# Necurs Malware Will Now Take a Screenshot of Your Screen, Report Runtime Errors

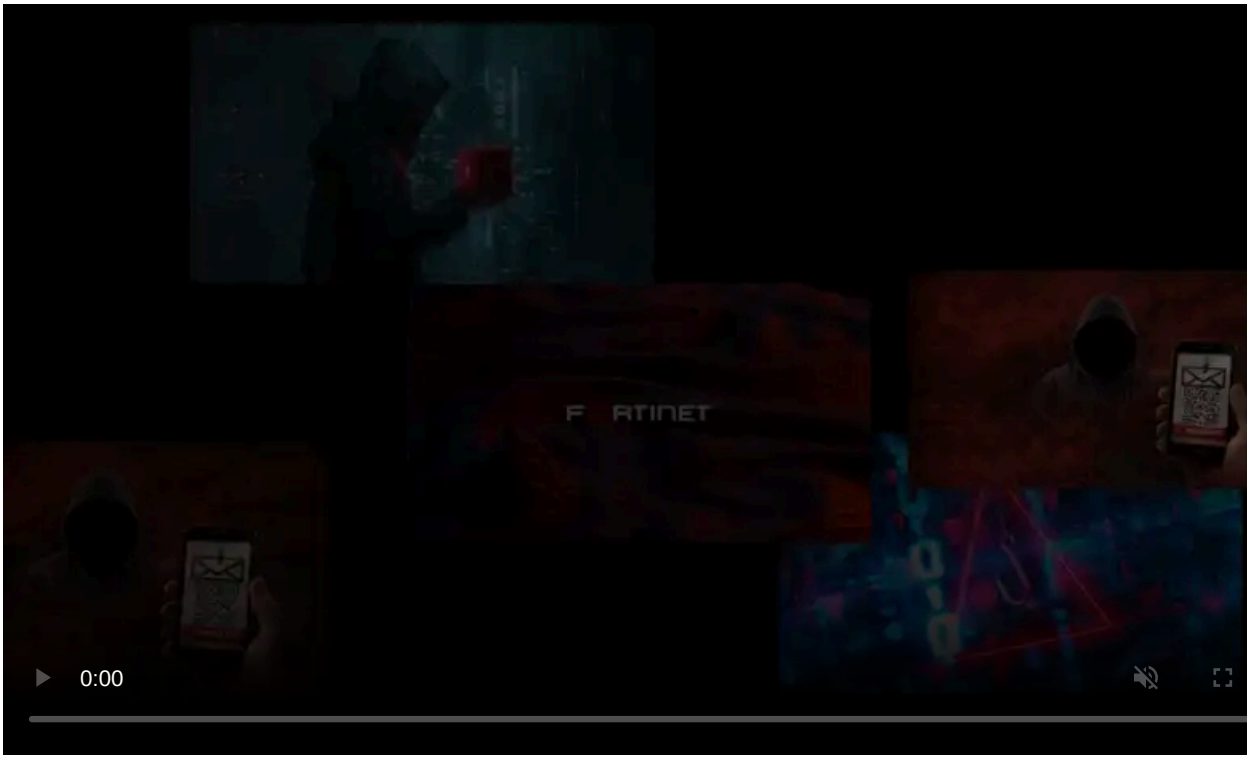
By Catalin Cimpanu

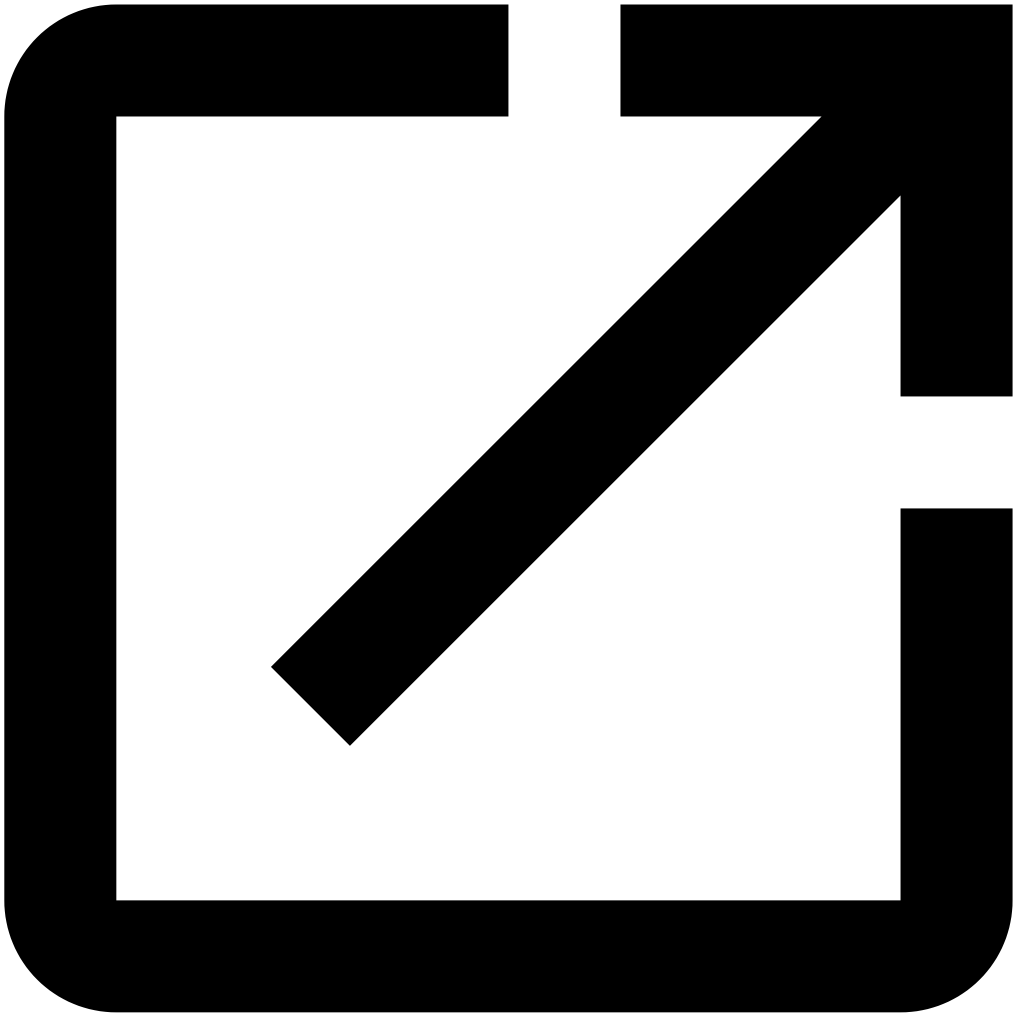
Published: 2017-10-17 · Archived: 2026-04-06 01:06:05 UTC


Malware families evolve on a daily basis, but some updates catch your eye more than others. Necurs has just gone through one of these "interesting" updates, according to US security firm Symantec.

Before we go on, we must explain that Necurs is a name given to both a malware strain and the botnet of infected computers it creates.

In the world of security research, the Necurs malware strain is a "downloader" or "loader," and just like similar downloaders, it only has three major functions: (1) gain boot persistence on an infected PC, (2) collect telemetry on infected hosts, and (3) download and install a second-stage payload.


F RTINET
0:00



The Necurs malware is distributed via spam sent by Necurs bots or hacked web servers. When you read news stories about "the Necurs botnet spreading the Locky ransomware," it's actually "the Necurs botnet spreading the Necurs downloader, which then installs the Locky ransomware."

## Necurs downloader gets two interesting new features

This Necurs downloader often gets ignored because it's usually pretty small and insignificant. Recently, researchers from Symantec observed two major additions to the Necurs downloader.

The first is the addition of a Powershell script that takes a screengrab of the infected user's screen, and after waiting a few seconds, it uploads the image to a remote server.

The second function is a built-in error reporting function that watches the Necurs downloader for errors, records problems, and sends the info back to Necurs operators.

Other malware families also come with these types of features, but they have never been seen in downloaders.

