New Noteworthy Changes to Necurs' Behaviors

blog.trendmicro.com/trendlabs-security-intelligence/the-new-face-of-necurs-noteworthy-changes-to-necurs-behaviors

June 28, 2018

Malware

We recently discovered noteworthy changes to the way Necurs makes use of its bots, such as pushing infostealers on them and showing a special interest in bots with specific characteristics.

By: Anita Hsieh, Rubio Wu, Kawabata Kohei, Fyodor Yarochkin June 28, 2018 Read time: (words)

Assets Filter Enter path Images Select Tag(s) Publish status Loading results NEW NOTEWORTHY CHANGES TO NECURS' BEHAVIORSEditPreview Text

Six years after it was first spotted in the wild, the Necurs malware botnet is still out to prove that it's a malware chameleon. We recently discovered noteworthy changes to the way Necurs makes use of its bots, such as pushing infostealers on them and showing a special interest in bots with specific characteristics. These behavioral changes could potentially create a big impact as Necurs has been used in large-scale cybercriminal deployments in the past.

As a modularized malware, Necurs can run any module on its network of bots. In 2017, we saw Necurs pushing spamming and proxy modules onto its bots. This year, however, there's a notable decrease on Necurs' spam volume compared to its spam campaigns in the last quarter of 2017. Instead, we see Necurs pushing cryptocurrency miners and infostealers — FlawedAmmyy RAT, AZORult, and a .NET module — as modules onto its bots.

Necurs pushes XMRig to its bots to mine Monero

In March, we saw Necurs pushing a Monero Miner — XMRig — to its bots. At the time we checked it, the wallet owner was able to earn around $USD 1,200.00 in 24 hours.

Figure 1. A screen capture showing the wallet owner's earnings using the XMRig to mine Monero. The user in the configuration of this XMRig module is "47CCqA1ERkT6jUT8yhgJj7dkdHXhBw86 xiKsCdZ6auDmCC3mAQLpBxP2nhpGuHA27tToNeZM98Tz FKe6vjCajdHdCz67iRB.worker" .

In April, we observed that it pushed the remote access trojan FlawedAmmyy onto its bots. FlawedAmmyy is trojanized from a legitimate remote access tool Ammyy Admin. Like the remote desktop tool, FlawedAmmyy has the functionalities of Ammyy Admin, including remote desktop control, file system management, proxy support and audio chat capabilities. Necurs pushes different modules via C&C commands. These modules check the bots if they qualify for any of the following criteria:

1. **Bots that are with crypto wallets.**[1] The Necurs modules check if the machines have files that contain any of the following strings that exist under "%APPDATA%" such as:

- *WALLET.DAT*
- *BITCOIN-QT*
- *ELECTRUM*
- *COINBASE*
- *MULTIBITHD*
- *WALLET.AES*
- *LITECOIN*
- *MONERO*
- *BITCOINCORE*

2. **Bots that are under or able to reach bank-related domains.**[2] The modules execute commands such as "net view" and "net user" to check for the following strings:

- *BANQ*
- *BANK*
- *BANC*
- *SWIFT*

- *BITCOIN*
- *WESTERNUNION*
- *MONEYGRAM*
- *CARD*

3. **Bots that are running in a network with more than 100 employees or users.**[3] The modules execute “net user” and “net domain” to see if a machine is connected to a network with more than 100 users.

4. **Bots that run POS-related processes.**[4]

5. **Bots that are logged in using an email address on a hardcoded list.**[5] The modules, which contain some hardcoded lists, will check whether the email accounts associated with a machine is on the list. We will detail this part in the section “Necurs Pushes Modules for Email Extraction” below.

If the bots qualify based on the criteria listed above, the modules will install the FlawedAmmyy RAT onto its bots. After the session initializes, the FlawedAmmyy RAT on the infected bots steals and sends back the information, which includes:

- *id*
- *os*
- *priv (privilege)*
- *cred (DOMAIN\username)*
- *pcname (Computer name)*
- *avname (Antivirus name)*
- *build_time (Malware build time)*
- *card (whether smart-card is connected or not)*

Figure 2. The information sent back by FlawedAmmyy RAT.

