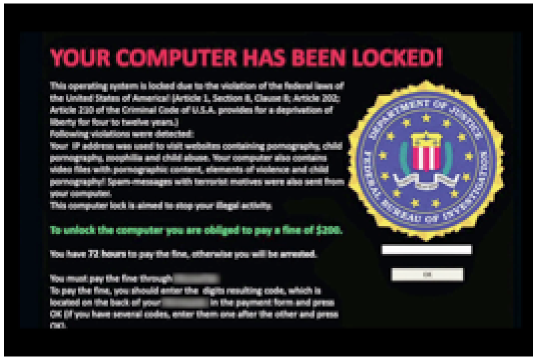
Ransomware: The New ‘Not-Normal’ Online Experience/Threat



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

by Nick Iandolo

In 2014 over *8.8 million* users were affected by a bold new malicious threat to the online web-surfing and e-commerce experience: **ransomware**![1]

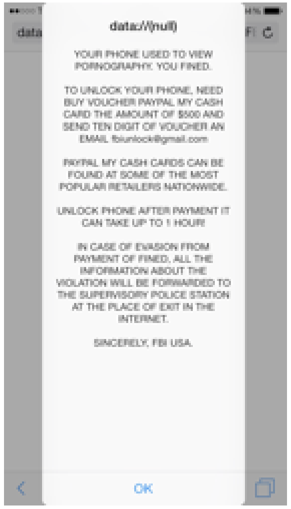
Put simply, this highly-disruptive form of Internet-viral malicious software (*malware* for short), not only infects your computer but holds all of your most precious files (i.e. photos, documents, apps, etc.) completely hostage—via permanently encrypting such files—until the victim is forced to pay a “ransom” to the criminal entity behind the attack for a decryption key to unlock the files. Usually to the tune of *$100 - $300* or more!

This kind of cyber attack can have disastrous consequences to private citizens, small business, or even corporations.

But the threat goes far beyond that.

Threat To The Modern Mobile Lifestyle

Since the early 2000s, people have become wholly dependent on their mobile devices for virtually every aspect of their lives. From banking in the middle of a park, chatting with friends who are thousands of miles away via *Facebook*, to preparing for a 5K run using the latest wearable fitness tracker connected to one’s mobile device, our modern society is becoming inexorably linked to these little internetworked boxes.



data://(null)

YOUR PHONE USED TO VIEW PORNOGRAPHY. YOU FINED.

TO UNLOCK YOUR PHONE, NEED BUY VOUCHER PAYPAL MY CASH CARD THE AMOUNT OF $500 AND SEND TEN DIGIT OF VOUCHER AN EMAIL fbiunlock@gmail.com

PAYPAL MY CASH CARDS CAN BE FOUND AT SOME OF THE MOST POPULAR RETAILERS NATIONWIDE.

UNLOCK PHONE AFTER PAYMENT IT CAN TAKE UP TO 1 HOUR!

IN CASE OF EVASION FROM PAYMENT OF FINED, ALL THE INFORMATION ABOUT THE VIOLATION WILL BE FORWARDED TO THE SUPERVISORY POLICE STATION AT THE PLACE OF EXIT IN THE INTERNET.

SINCERELY, FBI USA.

And there’s where the prime opportunity for hackers to exploit such dependencies come into play.

Ransomware is a virtual gold mine of quick cash extorted from on-the-go people who need to have their smartphones up and running 24/7. People would rather pay $100 in untraceable *Bitcoin* funds than have their busy lives so disrupted.

For example, in 2014 ***Kaspersky Lab*** detected a new type of malicious ransomware code that affects Android devices designated: **Trojan.AndroidOS.Koler.a**.[2]

This nasty bit of business not only affects Android phones such as a *Samsung Galaxy* but also the computers they were synched with, making it virtually impossible to eradicate.

Even Fun, Health, And Safety Is At Risk

This is just the frontal assault on a deeper incursion that threatens all of our connected devices, and our lives in general.

In 2015 *Bromium Labs* reported a list of *Single User* and *MMORPG* games that were directly affected by ransomware.[3] Such games included on that list were:

- *Call of Duty*
- *Minecraft*
- *Assassin's Creed*
- *World of Warcraft*
- *League of Legends*

When countless hours have been spent on playing these immersive games, building extensive profiles, and achieving the highest-levels of gameplay, these files are not so quickly abandoned should an affected game system be held hostage by an unscrupulous hacker.

But there are even more far-reaching concerns involving the real threat of ransomware.

Wired Magazine posted an article in their July 2015 issue[4] demonstrating that through the use of ransomware-like malware, a motorist's car can be hacked and disabled even while in transit posing a huge threat to the safety of the passengers inside.

Other equally troubling concerns involve the next generation of biomechanical devices such as pacemakers or deep-brain implants. Imagine a dystopian science fiction scenario where one's very survival depended on paying protection to a nefarious *black hat racket* in order to keep one's heart pumping or brain working properly.

This is a very real possibility in the coming years as these biomedical devices become "smarter" and wirelessly inter-connected.

New Allies In The Fight Against Ransomware

However, all is not lost as Internet and computer software anti-virus and security companies like *Symantec*, *Norton*, and *Kaspersky Lab* work round-the-clock to not only identify and neutralize these virulent forms of malware but also work in concert with local, national, and international law enforcement agencies to bring these shadowy *dark-web criminals* to justice.

In the meantime, while facing this *new not-normal* online and connected experience/threat, users are encouraged to always back up their data on external drives, keep their anti-virus software up-to-date, and **never open any files from an untrusted source**.

And always check with your doctor to make sure your biomedical device comes with its own built-in firewall!

Sources Cited

[1] http://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

[2] http://www.kaspersky.com/about/news/virus/2014/Koler-police-mobile-ransomware-now-targets-PCs-as-well-as-Android-features-exploit-kit

[3] http://labs.bromium.com/2015/03/12/achievement-locked-new-crypto-ransomware-pwns-video-gamers/

[4] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Meta-description

The threat of ransomware has gone beyond just infecting personal computers. Users must be ever vigilant to protect their mobile devices from being infected and disabled. New concerns for health and safety are also being investigated as the threat of ransomware creeps into every aspect of our lives.

Keywords

ransomware, malware, virus, threat, online, internet, mobile, devices, health, safety, gaming, kaspersky, lab, anti-virus, software, hackers, criminals, biomechanical, dark, web, black, hat, files, game, systems, single, user, mmorpg