An alert researcher, cooperation helped stem cyberattack

May 14 2017

People walk past a Megafon mobile phones shop in Moscow, Russia, Saturday, May 13, 2017. A top Russian mobile operator said Friday it had come under cyberattacks that appeared similar to those that have crippled some U.K. hospitals. Pyotr Lidov, a spokesman for Megafon, said Friday's attacks froze computers in company's offices across Russia. (AP Photo/Ivan Sekretarev)

The cyberattack that spread malicious software around the world, shutting down networks at hospitals, banks and government agencies, was stemmed by a young British researcher and an inexpensive domain

registration, with help from another 20-something security engineer in the U.S.

Britain's National Cyber Security Center and others were hailing the cybersecurity researcher, a 22-year-old identified online only as MalwareTech, who—unintentionally at first—discovered a "kill switch" that halted the unprecedented outbreak.

By then, the "ransomware" attack had hobbled Britain's hospital network and computer systems in several countries, in an effort to extort money from computer users. But the researcher's actions may have saved companies and governments millions of dollars and slowed the outbreak before computers in the U.S. were more widely affected.

MalwareTech said in a in a blog post Saturday that he had returned from lunch with a friend on Friday and learned that networks across Britain's health system had been hit by ransomware, tipping him off that "this was something big."

He began analyzing a sample of the malicious software and noticed its code included a hidden web address that wasn't registered. He said he "promptly" registered the domain, something he regularly does to try to discover ways to track or stop malicious software.

In this May 12, 2017 photo, a display panel with an error can be seen at the main railway station in Chemnitz, Germany. Germany's national railway says that it was among the organizations affected by the global cyberattack but there was no impact on train services. Deutsche Bahn said early Saturday that departure and arrival display screens at its stations were hit Friday night by the attack. (P. Goezelt/dpa via AP)

Across an ocean, Darien Huss, a 28-year-old research engineer for the cybersecurity firm Proofpoint, was doing his own analysis. The western Michigan resident said he noticed the authors of the malware had left in a feature known as a kill switch. Huss took a screen shot of his discovery and shared it on Twitter.

MalwareTech and Huss are part of a large global cybersecurity community of people, working independently or for security companies, who are constantly watching for attacks and working together to stop or prevent them, often sharing information via Twitter. It's not uncommon for them to use aliases, either to protect themselves from retaliatory attacks or for privacy.

Soon Huss and MalwareTech were communicating about what they'd found: That registering the domain name and redirecting the attacks to the server of Kryptos Logic, the security firm Malware Tech worked for, had activated the kill switch, halting the ransomware's infections—creating what's called a "sinkhole."

Who perpetrated this wave of attacks remains unknown. Two security firms—Kaspersky Lab and Avast—said they identified the malicious software in more than 70 countries. Both said Russia was hit hardest.

An exterior view shows the main entrance of St Bartholomew's Hospital, in London, one of the hospitals whose computer systems were affected by a cyberattack, Friday, May 12, 2017. A large cyberattack crippled computer systems at hospitals across England on Friday, with appointments canceled, phone lines down and patients turned away. (AP Photo/Matt Dunham)

These hackers "have caused enormous amounts of disruption— probably the biggest ransomware cyberattack in history," said Graham Cluley, a veteran of the anti-virus industry in Oxford, England.

The ransomware exploits a vulnerability in Microsoft Windows that was purportedly identified by the U.S. National Security Agency for its own intelligence-gathering purposes. Hackers said they stole the tools from the NSA and dumped them on the internet.

A malware tracking map showed "WannaCry" infections were widespread. Britain canceled or delayed treatments for thousands of patients. Train systems were hit in Germany and Russia, and phone companies in Madrid and Moscow. Renault's futuristic assembly line in Slovenia, where rows of robots weld car bodies together, was stopped cold. In Brazil, the social security system had to disconnect its computers and cancel public access.

