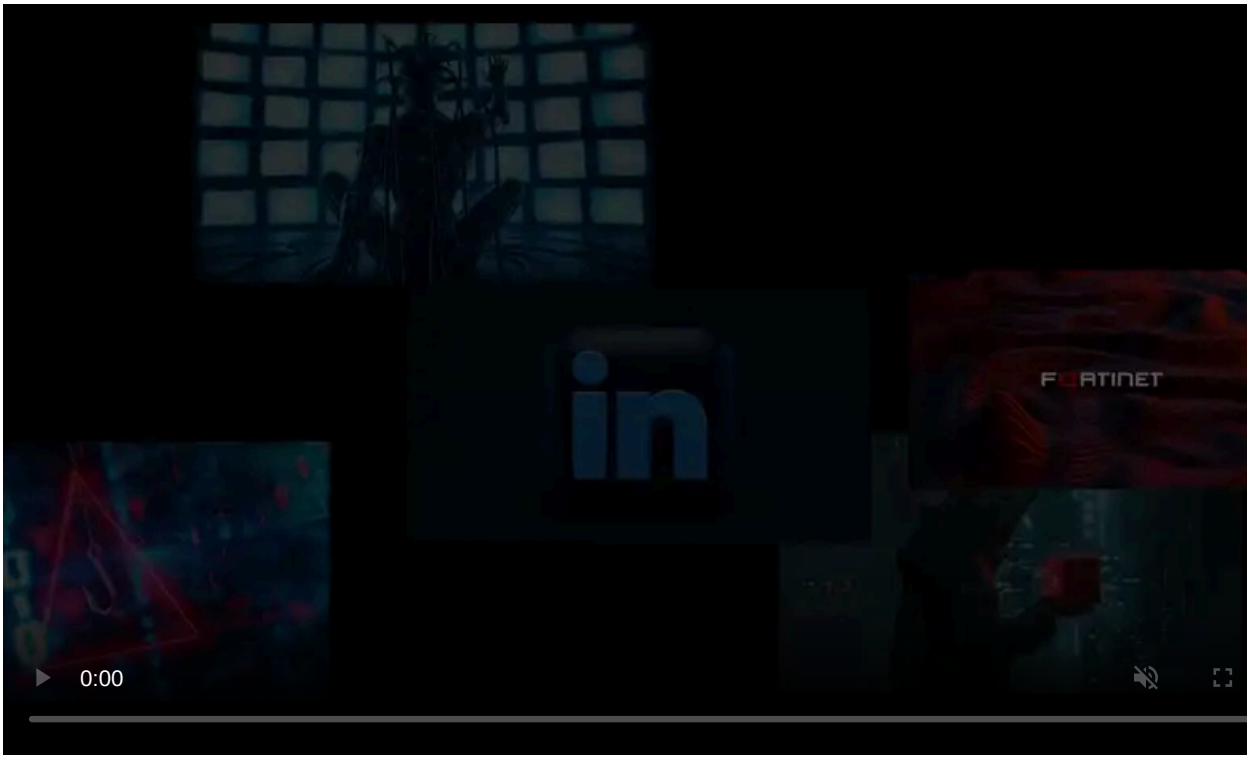
Published: 2018-04-27 · Archived: 2026-04-05 20:17:29 UTC

