New Locky Ransomware Phishing Attacks Beat Machine Learning Tools

By Jai Vijayan

Published: 2017-09-28 · Archived: 2026-04-05 18:35:15 UTC

The Locky ransomware strain, initially spotted in February 2016, has emerged as one of the most dangerous examples of the highly persistent and pernicious nature of modern cyber extortion campaigns.

The operators of the malware—among the most prolific ransomware samples ever—have shown a tendency to launch brief waves of attacks, go dormant for some time and then come back with a vengeance to torment businesses and consumers.

The most recent of those waves happened in late September and appeared targeted at businesses in multiple regions including North America, Europe and Southeast Asia, security vendor Comodo said in a soon-to-be-published special report.

Comodo described the September Locky campaign as building on two previous attack waves that the vendor reported on last month (here & here). As with the earlier attacks, the latest ones too used a botnet of zombie computers distributed around the word to send highly convincing looking phishing emails to potential victims.

One of the emails used in the phishing campaign was designed to appear like a scanned document from a business printer located at the victim's organization. To lend credibility, the phishing email included a model number for a very popular Konica Minolta scanner/printer widely deployed in businesses around the world.

A second email used in the phishing campaign was spoofed to appear like a query pertaining to the status of a vendor invoice. Recipients, who were lured into opening the attachments in these emails, downloaded Locky on their systems. The average ransom amount for the decryption key tended to range between $2,000 and $4,000.

The social engineering that was used to engage victims was carefully designed to slip past malware detection tools including those using machine-learning algorithms to spot phishing emails, says Fatih Orhan, vice president, threat labs at Comodo.

The attachment in one of the emails for instance was disguised as a printer output, and it contained a script inside an archive file. "This is not enough to make a phishing detection," Orhan says.

"Machine learning algorithms need to extract the attachment, open the archive, extract the script and understand it has a malicious intent," he notes. "Usually, these scripts contain just a download component and do not have malicious intent on their own. That’s why even machine learning is not sufficient in making these kinds of detections."

Additional measures are needed to run the script dynamically and to download the actual payload, and conduct malware analysis to detect phishing, Orhan explains.

Security researchers at Comodo detected and analyzed over 110,000 Locky-related emails at customer endpoints over a three-day period between Sept. 17 and Sept. 20.

The phishing emails that purported to be printer output were sent from a total of nearly 120,000 IP addresses from 139 country code top-level domains, according to Comodo. The other phishing email that was utilized in the September Locky campaign was sent from over 12,350 IP addresses in 142 countries. In total, the IP addresses used in the September attacks were scattered across more than half of all countries in the world.

Many of the IP addresses belonged to infected computers belonging to individual consumers. But there were a fair number of systems belonging to ISPs as well, Orhan says.

Significantly, a considerable number of servers used to spread the phishing email were the same as ones used in previous campaigns. "These are mostly compromised servers as we understand," Orhan said. "The fact that they are used for multiple attacks shows there is no remediation on these servers."

Many ISPs also do not appear to have controls for spotting infected systems belonging to their customers that are being used to continuously send phishing emails over weeks. "It's possible they don't have real-time detection capabilities. But the attacks being continuous over weeks, shows they are incompetent in securing the network traffic they are providing," Orhan says.

Locky was one of the most widely distributed ransomware tools in 2016 and looks set to be among the most widely distributed pieces of malware this year as well. One of its most notable victims—at least publicly disclosed ones—is Hollywood Presbyterian Medical Center, which was forced to pay $17,000 to retrieve a critical database that was encrypted with the malware.

News about the latest Locky attacks comes even as Europol this week warned of ransomware eclipsing all other forms of cyber threat for the second year in a row.

"Ransomware attacks have eclipsed most other global cybercrime threats, with the first half of 2017 witnessing ransomware attacks on a scale previously unseen following the emergence of self-propagating 'ransomworms,' " Europol said citing examples like WannaCry and Petya/NotPetya outbreaks.

Related content:

About the Author

Contributing Writer

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year career at Computerworld, Jai also covered a variety of other technology topics, including big data, Hadoop, Internet of Things, e-voting, and data analytics. Prior to Computerworld, Jai covered technology issues for The Economic Times in Bangalore, India. Jai has a Master's degree in Statistics and lives in Naperville, Ill.