But while FedEx Corp. reported that its Windows computers were "experiencing interference" from malware—it wouldn't say if it had been hit by the ransomware—other impacts in the U.S. were not readily apparent on Saturday.

A security guard stands outside the Telefonica headquarters in Madrid, Spain, Friday, May 12, 2017. The Spanish government said several companies including Telefonica had been targeted in ransomware cyberattack that affected the Windows operating system of employees' computers. (AP Photo/Paul White)

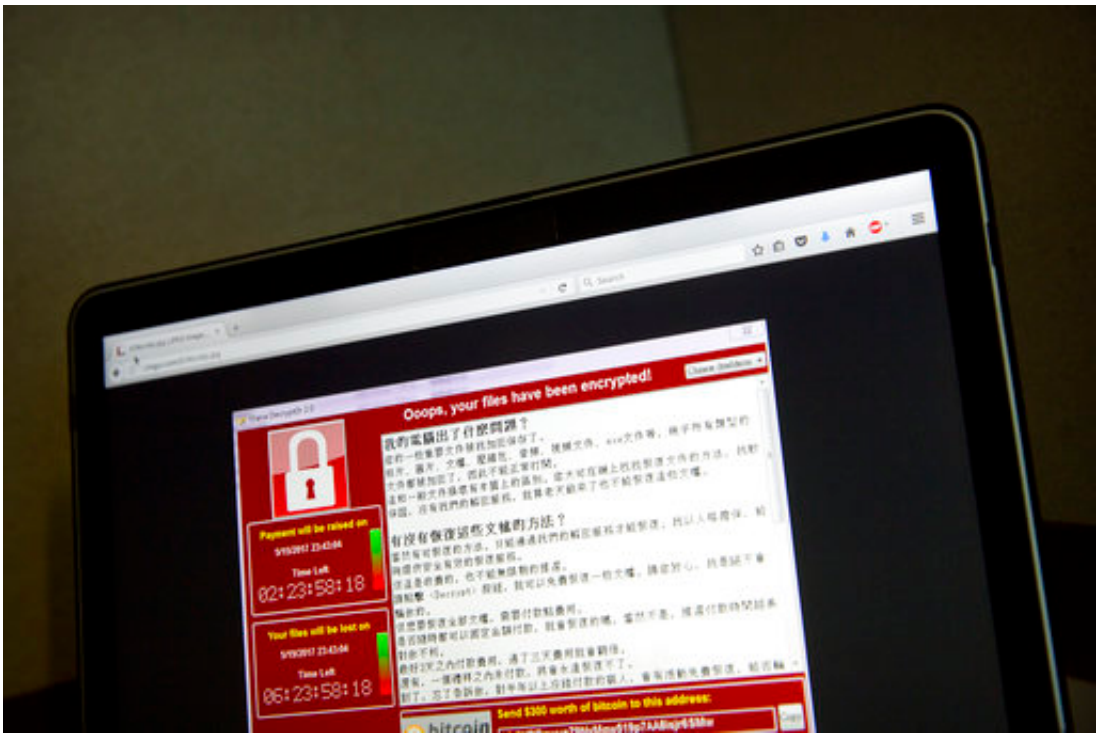
The worldwide effort to extort cash from computer users spread so widely that Microsoft quickly changed its policy, making security fixes for this vulnerability available for free for the older Windows systems still used by millions of individuals and smaller businesses.

Britain's home secretary said one in five of 248 National Health Service groups had been hit. Home Secretary Amber Rudd said all but six of the NHS trusts back to normal Saturday.

The U.K.'s National Cyber Security Center was "working round the clock" to restore vital health services, while urging people to update

security software fixes, run anti-virus software and back up their data elsewhere.

All this may be just a taste of what's coming, another cyber security expert warned.



