For PC Virus Victims, Pay or Else

By NICOLE PERLROTH

Published: December 5, 2012 | 94 Comments

FACEBOOK

TWITTER

GOOGLE+

SAVE

E-MAIL

SHARE

PRINT

REPRINTS

CULVER CITY, Calif. — Kidnappers used to make ransom notes with letters cut out of magazines. Now, notes simply pop up on your computer screen, except the hostage is your PC.

Enlarge This Image

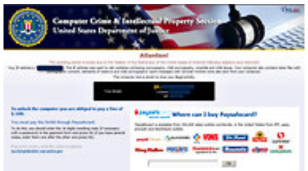
Michal Czerwonka for The New York Times

Security researchers Eric Chien, left, and Vikram Thakur at Symantec, where Mr. Chien has been tracking ransomware schemes.

In the past year, hundreds of thousands of people across the world have switched on their computers to find distressing messages alerting them that they no longer have access to their PCs or any of the files on them.

The messages claim to be from the Federal Bureau of Investigation, some 20 other law enforcement agencies across the globe or, most recently, Anonymous, a shadowy group of hackers. The computer users are told that the only way to get their machines back is to pay a steep fine.

Enlarge This Image



Computer Crime & Intellectual Property Section
United States Department of Justice

Attention!

Where can I buy Paysafecard?

Sometimes victims get a message, ostensibly from the F.B.I., accusing them of breaking the law and demanding a fine.

And, curiously, it's working. The scheme is making more than $5 million a year, according to computer security experts who are tracking them.

The scourge dates to 2009 in Eastern Europe. Three years later, with business booming, the perpetrators have moved west. Security experts say that there are now more than 16 gangs of sophisticated criminals extorting millions from victims across Europe.

Readers' Comments

Readers shared their thoughts on this article.

Read All Comments (94) »

The threat, known as ransomware, recently hit the United States. Some gangs have abandoned previously lucrative schemes, like fake antivirus scams and banking trojans, to focus on ransomware full time.

Essentially online extortion, ransomware involves infecting a user's computer with a virus that locks it. The attackers demand money before the computer will be unlocked, but once the money is paid, they rarely unlock it.

In the vast majority of cases, victims do not regain access to their computer unless they hire a computer technician to remove the virus manually. And even then, they risk losing

Log in to see what your friends are sharing on nytimes.com. Privacy Policy | What's This?

Log In With Facebook

What's Popular Now

Dave Brubeck, Jazz Musician, Dies at 91

Oscar Niemeyer, Modernist Architect of Brasília, Dies at 104

Today's Headlines Daily E-Mail

Sign up for a roundup of the day's top stories, sent every morning.

Sign Up

See Sample | Privacy Policy

Subscribe to Technology RSS Feeds

Technology News | Bits Blog
Internet | Start-Ups | Personal Tech
Business Computing | Companies | Pogue's Posts

MOST E-MAILED | MOST VIEWED

1. A Dark and Itchy Night

2. NICHOLAS D. KRISTOF
Gifts That Change Lives

all files and data because the best way to remove the virus is to wipe the computer clean.

It may be hard to fathom why anyone would agree to fork over hundreds of dollars to a demanding stranger, but security researchers estimate that 2.9 percent of compromised computer owners take the bait and pay. That, they say, is an extremely conservative estimate. In some countries, the payout rate has been as high as 15 percent.

That people do fall for it is a testament to criminals' increasingly targeted and inventive methods. Early variations of ransomware locked computers, displayed images of pornography and, in Russian, demanded a fee — often more than $400 — to have it removed. Current variants are more targeted and toy with victims' consciences.

Researchers say criminals now use victims' Internet addresses to customize ransom notes in their native tongue. Instead of pornographic images, criminals flash messages from local law enforcement agencies accusing them of visiting illegal pornography, gambling or piracy sites and demand they pay a fine to unlock their computer.

Victims in the United States see messages in English purporting to be from the F.B.I. or Justice Department. In the Netherlands, people get a similar message, in Dutch, from the local police. (Some Irish variations even demand money in Gaelic.) The latest variants speak to victims through recorded audio messages that tell users that if they do not pay within 48 hours, they will face criminal charges. Some even show footage from a computer's webcam to give the illusion that law enforcement is watching.

The messages often demand that victims buy a preloaded debit card that can be purchased at a local drugstore — and enter the PIN. That way it's impossible for victims to cancel the transaction once it becomes clear that criminals have no intention of unlocking their PC.

The hunt is on to find these gangs. Researchers at Symantec said they had identified 16 ransomware gangs. They tracked one gang that tried to infect more than 500,000 PCs over an 18-day period. But even if researchers can track their Internet addresses, catching and convicting those responsible can be difficult. It requires cooperation among global law enforcement, and such criminals are skilled at destroying evidence.

