# Numbers Show Locky Ransomware Is Slowly Fading Away

By Catalin Cimpanu

Published: 2017-03-20 · Archived: 2026-04-05 13:58:29 UTC

Over the past six months, the number of Locky ransomware infections has gone down and is expected to reach an all-time low this month, in March.

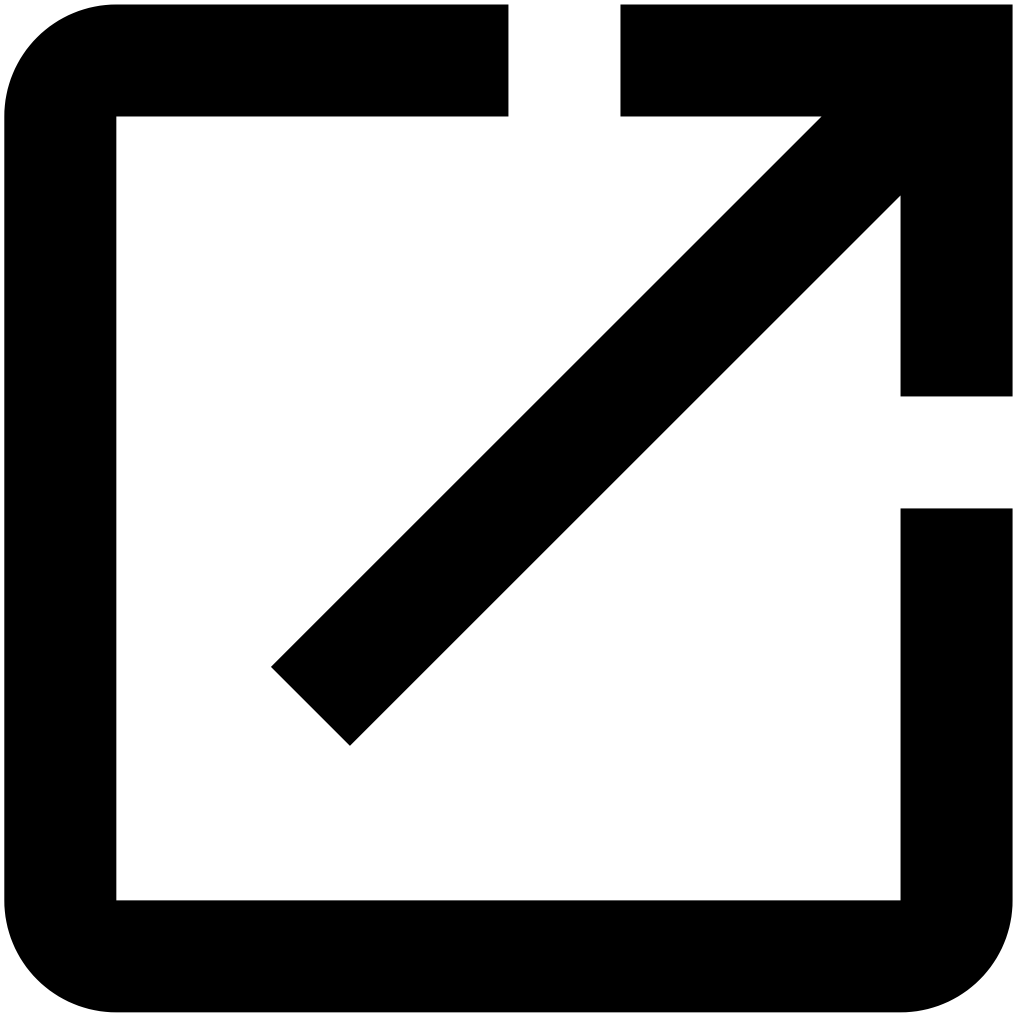
Ever since the ransomware launched in mid-February 2016, Locky has been one of the most active and prevalent ransomware families on the Internet.

## The Necurs and Locky connection

From the start, it became apparent that Locky's growth was powered by Necurs, a huge botnet of infected devices used to send email spam.

Prior to Locky's appearance, Necurs had been used exclusively to deliver the Dridex banking trojan. This changed when Locky appeared, and Necurs slowly replaced Dridex with Locky as its primary payload.


DIE LINKE.
0:00



Necurs spewed out so much Locky ransomware spam, that Locky became the first ever ransomware strain to reach Check Point's malware top 3, back in September 2016.

## Necurs abandons Locky at the start of 2017

But not all things last forever and things changed over the New Year. Necurs operators are known to take a few weeks off from before Christmas to mid-January. They've been taking this break all the years they've been in business, and they did the same in the 2016-2017 holiday.