A screenshot of the warning screen from a purported ransomware attack, as captured by a computer user in Taiwan, is seen on laptop in Beijing, Saturday, May 13, 2017. Dozens of countries were hit with a huge cyberextortion attack Friday that locked up computers and held users' files for ransom at a multitude of hospitals, companies and government agencies. (AP Photo/Mark Schiefelbein)

Computer users worldwide—and everyone else who depends on them—should assume that the next big "ransomware" attack has already been launched, and just hasn't manifested itself yet, said Ori Eisen,

founder of the Trusona cybersecurity firm in Scottsdale, Arizona.

The attack held hospitals and other entities hostage by freezing computers, encrypting data and demanding money through online bitcoin payments. But it appears to be "low-level" stuff, Eisen said Saturday, given the amount of ransom demanded—$300 at first, rising to $600 before it destroys files hours later.

This is already believed to be the biggest online extortion attack ever recorded, disrupting services in nations as diverse as the U.S., Ukraine, Brazil, Spain and India. Europol, the European Union's police agency, said the onslaught was at "an unprecedented level and will require a complex international investigation to identify the culprits."

Huss and others were calling MalwareTech a hero on Saturday, with Huss adding that the global cybersecurity community was working "as a team" to stop the infections from spreading.

People outside a Megafon mobile phone shop in Moscow, Russia, on Saturday, May 13, 2017. A top Russian mobile operator said Friday it had come under cyberattacks that appeared similar to those that have crippled some U.K. hospitals. Pyotr Lidov, a spokesman for Megafon, said Friday's attacks froze computers in company's offices across Russia. (AP Photo/Ivan Sekretarev)

"I think the security industry as a whole should be considered heroes," he said.

But he also said he's concerned the authors of the malware could re-release it—perhaps in the next few days or weeks—without a kill switch or with a better one, or that copycats could mimic the attack.

The MalwareTech researcher agreed that the threat hasn't disappeared.

"One thing that is very important to note is our sinkholing only stops this sample and there is nothing stopping them removing the domain check and trying again, so it's incredibly important that any unpatched systems are patched as quickly as possible," he warned.

This April 12, 2016 file photo shows the Microsoft logo in Issy-les-Moulineaux, outside Paris, France. The cyberextortion attack hitting dozens of countries was a "perfect storm" of sorts. It combined a known and highly dangerous security hole in Microsoft Windows, tardy users who didn't apply Microsoft's March software fix, and a software design that allowed the malware to spread quickly once inside university, business and government networks. (AP Photo/Michel Euler, File)

The kill switch also couldn't help those already infected. Short of paying, options for these individuals and companies are usually limited to recovering data files from a backup, if available, or living without them.

Security experts said it appeared to be caused by a self-replicating piece of software that enters companies when employees click on email attachments, then spreads quickly as employees share documents.

The security holes it exploits were disclosed weeks ago by

TheShadowBrokers, a mysterious hacking group. Microsoft swiftly released software "patches" to fix those holes, but many users still haven't installed updates or still use older versions of Windows.

People inside a Megafon mobile phones shop in Moscow, Russia, Saturday, May 13, 2017. A top Russian mobile operator said Friday it had come under cyberattacks that appeared similar to those that have crippled some U.K. hospitals. Pyotr Lidov, a spokesman for Megafon, said Friday's attacks froze computers in company's offices across Russia. (AP Photo/Ivan Sekretarev)

A view of the logo of a Megafon mobile phone shop, in Moscow, Russia, on Saturday, May 13, 2017. A top Russian mobile operator said Friday it had come under cyberattacks that appeared similar to those that have crippled some U.K. hospitals. Pyotr Lidov, a spokesman for Megafon, said Friday's attacks froze computers in company's offices across Russia. (AP Photo/Ivan Sekretarev)

© 2017 The Associated Press. All rights reserved.

Citation: An alert researcher, cooperation helped stem cyberattack (2017, May 14) retrieved 20 June 2024 from https://phys.org/news/2017-05-cooperation-stem-cyberattack.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.