Necurs Poses a New Challenge Using Internet Query File

Published: 2018-06-22 · Archived: 2026-04-05 14:28:32 UTC

Our last report on the Necurs botnet malware covered its use of an internet shortcut or .URL fileopen on a new tab to avoid detection, but its authors seem to be updating it again. Current findings prove that its developers are actively devising new means to stay ahead of the security measures meant to thwart it. This time, the new wave of spam from this botnet is using the internet query file IQY to evade detection.

Necurs has cropped up in various cyberattack reports through the years, including a 2017 incident in which it was used to distribute Lockyopen on a new tab ransomware. Its current use of the IQY file type as an initial infection vector makes it notable. IQY files are also text files with a specific format. Its purpose is to allow users to import data from external sources to the user's Excel spreadsheet. By default, Windows recognizes IQY files as MS Excel Web Query Files and automatically executes it in Excel.

The role of IQY files

The new wave of spam samples has IQY file attachments. The subject and attachment file contains terms that refer to sales promotions, offers, and discounts, likely to disguise it as the type of information opened in Excel.

Figure 1. Sample email that has IQY attachment

Once the user executes the IQY file it queries to the URL indicated in its code, the web query file pulls data — 2.dat in the sample — from the targeted URL into an Excel worksheet.

Figure 2. Code snippet of the sample IQY file

Closer examination of the pulled data shows that it contains a script that can abuse Excel's Dynamic Data Exchange (DDE) feature, enabling it to execute a command line that begins a PowerShell process. This process allows the fileless execution of the remote PowerShell script, seen as 1.dat in the sample.

Figure 3. Code snippet of the pulled data

Figure 4. Code snippet of the PowerShell script

The PowerShell script enables the download of an executable file, a trojanized remote access application, and its final payload: the backdoor FlawedAMMYY (detected as BKDR_FlawedAMMYY.A). This backdoor appears to have been developed from the leaked source code of the remote administration software called Ammyy Admin.

In a more recent spam wave, the script downloads an image file before the final payload. The downloaded image is a disguised downloader malware (detected as BKDR_FlawedAMMYY.DLOADRopen on a new tab) that downloads an encrypted component file (detected as BKDR_FlawedAMMYY.B) containing the same main backdoor routines.

Figure 5. Infection chain starting with the attached IQY file

The backdoor FlawedAMMYY executes the following commands from a remote malicious server.

- File Manager
- View Screen
- Remote Control
- Audio Chat
- RDP SessionsService - Install/Start/Stop/RemoveDisable desktop background
- Disable desktop composition
- Disable visual effects
- Show tooltip - mouse cursor blinking cause

Adding this new layer of evasion to Necurs poses new challenges because web queries generally come in the form of plaintext files, which makes the attached IQY file's URL the only indication of malware activity. In addition, its structure is the same as normal Web Queries. Therefore, a security solution that blocks malicious URLs could be used to defend against this threat.

Solutions and mitigation

Against Necurs and other threats delivered via spam, employing strict security protocols and best practices can still make a difference in defending against them. In this case, users should download and execute uncommon attachments with extreme caution. Microsoft is aware of the abuse in DDE that this infection vector uses. This is why it issues two explicit pop-up warnings upon execution of the IQY file attachment, giving users a chance to reconsider opening the file.

Figure 6. First pop-up warning

Figure 7. Second pop-up warning

Necurs' activities show that this botnet has all the signs of developing evasion techniques that might overtake an unpatched or outdated security solution. To protect against evolving spammed threats like Necurs, enterprises can use Trend Micro™ endpoint solutions such as Trend Microproducts Smart Protection Suitesopen on a new tab and Worry-Freeopen on a new tab™ Business Securityopen on a new tab. Both solutions protect users and businesses from threats by detecting malicious files and spammed messages, and blocks all related malicious URLs. Trend Microopen on a new tab Deep Discoveryopen on a new tab™ has a layer for email inspection that can protect enterprises because it detects malicious attachment and URLs. Deep Discovery can detect the remote script even if it is not being downloaded in the physical endpoint.

Trend Microopen on a new tab™ Hosted Email Securityopen on a new tab 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 365open on a new tab, Google Apps, and other hosted and on-premises email solutions. Trend Micro™ Email Reputation Services™ detects the spam mail used by this threat upon arrival.

Trend Microopen on a new tab™ OfficeScanopen on a new tab™ with XGenopen on a new tab™ endpoint security infuses high-fidelity machine learningopen on a new tab with other detection technologies and global threat intelligence for comprehensive protection against advanced malware.

Indicators of Compromise

SHA-256s	Detection Names
30e2f8e905e4596946e651627c450e3cc574fdf58ea6e41cdad1f06190a05216	TROJ_CVE20143524.A
0bd5f1573a60d55c857da78affa85f8af38d62e13e75ebdd15a402992da14b0b	TROJ_MALIQY.A
602a7a3c6a49708a336d4c9bf63c1bd3f94e885ef7784be62e866462fe36b942	TROJ_FlawedAMMYY.A
7c641ae9bfacad1e4d1d0feef3ec9e97c55c6bd66812f5d9cf2a47ba40a16dd4	TROJ_FlawedAMMYY.A
7f9cedd1b67cd61ba68d3536ee67efc1140bdf790b02da7aab4e5657bf48bb6f	BKDR_FlawedAMMYY.DLOADR
a560c53982dd7f27b2954688256734ae6ca305cc92c3d6e82ac34ee53e88e4d3	BKDR_FlawedAMMY.ENC
ba8ed406005064fdffc3e00a233ae1e1fb315ffdc70996f6f983127a7f484e99	BKDR_FlawedAMMYY.B
ca0da220f7691059b3174b2de14bd41ddb96bf3f02a2824b2b8c103215c7403c	BKDR_FlawedAMMYY.A
d9cd31184c56931ae35b26cf5fa46bf2de0bdb9f88e5e84999d2c289cbaf1507	TROJ_POWLOAD.IQY