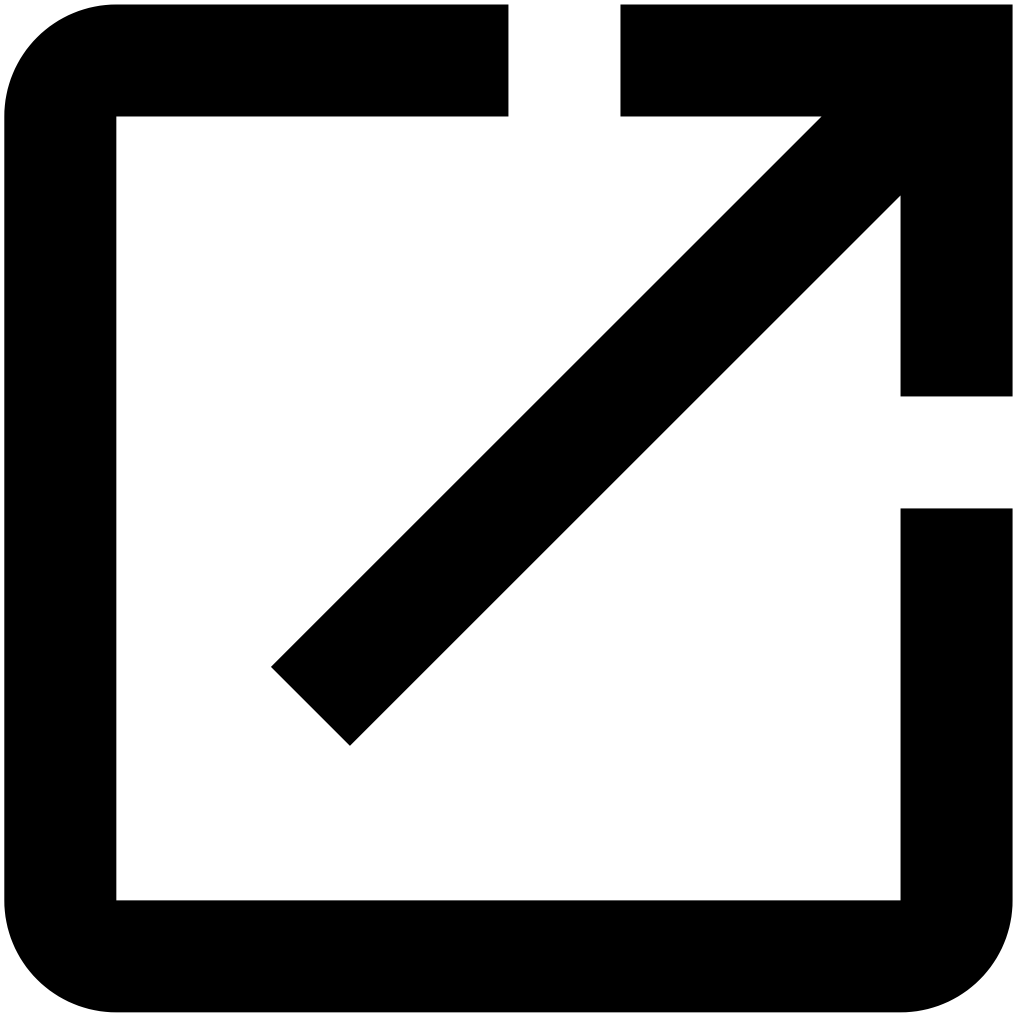


Necurs, the world's largest spam botnet, with millions of infected computers under its control, has updated its arsenal and is currently utilizing a new technique to infect victims.

This new technique consists of sending an email to a potential victim containing an archive file, which unzips to a file with the extension of .URL. This is a typical Windows shortcut file that opens a web page directly into a browser, instead of a location on disk.

The final destination of this link is a remote script file that downloads and automatically executes a final payload.


0:00



Necurs dropping Quant Loader via .URL shortcut files

For this particular spam run, Necurs had been infecting victims with Quant Loader, a run-of-the-mill and nothing-special malware family that is intended only to gain boot persistence and download another strain of more potent malware down the road.

While this technique is most likely not new entirely, as crooks have abused .URL files in the past, it is new for Necurs. What makes this technique stand out is the simplified infection chain, which now relies only on delivering a zipped .URL shortcut file.

For the past six years, since Necurs has been around, the botnet's operators have rarely used such a simple spam technique and have always relied on complicated infection chains.

We've seen stuff like one-time or double-zipped archives delivering WSF files, JS files, Visual Basic scripts, and all sorts of Office file formats, either boobytrapped with macros or leveraging exploits to infect victims.

