10-The New York Times-Hackers

Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool

Send any friend a story

As a subscriber, you have 10 gift articles to give each month. Anyone can read what you share.

Give this article

763

Read in app

Ambulance staff at a National Health Service hospital in London on Friday. Several hospitals across Britain were hit by a large-scale cyberattack, causing failures to computer systems.Credit…Andy Rain/European Pressphoto Agency

Leer en español

SAN FRANCISCO — Hackers exploiting malicious software stolen from the National Security Agency executed damaging cyberattacks on Friday that hit dozens of countries worldwide, forcing Britain's public health system to send patients away, freezing computers at Russia's Interior Ministry and wreaking havoc on tens of thousands of computers elsewhere.

The attacks amounted to an audacious global blackmail attempt spread by the internet and underscored the vulnerabilities of the digital age.

Transmitted via email, the malicious software locked British hospitals out of their computer systems and demanded ransom before users could be let back in — with a threat that data would be destroyed if the demands were not met.

By late Friday the attacks had spread to more than 74 countries, according to security firms tracking the spread. Kaspersky Lab, a Russian cybersecurity firm, said Russia was the worst-hit, followed by Ukraine, India and Taiwan. Reports of attacks also came from Latin America and Africa.

The attacks appeared to be the largest ransomware assault on record, but the scope of the damage was hard to measure. It was not clear if victims were paying the ransom, which began at about $300 to unlock individual computers, or even if those who did pay would regain access to their data.

Security experts described the attacks as the digital equivalent of a perfect storm. They began with a simple phishing email, similar to the one Russian hackers used in the attacks on the Democratic National Committee and other targets last year. They then quickly spread through victims' systems using a hacking method that the N.S.A. is believed to have developed as part of its arsenal of cyberweapons. And finally they encrypted the computer systems of the victims, locking them out of critical data, including patient records in Britain.

The connection to the N.S.A. was particularly chilling. Starting last summer, a group calling itself the "Shadow Brokers" began to post software tools that came from the United States government's stockpile of hacking weapons.

The attacks on Friday appeared to be the first time a cyberweapon developed by the N.S.A., funded by American taxpayers and stolen by an adversary had been unleashed by cybercriminals against patients, hospitals, businesses, governments and ordinary citizens.

Something similar occurred with remnants of the "Stuxnet" worm that the United States and Israel used against Iran's nuclear program nearly seven years ago. Elements of those tools frequently appear in other, less ambitious attacks.

The United States has never confirmed that the tools posted by the Shadow Brokers belonged to the N.S.A. or other intelligence agencies, but former intelligence officials have said that the tools appeared to come from the

N.S.A.’s “Tailored Access Operations” unit, which infiltrates foreign computer networks. (The unit has since been renamed.) *[Deny]*

The attacks on Friday are likely to raise significant questions about whether the growing number of countries developing and stockpiling cyberweapons can avoid having those same tools purloined and turned against their own citizens. *[Worry]*

A new strain of ransomware spread rapidly around the world on Friday.

They also showed how easily a cyberweapon can wreak havoc, even without shutting off a country’s power grid or its cellphone network.

In Britain, hospitals were locked out of their systems and doctors could not call up patient files. Emergency rooms were forced to divert people seeking urgent care.

In Russia, the country’s powerful Interior Ministry, after denying reports that its computers had been targeted, confirmed in a statement that “around 1,000 computers were infected,” which it described as less than 1 percent of its total. The ministry, which oversees Russia’s police forces, said technicians had contained the attack.

Some intelligence officials were dubious about that announcement because they suspect Russian involvement in the theft of the N.S.A. tools.

But James Lewis, a cybersecurity expert at the Center for Strategic and International Studies in Washington, said he suspected that criminals operating from Eastern Europe acting on their own were responsible. “This doesn’t look like state activity, given the targets that were hit,” he said.

Those targets included corporate computer systems in many other countries — including FedEx in the United States, one of the world’s leading international shippers, as well as Spain’s Telefónica and Russia’s MegaFon telecom giant.

It could take months to find who was behind the attacks — a mystery that may go unsolved. But they alarmed cybersecurity experts everywhere,

reflecting the enormous vulnerabilities to internet invasions faced by disjointed networks of computer systems.

There is no automatic way to “patch” their weaknesses around the world.

“When people ask what keeps you up at night, it’s this,” said Chris Camacho, the chief strategy officer at Flashpoint, a New York security firm tracking the attacks. Mr. Camacho said he was particularly disturbed at how the attacks spread like wildfire through corporate, hospital and government networks. *[Disappointment]*

Another security expert, Rohyt Belani, the chief executive of PhishMe, an email security company, said the wormlike capability of the malware was a significant shift from previous ransom attacks. “This is almost like the atom bomb of ransomware,” Mr. Belani said, warning that the attack “may be a sign of things to come.”

The hackers’ weapon of choice on Friday was Wanna Decryptor, a new variant of the WannaCry ransomware , which encrypts victims’ data, locks them out of their systems and demands ransoms.