Charlie Hurel, an independent security researcher based in France, was able to hack into one group's computers to discover just how gullible their victims could be. On one day last month, the criminals' accounting showed that they were able to infect 18,941 computers, 93 percent of all attempts. Of those who received a ransom message that day, 15 percent paid. In most cases, Mr. Hurel said, hackers demanded 100 euros, making their haul for one day's work more than $400,000.

That is significantly more than hackers were making from fake antivirus schemes a few years ago, when so-called "scareware" was at its peak and criminals could make as much as $158,000 in one week.

Scareware dropped significantly last year after a global clampdown by law enforcement and private security researchers. Internecine war between scareware gangs put the final nail in the coffin. As Russian criminal networks started fighting for a smaller share of profits, they tried to take each other out with denial of service attacks.

Now, security researchers are finding that some of the same criminals who closed down scareware operations as recently as a year ago are back deploying ransomware.

"Things went quiet," said Eric Chien, a researcher at Symantec who has been tracking ransomware scams. "Now we are seeing a sudden ramp-up of ransomware using similar methods."

3. GAIL COLLINS
Santorum Strikes Again

4. TOOL KIT
The iPad as a Hand-Held Darkroom

5. For PC Virus Victims, Pay or Else

6. PAUL KRUGMAN
The Forgotten Millions

7. WELL
For Athletes, Risks From Ibuprofen Use

8. ROGER COHEN
Thanks for Not Sharing

9. DAVE BRUBECK | 1920-2012
His Music Gave Jazz New Pop

10. ART REVIEW
The Audience as Art Movement

Go to Complete List » Show My Recommendations

"Hyde Park on Hudson," with Bill Murray and Laura Linney

ALSO IN ARTS »
- Not a member of the Kathryn Bigelow fan club
- Dave Brubeck: 1920-2012

nytimes.com ARTS

Victims become infected in many ways. In most cases, people visit compromised Web sites that download the program to their machines without so much as a click. Criminals have a penchant for infecting pornography sites because it makes their law enforcement threats more credible and because embarrassing people who were looking at pornography makes them more likely to pay. Symantec's researchers say there is also evidence that they are paying advertisers on sex-based sites to feature malicious links that download ransomware onto victims' machines.

"As opposed to fooling you, criminals are now bullying users into paying them by pretending the cops are banging down their doors," said Kevin Haley, Symantec's director of security response.

More recently, researchers at Sophos, a British computer security company, noted that thousands of people were getting ransomware through sites hosted by GoDaddy, the popular Web services company that manages some 50 million domain names and hosts about five million Web sites on its servers.

Sophos said hackers were breaking into GoDaddy users' accounts with stolen passwords and setting up what is known as a subdomain. So instead of, say, www.nameofsite.com, hackers would set up the Web address blog.nameofsite.com, then send e-mails to customers with the link to the subdomain which — because it appeared to come from a trusted source — was more likely to lure clicks.

Scott Gerlach, GoDaddy's director of information security operations, said it appeared the accounts had been compromised because account owners independently clicked on a malicious link or were compromised by a computer virus that stole password credentials. He advised users to enable GoDaddy's two-step authentication option, which sends a second password to users' cellphones every time they try to log in, preventing criminals from cracking their account with one stolen password and alerting users when they try.

One of the scarier things about ransomware is that criminals can use victims' machines however they like. While the computer is locked, the criminals can steal passwords and even get into the victims' online bank accounts.

Security experts warn to never pay the ransom. A number of vendors offer solutions for unlocking machines without paying the ransom, including Symantec, Sophos and F-Secure. The best solution is to visit a local repair shop to wipe the machine clean and reinstall backup files and software.

"This is the new Nigerian e-mail scam," Mr. Haley said. "We'll be talking about this for the next two years."

This article has been revised to reflect the following correction:

Correction: December 7, 2012

An article on Thursday about a new computer threat called ransomware constructed incorrectly a hypothetical Web address incorporating a subdomain. The address would be blog.nameofsite.com, not nameofsite.blog.com. (Subdomain names precede the domain name; they do not follow it.)

A version of this article appeared in print on December 6, 2012, on page B1 of the New York edition with the headline: For PC Virus Victims, Pay or Else.

SAVE E-MAIL SHARE

94 Comments

Readers shared their thoughts on this article.

ALL | READER PICKS | Newest ▼ | Comments Closed

INSIDE NYTIMES.COM

ART & DESIGN »

A Sun's Influence on a Galaxy of Stars

THEATER »

'Golden Boy,' Directed by Bartlett Sher

U.S. »

Two Laws Are Welcomed After Midnight in Seattle

OPINION »

Op-Ed: Going Beyond Carbon Dioxide

A short-term strategy to slow global warming is to reduce emissions of other pollutants.

REAL ESTATE »

Where Sotheby's Scorns to Tread

OPINION »

Townies: The Portrait of a Lady

OPEN

MORE IN TECHNOLOGY (14 O

Memo From Afgha
Ban, Spurred by A
Met With Shrugs

Read More »