New technique evades email malware scanners

The purpose of this much simpler routine is to avoid malware scanners that analyze emails, looking for malicious links or boobytrapped attachments. Such solutions work on preset rules, many of which have been set up by security researchers based on previously observed malicious patterns.

The deployment of a simple .URL file is not a game-breaker, as security researchers only need to update existing detection rules with a new one, but this will give the Necurs botnet time to breathe and infect victims easier in the following weeks, as email malware scanners will receive updated detection rules.

At that point, just like we've seen Necurs in the past years, botnet operators will just make a small tweak to the infection chain —like putting the .URL file inside a double-zipped file instead of a one-time zipped file— and this whole cat and mouse game will start anew.

How users can protect themselves

What users need to know —or remember, if they're old enough to have seen this trick before— is that .URL files work like typical Windows shortcut file, such as .LNK, and hence, can use custom icons.

Trend Micro, the cyber-security firm who spotted this recent Necurs .URL-based malspam campaign, warns that crooks are using the standard folder icon to hide .URL files.

This makes it somewhat easy to trick users into thinking the email file attachment they just unzipped has created a folder that they need to enter and view the actual file. Unfortunately, this is what crooks want because trying to access this faux folder will launch the infection chain.

But there is a giveaway that may protect users. Just like every other typical Windows shortcut file, .URL files also show the classic arrow icon on the bottom-left corner of the folder icon, like in the image below.

Name	Date modified	Type
2807VIFT_R	4/2/2018 6:49 PM	Internet Shortcut
3513JBKX_M	4/2/2018 6:49 PM	Internet Shortcut
6685ZFYL_R	4/2/2018 6:49 PM	Internet Shortcut
6828R8OO_B	4/2/2018 6:49 PM	Internet Shortcut
7805VXJG_A	4/2/2018 6:49 PM	Internet Shortcut
9959HYX6_X	4/2/2018 6:49 PM	Internet Shortcut
49032IRG_F	4/2/2018 6:49 PM	Internet Shortcut
IMG-20180404-9AC4DD	4/4/2018 1:02 PM	Internet Shortcut
IMG-20180404-FEFCDE	4/4/2018 1:02 PM	Internet Shortcut
JPG-20180404-36BFD9	4/4/2018 1:02 PM	Internet Shortcut
PIC-20180404-ADEEEE	4/4/2018 1:02 PM	Internet Shortcut
SCN-20180404-268CC1	4/4/2018 1:02 PM	Internet Shortcut
SCN-20180404-C6DBA9	4/4/2018 1:02 PM	Internet Shortcut
SCN-20180404-F257E5	4/4/2018 1:02 PM	Internet Shortcut
SH-20180404-38A4BB	4/4/2018 1:02 PM	Internet Shortcut
SH-20180404-B92D36	4/4/2018 1:02 PM	Internet Shortcut
SH-20180404-BBDBAA	4/4/2018 1:02 PM	Internet Shortcut
VM_03-04-2018_1017631	4/3/2018 1:16 PM	Internet Shortcut
VM_03-04-2018_2494737	4/3/2018 5:15 PM	Internet Shortcut
VM_03-04-2018_2926009	4/3/2018 1:16 PM	Internet Shortcut
VM_03-04-2018_4243941	4/3/2018 1:16 PM	Internet Shortcut
VM_03-04-2018_4430108	4/3/2018 1:16 PM	Internet Shortcut
VM_03-04-2018_5200865	4/3/2018 1:16 PM	Internet Shortcut
VM_03-04-2018_5270472	4/3/2018 1:16 PM	Internet Shortcut
VM_03-04-2018_5478686	4/3/2018 1:16 PM	Internet Shortcut
VM_03-04-2018_7795442	4/3/2018 1:16 PM	Internet Shortcut
VM_03-04-2018_8030908	4/3/2018 5:15 PM	Internet Shortcut

If you ever spot such markers on files you received via email attachments, these files are malicious 100 percent, and users should avoid opening them.

Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