## Necurs team looking for valuable hosts

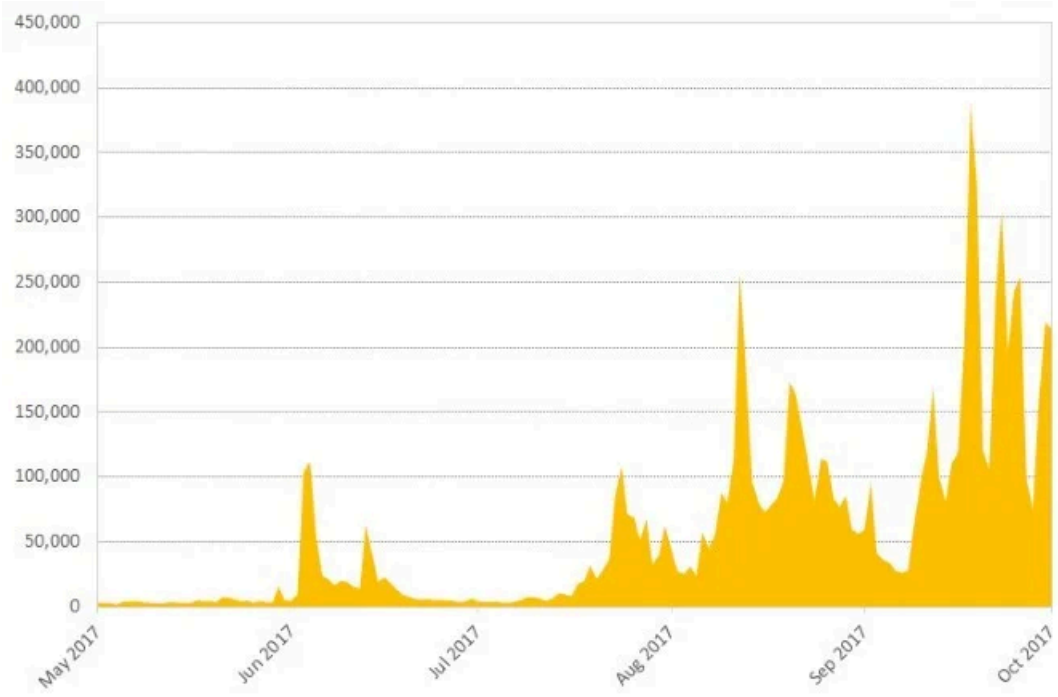
According to Symantec, the reasons for the screenshot behavior may be that Necurs operators are looking for more clues about the computers they infect, besides the telemetry data they collect shortly after infection.

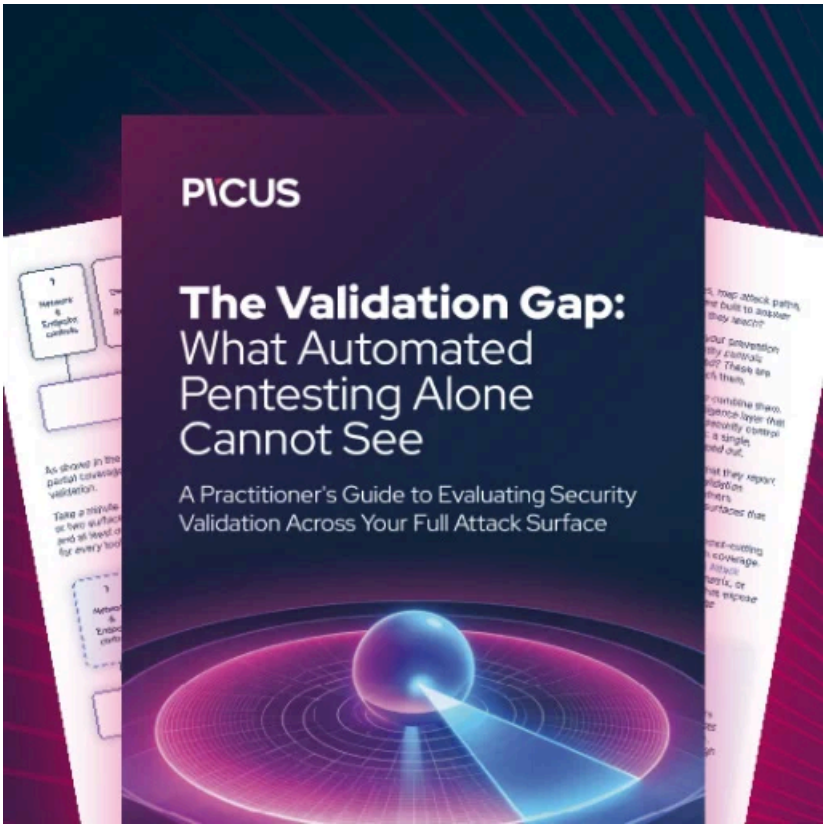
This info could allow them to detect when they infect more valuable environments, like the ones running professional office-related software, which usually mean computers on corporate networks.

As for the error reporting feature, this is easily explained, as malware authors, just like any other software developer, are always looking to gather data on crashes to improve their application.

"After all, you can’t count on the victims to report back errors and issues!," Symantec points out about the crash reporting functionality.

Symantec also provided a graphic with Necurs spam waves this year, confirming previous reports of increased activity in the past few months. Currently, the Necurs botnet is busy pushing the Locky ransomware and the TrickBot banking trojan.






## 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.

---

Source: https://www.bleepingcomputer.com/news/security/necurs-malware-will-now-take-a-screenshot-of-your-screen-report-runtime-errors/