Researchers said the impact and speed of Friday’s attacks had not been seen in nearly a decade, when the Conficker computer worm infected millions of government, business and personal computers in more than 190 countries, threatening to overpower the computer networks that controlled health care, air traffic and banking systems over the course of several weeks.

One reason the ransomware on Friday was able to spread so quickly was that the stolen N.S.A. hacking tool, known as “Eternal Blue,” affected a vulnerability in Microsoft Windows servers.

Hours after the Shadow Brokers released the tool last month, Microsoft assured users that it had already included a patch for the underlying vulnerability in a software update in March.

Image

The home page of the East and North Hertfordshire N.H.S. Trust website on Friday.Credit…East And North Hertfordshire NHS/Press Association, via Associated Press

But Microsoft, which regularly credits researchers who discover holes in its products, curiously would not say who had tipped the company off to the issue. Many suspected that the United States government itself had told Microsoft, after the N.S.A. realized that its hacking method exploiting the vulnerability had been stolen.

What to Know About Ransomware Attacks

Card 1 of 5

What are ransomware attacks? This form of cybercrime involves hackers breaking into computer networks and locking digital information until the victim pays for its release. Recent high-profile attacks have cast a spotlight on this rapidly expanding criminal industry, which is based primarily in Russia .

Why are they becoming more common? Experts say ransomware is attractive to criminals because the attacks take place mostly anonymously online, minimizing the chances of getting caught. The Treasury Department has estimated that Americans have paid $1.6 billion in ransoms since 2011.

Is there any connection to the rise of cryptocurrencies? The criminal industry’s growth has been abetted by cryptocurrencies , like Bitcoin, which allow hackers to transact with victims anonymously, though experts see virtual currency exchanges as a weak point for ransomware gangs.

What is being done about these attacks? The U.S. military has taken offensive measures against ransomware groups, and the Biden administration has taken legal and economic action. Recent attacks have propelled ransomware to the top of President Biden’s national security agenda .

Why is the government getting involved? The attacks, which were mostly directed at individuals a few years ago, have dramatically escalated as

hackers have begun targeting critical infrastructure in the U.S. , including a major gasoline pipeline and meat processing plants .

Privacy activists said if that were the case, the government would be to blame for the fact that so many companies were left vulnerable to Friday's attacks. It takes time for companies to roll out systemwide patches, and by notifying Microsoft of the hole only after the N.S.A.'s hacking tool was stolen, activists say the government would have left many hospitals, businesses and governments susceptible.

"It would be deeply troubling if the N.S.A. knew about this vulnerability but failed to disclose it to Microsoft until after it was stolen," Patrick Toomey, a lawyer at the American Civil Liberties Union, said on Friday. "These attacks underscore the fact that vulnerabilities will be exploited not just by our security agencies, but by hackers and criminals around the world."

During the Obama administration, the White House created a process to review software vulnerabilities discovered by intelligence agencies, and to determine which should be "stockpiled" for future offensive or defensive cyberoperations and which should be reported to the companies so that they could be fixed.

Last year the administration said that only a small fraction were retained by the government. But this vulnerability appeared to be one of them, and it was patched only recently, suggesting that the N.S.A. may have concluded the tool had been stolen and therefore warned Microsoft.

But that was clearly too little, and far too late.

On Friday, hackers took advantage of the fact that vulnerable targets — particularly hospitals — had yet to patch their systems, either because they had ignored advisories from Microsoft or because they were using outdated software that Microsoft no longer supports or updates.

The malware was circulated by email. Targets were sent an encrypted, compressed file that, once loaded, allowed the ransomware to infiltrate its targets. The fact that the files were encrypted ensured that the ransomware

would not be detected by security systems until employees opened them, inadvertently allowing the ransomware to replicate across their employers' networks.

Employees at Britain's National Health Service had been warned about the ransomware threat earlier on Friday. But it was too late. As the disruptions rippled through at least 36 hospitals, doctors' offices and ambulance companies across Britain, the health service declared the attack a "major incident," warning that local health services could be overwhelmed.

Britain's health secretary, Jeremy Hunt, was briefed by cybersecurity experts, while Prime Minister Theresa May's office said on television that "we're not aware of any evidence that patient data has been compromised."

As the day wore on, dozens of companies across Europe, Asia and the United States discovered that they had been hit with the ransomware when they saw criminals' messages on their computer screens demanding $300 to unlock their data. But the criminals designed their ransomware to increase the ransom amount on a set schedule and threatened to erase the hostage data after a predetermined cutoff time, raising the urgency of the attack and increasing the likelihood that victims would pay.

Without the ability to decrypt their data on their own, security experts said that victims who had not backed up their data were faced with a choice: Either live without their data or pay. It was not clear how many victims ultimately paid.

Security experts advised companies to immediately update their systems with the Microsoft patch.

Until organizations use the Microsoft patch, Mr. Camacho said, they could continue to be hit — not just by ransomware, but by all kinds of malicious tools that can manipulate, steal or delete their data.

"There is going to be a lot more of these attacks," he said. "We'll see copycats, and not just for ransomware, but other attacks."