Necurs pushes modules for email extraction

In late May, we saw some Necurs modules that exfiltrated email accounts and sent them to hxxp://185[.]176[.]221[.]24/l/s[.]php. If someone installs and logs in to Outlook, Outlook creates a directory “%AppData%\Roaming\Microsoft\Outlook\” wherein it will store credentials with an email string in the filename (Figure 3). The module will search for the files with email strings in the filenames and send those strings back.

Figure 3. Example: the directory storing credentials with a string in email format as part of the filename

After just a few days, we saw four new modules that also dropped FlawedAmmyy RATs but with a distinct feature — they contained hardcoded email lists inside. The four modules checked if the email addresses on the bots were in any of the lists — the same manner in which they were able to extract the email addresses that make up the lists — and if so, dropped the FlawedAmmyy RATs.

After checking the hardcoded email lists, we discovered that it's possible that the threat actors used keyword matching to pick up email addresses that interest them.

Figure 4. A list of email addresses that feature notable similarities. Aside from bank-related email addresses, some of the email addresses on the list seem to belong to government institutions.

After further analysis, we extracted the different keywords used in the email address lists. Based on the keywords, threat actors appear to show interest in governments, financial institutions, tourism and food industries, and real estate companies.

Figure 5. Keywords extracted from the email address lists in the four Necurs modules.

A possible change in spamming tactics

Another notable action of Necurs is the possible change in its spamming tactics.

On June 11, 2018, we saw Necurs push a .NET spamming module that is capable of sending emails and stealing credentials from Internet Explorer, Chrome, and Firefox. Some parts of this .NET spamming module overlap with an open-source remote access tool.

Figure 6. The Firefox StealerModule in the .NET spamming module on the left-hand side has overlaps with QuasarRAT on the right-hand side.

When Necurs drops the .NET spamming module onto its bots, it gives the arguments that the bots should execute the binary. The following is a screen capture of the command we received from Necurs' C&Cs:

Figure 7. A .NET module command screen capture.

The .NET spamming module (sha1: c25fcdf464202ef4226d085b8e495f4e5064125e) performs different actions according to the arguments given ("args" in Figure 7). The following are some arguments it accepts:

- "-sendcorp": send the emails via victims' Outlook
- "-sendprivate": send emails via victims' Gmail and Yahoo
- "-subject": the subject for the email

- “-attach”: the attachment for the email in base64 format
- “-name”: the “FROM” address for the email
- “-body”: the body for the email in base64 format
- “-demo”: send a copy to the given email address

The mail sent with the arguments in Figure 7 will be as follows:

Figure 8. The email sent by .NET spamming module with the arguments in Figure 7.

The following are some of the .NET module’s noteworthy features: it can send spam using the logged-in email accounts on a victim’s machine, and it can access a victim’s contact list stored in email clients and the email addresses with which a victim has previously corresponded. The victims will not be able to notice the spam being sent from their email addresses as the .NET module can delete the last email sent from the victim’s email account and catch all alerts.

In the past, Necurs sent spam to its victims directly via its bots, which allowed blacklisting bot IPs to block them. However, if the spam emails are sent via legitimate email clients with whitelisted IPs, the IP-blocking solution might not work properly. Moreover, those spam emails are from email accounts that the receivers already recognize. Although this technique is not new — some malware campaigns such as EMOTET and Ursnif/Dreambot have already adopted this kind of spamming technique — this is a new technique for Necurs.

With the “demo” argument set, we believe that this module is a test run for possible future campaigns and a way for the malware author to demonstrate the .NET module’s capabilities to possible customers.

Defending against Necurs malware

To defend against Necurs and other continuously evolving spammed threats, businesses can take advantage of Trend Micro™ endpoint solutions such as Trend Micro Smart Protection Suites 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™ has an email inspection layer that can protect enterprises by detecting malicious attachment and URLs. Deep Discovery can detect the remote script despite it not being downloaded in the physical endpoint.

Trend Micro™ Hosted Email Security 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 365, Google Apps, and other hosted and on-premises email solutions.

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 (SHA256) is in this list.

[1] List of strings gathered as of April 11, 2018. [2] First detected on April 11, 2018. [3] First detected on April 18, 2018. [4] First detected on April 26, 2018. [5] First detected on June 1, 2018.