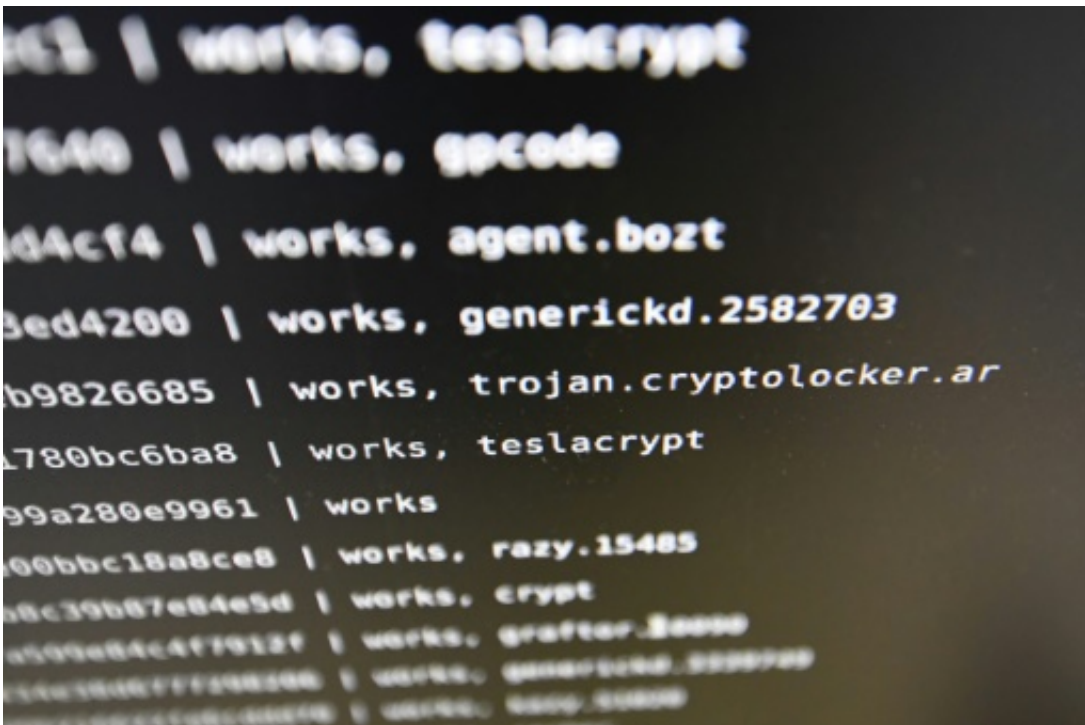


Growing global cyberattack hits 200,000 victims so far

May 14 2017, by Robin Millard



The wave of attacks on May 12 hit Britain's health service, Russia's interior ministry and French carmaker Renault, along with many other organisations around the world

The unprecedented global cyberattack has hit more than 200,000 victims in scores of countries, Europol said Sunday, warning that the situation could escalate when people return to work.

An international manhunt was well under way for the plotters behind the world's biggest-ever computer ransom assault.

The indiscriminate attack, which began Friday, struck banks, hospitals and government agencies in more than 150 countries, exploiting known vulnerabilities in old Microsoft computer operating systems.

US package delivery giant FedEx, European car factories, Spanish telecoms giant Telefonica, Britain's health service and Germany's Deutsche Bahn rail network were among those hit.

Europol executive director Rob Wainwright said the situation could worsen on Monday as workers return to their offices after the weekend and log on.

"We've never seen anything like this," the head of the European Union's policing agency told Britain's ITV television, calling its reach "unprecedented".

"The latest count is over 200,000 victims in at least 150 countries. Many of those victims will be businesses, including large corporations.

"We're in the face of an escalating threat.

"I'm worried about how the numbers will continue to grow when people go to work and turn on their machines on Monday."

The 5,500-strong Renault factory in Douai, northern France, one of the most important car plants in the country, will not open on Monday due to the attack, sources told AFP.

'Oops' message, \$300 ransom

Images appear on victims' screens demanding payment of \$300 (275 euros) in the virtual currency Bitcoin, saying: "Oops, your files have been encrypted!"

The 'Wannacry' ransomware attack

The attack has hit more than 200,000 victims in at least 150 countries, says Europol



The 'Wannacry' ransomware attack

Payment is demanded within three days or the price is doubled, and if none is received within seven days the locked files will be deleted, according to the screen message.

Bitcoin, the world's most-used virtual currency, allows for anonymous transactions, which happen via heavily encrypted codes.

Experts and governments alike warn against ceding to the demands and Wainwright said few victims so far have been paying up.

US software firm Symantec said that part-way through Saturday,

transactions totalling \$28,600 had taken place through the five Bitcoin addresses used by the ransomware.

"Paying the ransom does not guarantee the encrypted files will be released," the US Department of Homeland Security's computer emergency response team said.

"It only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information."

The culprits used a digital code believed to have been developed by the US National Security Agency—and subsequently leaked as part of a document dump, according to researchers at the Moscow-based computer security firm Kaspersky Lab.

A hacking group called Shadow Brokers released the malware in April, claiming to have discovered the flaw from the NSA, Kaspersky said.

The attack is unique, according to Europol, because it combines ransomware with a worm function, meaning once one machine is infected, the entire internal network is scanned and other vulnerable machines are infected.

The attack therefore spread faster than previous, smaller-scale ransomware attacks.

Microsoft said the situation was "painful" and that it was taking "all possible actions to protect our customers".

It issued guidance for people to protect their systems, while taking the highly unusual step of reissuing security patches first made available in March for Windows XP and other older versions of its operating system.



A computer technician connects a computer into a network server in an office building in Washington, DC on May 13, 2017

Banks, trains and automobiles

Symantec said the majority of organisations affected were in Europe.

The companies and [government agencies](#) targeted were diverse.

Europol's Wainwright said few banks in Europe had been affected, having learned through the "painful experience of being the number one target of cyber crime" the value of having the latest cyber security in place.

Russia's interior ministry said some of its computers had been hit, while

the country's banking system was also attacked, although no problems were detected, as was the railway system.

French carmaker Renault was forced to stop production at sites in France, Slovenia and Romania, while FedEx said it was "implementing remediation steps as quickly as possible".

Germany's rail operator Deutsche Bahn said its station display panels were affected. Universities in China, Italy and Greece were also hit.

Meanwhile G7 finance ministers meeting in Italy vowed to unite against cyber crime, as it represented a growing threat to their economies and should be tackled as a priority.

The danger will be discussed at the G7 leaders' summit next month.

The US Treasury Department said it will play a "leading role" in protecting the global financial system's IT infrastructure.

US Treasury Secretary Steven Mnuchin "has made protecting America's financial infrastructure from cyberattacks a top priority," a senior department official told reporters on the return flight from Italy.

© 2017 AFP

Citation: Growing global cyberattack hits 200,000 victims so far (2017, May 14) retrieved 3 July 2024 from <https://phys.org/news/2017-05-global-cyberattack-victims.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.