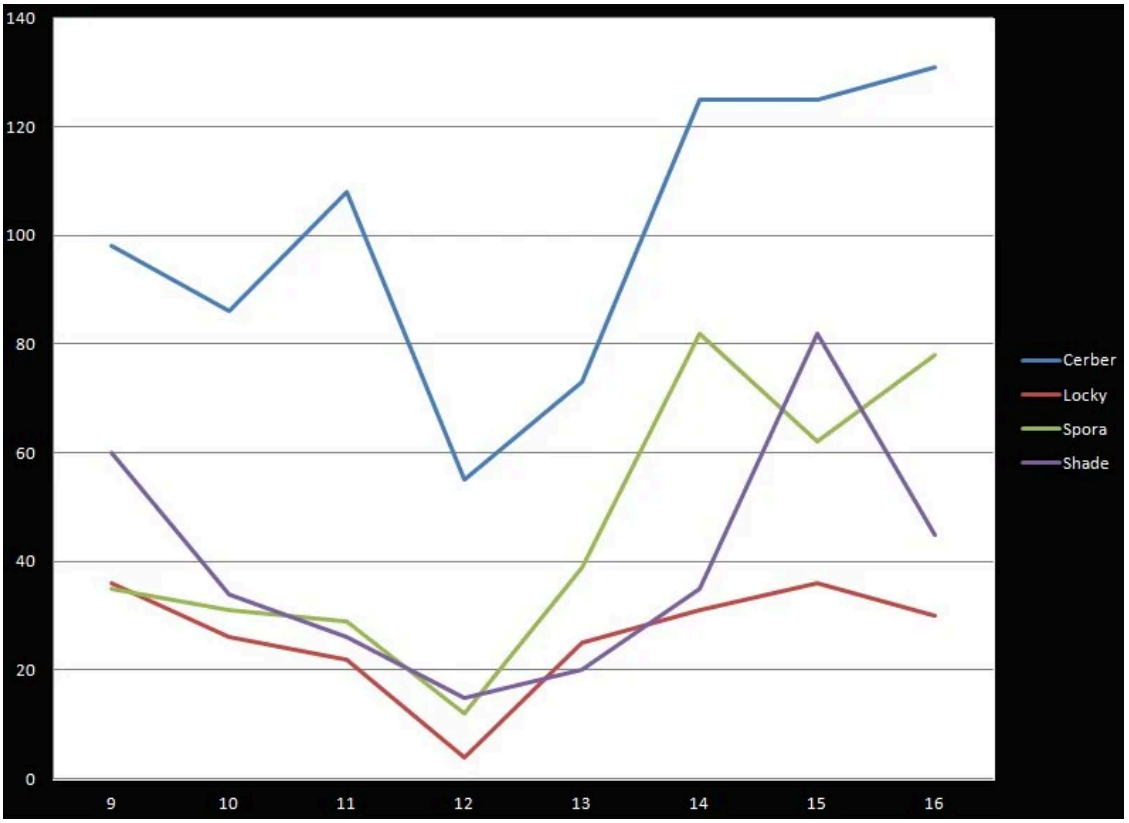
Something happened over this past holiday season because when it came back, the Necurs botnet wasn't pushing Locky at the same levels.

Many researchers noted this event, such as Cisco Talos. The team behind the ID Ransomware service noticed the same thing.

The graph below shows the number of users who used the ID-Ransomware service to identify Locky infections. The drop in Locky activity since the start of the new year is evident.


On the other hand, Cerber, who once looked dead, has now taken Locky's place as today's top ransomware threat. Researchers from Morphisec have documented Cerber's recent rise.


Another graph from the ID Ransomware team provided by MalwareHunter shows Locky's activity during the past week. The graph clearly shows that Locky is being "outperformed" even by newcomers like Spora.




Besides Cisco and ID Ransomware, others have also noticed Locky's downfall in recent months.

## Researchers: No new Locky spam from Necurs

MalwareTech, a security researcher that keeps track of the Necurs botnet in particular, confirmed ID Ransomware's observation.

"There's been none [Locky spam from Necurs] at all this year," the researchers told Bleeping Computer. "Necurs is back and doing something totally different: penny stock pump & dumps," the researcher later tweeted, referring to pump & dump spam campaigns which try to artificially boost stock prices so crooks can buy low and sell high.

Similarly, a security researcher that goes by @dvk01uk, specialized in email spam analysis, also noticed a fall in Locky spam numbers.

"Yes, very reduced," he told Bleeping Computer today. "About all I see are the daily fake FedEx, UPS, USPS 'cannot deliver your parcel' messages."

These are spam messages that come with email attachments laced with the Nemucod downloader, which in turn downloads the Kovter click fraud malware and the Locky ransomware.

This distribution scheme is the hallmark sign of an affiliate system distributing Locky. Previously, last year's massive spam campaigns sending Locky have not relied on Nemucod.

## No new Locky versions this year

Additionally, prior to going silent during the Christmas holiday, Locky received monthly updates, going through various extensions such as Zepto, Odin, Shit, Thor, Aesir, ZZZZZ, and Osiris. No new Locky variant has been seen since December.

Now, let's look at the big picture. Locky's first campaigns came via the Necurs botnet. Most of the massive spam distributing Locky also came via Necurs, which shows a clear connection between the Locky and the Necurs crews, who could be very well the same.

Furthermore, no new Locky activity has been spotted from the Necurs botnet, and no new version came out since the last Necurs+Locky campaigns last year.

All clues point to the (temporary) death of Locky, albeit the ransomware appears to alive in some RaaS affiliate schemes. We'll just have to wait and see what happens with Locky in the coming months. Who knows, maybe they'll release decryption keys like the TeslaCrypt group. Fingers crossed!



---

Source: https://www.bleepingcomputer.com/news/security/numbers-show-locky-ransomware-is-slowly-fading-away/