Necurs Evades Detection via Internet Shortcut File

By By: Miguel Carlo Ang Apr 26, 2018 Read time: 3 min (942 words)

Published: 2018-04-26 · Archived: 2026-04-05 13:20:11 UTC

Necurs, a botnet malware that's been around since 2012, has been improved with the hopes of better defeating cybersecurity measures — it was seen to evolve its second layer of infection using a .URL file (with remote script downloaders detected by Trend Micro as MAL_CERBER-JS03D, MAL_NEMUCOD-JS21B, VBS_SCARAB.SMJS02, and MAL_SCARAB-VBS30.

Necurs, a modular malware with variants that are capable of spam distribution, information theft, and disabling security services and elements, has been around since 2012, propagating in the wild via the Necurs botnet. In 2017, it pushed Locky — a ransomware family with one variant that was notable for being distributed via 23 million emails in just 24 hoursnews- cybercrime-and-digital-threats — via a URL-only spam email campaign. Last year, we also saw how Necurs pushed double-zipped attachments that either contained JavaScript, Visual Basic scripts, or macro files with the capability to download its final payload. In an attempt to evade spam detection through its attachments, Necurs used archives that included .ZIP files to disguise the script downloader, which was later enclosed in another .ZIP to hide itself.

The Necurs Transformation: The .URL File Layer

Necurs is indeed constantly evolving to find other effective measures of tricking victims while defeating countermeasures waged against it. And since it has a highly effective botnet component that may also be sold as a service, malicious actors will continue to find ways to circumvent detection and improve how they trick the weakest link in cybersecurity — the user. As security vendors are wise to Necurs's traditional infection chain (a script, a macro, or archives containing certain file formats), the malware has started using an internet shortcut or .URL file to bypass detection.

Figure 1. A diagram of a previous version of the Necurs malware

Figure 2. A diagram of the evolved Necurs malware

Internet shortcuts, or .URLs, take the form of clickable icons and are objects used to access internet sites or web documents faster. Internet shortcuts have contents that are in the INI file format, which allows the changing of icons. Necurs malware uses this to its advantage by changing the folder icon to trick the victim into thinking that it's a different file type, as it is less suspicious than clicking on a script. The .URL will then access the remote resource that downloads another downloader. The second downloader remotely executes the payload.

Figure 3. A .URL file disguised as a .ZIP file of a voicemail message

Notice that aside from the icons disguised as folders, the filenames were also crafted to resemble typical folder names such as IMG-20180404-9AC4DD, SCN-20180404-268CC1, and PIC-20180404-ADEEEE shown in Figure 2, to name a few.

Figure 4. A screen capture of an internet shortcut's extracted files

Furthermore, the actual attachment archive does not contain the script downloader Necurs uses to download its payload. The .URL file accesses the remote server, which then executes through the Server Message Block (SMB) protocol — a tactic that may be successful in evading certain spam filters.

Figure 5. A screen capture of a remote file being accessed through the SMB protocol

The malware doesn't stop at disguising .URL files. The latest Necurs variant no longer has the actual script downloader in its attachment. It only contains the internet shortcut to the remote site that contains the script that is then executed remotely. This means that it does not "download" the actual script on the victim's machine. This is the closest it gets to its previous malicious spam runs: Attaching a URL in the email and tricking a victim into clicking on the link to download a malicious file.

Figure 6. A look at Necurs's attachment

Interestingly, Necurs does not infect computers using Russian as a language.

Further Evolution: Using QUANTLOADER

Previously, Necurs's JavaScript downloader downloads the final payload. But in its latest iteration, the remote script downloads QUANTLOADER (detected by Trend Micro as TROJ_QUANT) – a different downloader – which then downloads the final payload. This is another layer added to Necurs's infection chain. The use of QUANTLOADER may be twofold: First, it adds another download stage before it downloads the final payload, possibly to mix things up and evade behavioral detections. Secondly, QUANTLOADER is persistent in nature — it drops a copy of itself and creates an autorun registry so that it executes at startup.

Indicators of Compromise

SHA-256s	Detection Names
03c770882e87585fea0272a8e6a7b7e37085e193475884b1316e14fb193e992d	TROJ_QUANT.K
b0c173e0fc28e0f1bc8debfe49de01f306d372a0516d88201b87e441f3de303e	TROJ_QUANT.J
b87e0dd9b0e032c6d2d5f0bf46f00243a2a866bf1d3d22f8b72737b4aa1148eb	TROJ_QUANT.L

00ca7e9e61a3ceaa4b9250866aface8af63e5ae71435d4fd6c770a8c9a167f22	TROJ_QUANT.K

Trend Micro Solutions

To protect against Necurs and other continuously evolving spammed threats, businesses can take advantage of Trend Micro™ endpoint solutions such as Trend Microproducts Smart Protection Suitesproducts and Worry-Free™ Business Security. Both solutions can protect users and businesses from threats by detecting malicious files, and spammed messages as well as blocking all related malicious URLs. Trend Micro Deep Discovery™products has an email inspection layer that can protect enterprises by detecting malicious attachment and URLs. Deep Discovery is able to detect the remote script despite it not being downloaded in the physical endpoint.

Trend Micro™ Email Securityproducts is a no-maintenance cloud solution that delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. It protects Microsoft Exchange, Microsoft Office 365products, Google Apps, and other hosted and on-premises email solutions. The spam mail used by this threat is detected on arrival by Trend Micro™ Email Reputation Services™, while our spam engine can detect Necurs's technique: an archive containing internet shortcut.

Trend Micro™ OfficeScan™ with XGen™ endpoint security infuses high-fidelity machine learning with other detection technologies and global threat intelligence for comprehensive protection against advanced malware.

A list of all the hashes (SHA-256) is in this appendix.
