November's Most Wanted Malware: Return of Necurs Botnet Brings New Ransomware Threat

By bferrite

Published: 2017-12-11 · Archived: 2026-04-05 14:04:20 UTC

During the month of November, the Necurs botnet has returned to Check Point's Global Threat Index's top ten most prevalent malware.

Check Point researchers found that hackers were using Necurs, considered to be the largest spam botnet in the world, to distribute the relatively new Scarab ransomware that was first seen in June 2017. The Necurs botnet started mass distribution of Scarab during the U.S. Thanksgiving holiday, sending over 12 million emails in a single morning. Necurs has previously been used to distribute some of the most insidious malware variants to hit business networks in the past 12 months, including the Locky and Globeimposter families.

The re-emergence of the Necurs botnet highlights how malware that may seem to be fading away, doesn't always disappear or become any less of a threat. Despite Necurs being well known to the security community, hackers are still enjoying lots of success distributing malware with this highly effective infection vehicle. This reinforces the need for advanced threat prevention technologies and a multi-layered cybersecurity strategy that protects against both previously encountered, established malware families as well as brand new, zero-day threats.

As in October, RoughTed, a large scale malvertising campaign, remained the most prevalent threat, ahead of the Rig ek exploit kit in second, and Cornficker, a worm that allows remote download of malware in third.

Top 10 'Most Wanted' Malware:

**Arrows relate to the change in rank compared to the previous month.*

1. ↔ **RoughTed** – a purveyor of ad-blocker aware malvertising responsible for a range of scams, exploits, and malware. It can be used to attack any type of platform and operating system, and utilizes ad-blocker bypassing and fingerprinting in order to make sure it delivers the most relevant attack.
2. ↑ **Rig ek** – Exploit Kit first introduced in 2014. Rig delivers Exploits for Flash, Java, Silverlight and Internet Explorer. The infection chain starts with a redirection to a landing page that contains JavaScript that checks for vulnerable plug-ins and delivers the exploit.
3. ↑ **Conficker** – Worm that allows remote operations and malware download. The infected machine is controlled by a botnet, which contacts its Command & Control server to receive instructions.
4. ↑ **Ramnit** – Banking Trojan that steals banking credentials, FTP passwords, session cookies and personal data.
5. ↑ **Fireball** – Browser-hijacker that can be turned into a full-functioning malware downloader. It is capable of executing any code on the victim machines, resulting in a wide range of actions from stealing credentials to dropping additional malware.

6. ↑ **Pushdo** – Trojan used to infect a system and then download the Cutwail spam module and can also be used to install additional third party malware.
7. ↑ **Nivdort** – Multipurpose bot, also known as Bayrob, that is used to collect passwords, modify system settings and download additional malware. It is usually spread via spam emails with the recipient address encoded in the binary, thus making each file unique.
8. ↑ **Necurs** – Botnet used to spread malware by spam emails, mainly Ransomware and Banking Trojans.
9. ↓ **Zeus** – Banking Trojan that uses man-in-the-browser keystroke logging and form grabbing in order to steal banking information.
10. ↓ **Locky** – Ransomware that started its distribution in February 2016, and spreads mainly via spam emails containing a downloader disguised as an Word or Zip attachment, which then downloads and installs the malware that encrypts the user files.

The most popular malware used to attack organizations' mobile estates remained unchanged from October, as Triada, a modular backdoor for Android, continued to increase in prevalence.

Top 3 'Most Wanted' mobile malware:

1. **Triada** – Modular Backdoor for Android that grants super-user privileges to downloaded malware and helps it to get embedded into system processes. Triada has also been seen spoofing URLs loaded in the browser.
2. **Lokibot** – Android banking Trojan and info-stealer, which can also turn into a ransomware that locks the phone in case its admin privileges are removed.
3. **LeakerLocker** – Android ransomware that reads personal user data, and then presents it to the user and threatens to leak it online if ransom payments aren't met.

Check Point's Global Threat Impact Index and its ThreatCloud Map is powered by Check Point's ThreatCloud intelligence, the largest collaborative network to fight cybercrime which delivers threat data and attack trends from a global network of threat sensors. The ThreatCloud database holds over 250 million addresses analyzed for bot discovery, more than 11 million malware signatures and over 5.5 million infected websites, and identifies millions of malware types daily.

Check Point's Threat Prevention Resources are available at:
http://www.checkpoint.com/threat-prevention-resources/index.html

BLOG FEEDBACK

Your feedback is important to us. Please tell us how we can improve on this blog.

Would you like to take the survey?

- Yes
- No
