Ransomware virus hacks 100k computers across 99 countries

LIVE UPDATES: Mass cyberattack strikes computer systems worldwide

An increase in activity of the malware was noticed starting from 8am CET (07:00 GMT) Friday, security software company Avast reported, adding that it "*quickly escalated into a massive spreading*."

In a matter of hours, over 75,000 attacks have been detected worldwide, the company said. Meanwhile, the MalwareTech tracker detected over 100,000 infected systems over the past 24 hours.

Читать

Jakub Kroustek @JakubKroustek

#wcry #WannaCry #WannaCrypt0r #ransomware hitting 100k Avast detections in less than 24 hours. 57% in Russia. Patch your systems!

02:25 - 13 May 2017

Dozens of countries around the globe have been affected, with the number of victims still growing, according to the Russian multinational cybersecurity and anti-virus provider, the Kaspersky Lab.

Follow

Costin Raiu

So far, we have recorded more than 45,000 attacks of the #WannaCry ransomware in 74 countries around the world. Number still growing fast.

7:01 PM - 12 May 2017

The ransomware, known as WanaCrypt0r 2.0, or WannaCry, is believed to have infected National Health Service (NHS) hospitals in the UK and Spain's biggest national telecommunications firm, Telefonica.

READ MORE: Hospital computers across Britain shut down by cyberattack, hackers demanding ransom

Britain and Spain are among the first nations who have officially recognized the attack. In Spain, apart from the telecommunications giant, Telefonica, a large number of other companies has been infected with the malicious software, Reuters reported.

The virus is said to attack computers on an internal network, as is the case with Telefonica, without affecting clients.

'Militarization of cyberspace going out of control': IT experts talk WannaCry ransomware hackstorm...

The WannaCry ransomware that has infected tens of thousands of Windows operating systems across the globe spread like wildfire because of the NSA exploit, security experts agree, noting the threats...

Computers at Russia's Interior Ministry have been infected with the malware, the ministry said Friday evening.

Some 1,000 Windows-operated PCs were affected, which is less than one percent of the total number of such computers in the ministry, spokeswoman Irina Volk said in a statement. The virus has been localized and steps are being taken to eliminate it.

The servers of the ministry have not been affected, Volk added, saying it's operated by different systems for Russia-developed data processing machines.

"*Several*" computers of Russia's Emergency Ministry had also been targeted, its representative told TASS, adding, that "*all of the attempted attacks had been blocked, and none of the computers were infected with the virus*."

Read more

Leaked NSA exploit blamed for global ransomware cyberattack

Russian telecom giant, Megafon has also been affected.

"*The very virus that is spreading worldwide and demanding $300 to be dealt with has been found on a large number of our computers in the second half of the day today*," Megafon's spokesperson Pyotr Lidov told RT.

The internal network had been affected, he said, adding that in terms of the company's customer services, the work of the support team had been temporarily hindered, "*as operators use computers*" to provide their services.

The company immediately took appropriate measures, the spokesperson said, adding that the incident didn't affect subscribers' devices or Megafon signal capabilities in any way.

British Prime Minister Theresa May has said the cyberattack on UK hospitals is part of a wider international attack.

In Sweden, the mayor of Timra said "*around 70 computers have had a dangerous code installed*," Reuters reported.

According to Avast, the ransomware has also targeted Ukraine and Taiwan.

The virus is apparently the upgraded version of the ransomware that first appeared in February. Believed to be affecting only Windows operated computers, it changes the affected file extension names to ".WNCRY."

It then drops ransom notes to a user in a text file, demanding $300 worth of bitcoins to be paid to unlock the infected files within a certain period of time.

Follow

Edward Snowden

In light of today's attack, Congress needs to be asking @NSAgov if it knows of any other vulnerabilities in software used in our hospitals.

9:08 PM - 12 May 2017

While the victim's wallpaper is being changed, affected users also see a countdown timer to remind them of the limited time they have to pay the ransom. If they fail to pay, their data will be deleted, cybercriminals warn.

According to security experts, the ransomware exploits a vulnerability that was discovered and developed by the National Security Agency. The exploit was leaked by a group calling itself the Shadow Brokers, that has been distributing the stolen NSA hacking tools online since last year

How to Protect Yourself as Ransomware Attack Spreads Around the Globe

Hospitals and other healthcare providers across England were forced to cancel countless appointments and divert ambulances on Friday after a massive ransomware attack crippled their computer systems. In the hours that followed, the crisis spread to facilities in at dozens of other countries, according to news reports.

FedEx was one of the big corporations affected by the attack, saying that "like many other companies, FedEx is experiencing interference with some of our Windows-based systems caused by malware. We are implementing remediation steps as quickly as possible. We regret any inconvenience to our customers."

Although this latest attack was massive in scope, ransomware threats often strike the personal computers of individual consumers, too.

Here's what you need to know and how to protect yourself.

What Is Ransomware?

Ransomware is a form of malware designed to steal money from individuals, businesses and other organizations by holding their data hostage. Imagine coming home to find a big padlock on your front door and a criminal standing next to it, demanding money to let you in. That's ransomware. Only instead of being locked out of your house, you're locked out of all your personal files. The next time you log on, your computer displays a ransom note saying your data has been encrypted, with instructions on how to pay to unlock it.

Can Hackers Really Make Money Doing This?

Oh, yes. Ransomware is big business. Ransoms can range from a few hundred to thousands of dollars and are usually paid in the "virtual" currency Bitcoin, which is nearly impossible to trace. In some cases, the longer you wait to pay, the higher the ransom becomes.

According to cybersecurity firm Symantec's Internet Security Threat Report released in April, the number of new versions of ransomware uncovered during 2016 more than tripled to 101, while the number of ransomware infections the company spotted jumped 36 percent. Verizon's recently released 2017 Data Breach Investigations Report notes that ransomware accounted for 72 percent of the malware incidents involving the heathcare industry last year.

Why Is This Particular Ransomware Attack Significant?

Friday's attack affected at least 25 of the UK's National Health Service's hospitals and other organizations. But NHS says it was not the specific target of the attack. It does not appear that patient information was accessed, according to the organization, but its investigation into the matter is still in the early stages. Barts Health, which manages a handful of major hospitals in London and elsewhere, also confirmed it was experiencing a "major IT disruption."

The malware arrived in encrypted files distributed by email. Once a computer was infected, the user received a note demanding $300 in bitcoin to restore access to patient information and other data on the device.

British Prime Minister Theresa May called it an "international attack" affecting a "number of countries and organizations." CNN put the figure at 74 countries.

Has This Ever Happened in the U.S.?

Yes. One of the best known examples involved L.A.'s Hollywood Presbyterian Medical Center, which in February 2016 said it paid a ransom of $17,000 to get its computer systems unlocked.

Because of the large amount of personal information collected about patients, hospitals and other healthcare providers are prime ransonware targets. If a doctor can't access information about a patient's medications and pre-exisiting conditions, it's virtually impossible to provide treatment, forcing the doctor and patient to reschedule appointments. And that can result in millions of dollars in lost productivity.

So, even though medical computer systems are routinely backed up, and nearly all that data can be recovered and restored, hospitals often pay the ransom in an effort to speed things up and minimize financial losses.

How Does Your Device Get Infected?

Whether they involve a computer nework run by a business or hospital, or just an average person's personal PC, most ransomware infections happen when a user is lured by a bogus “phishing” email to a site that infects his or her computer, or by clicking on an attached file that secretly installs it.

How can you avoid having your data taken hostage?

You avoid ransomware the same way you avoid any malware infection: By being careful. While that's not always easy, there are things you can do to steer clear of problems.

Don’t casually click a link inside an email; instead, type the web address directly into your browser.

Never open an attachment unless you were expecting to receive it and you're certain of what it is.

Don't spend time in the disreputable corners of the internet that specialize in risqué content or pirated movies; you can get infected simply by visiting a dodgy site.

Never install software just because a web site tells you to do it.

And always keep a backup copy of all your personal files on a separate drive or with a "cloud"-based backup service. That way, if the worst happens, you'll always have access to your most important data.

Medical EXPOSE

http://www.medicalexpose.com/