10 Weird and Scary Things Ransomware Can Do

PRESENTED BY

StorageCraft.

ChannelPro
IT and Business Insights for SMB Solution Providers
WHITE PAPER

By Contel Bradford

From out of nowhere, it seems, ransomware has emerged as one of the most dangerous security threats today. Although this malicious trend isn't entirely new, the attacks have become alarmingly more sophisticated. Also, the victim count has steadily increased and it looks like the trend is not slowing down.

By now you should be familiar with the ransomware basics. Once installed, the malware blocks access to your files and demands you pay a ransom amount in order to regain access. Unfortunately for the victims, this new wave of attacks goes far beyond the basics. Here are 10 things you may or may not have known ransomware can do:

1. Wears a Clever Disguise

Although ransomware is pretty unique in functionality, it gets around like the malware we've all come to know and loathe. For example, *RAA*, which is written entirely in JavaScript, is distributed in an email attachment pretending to be a legitimate .doc file. In the latest version, the message claims that you owe money to a supplier and must download an invoice to see the balance. If you fall for it, you install both the ransomware and a password-stealing Trojan. A .doc file will usually evade anti-virus scanners.

The latest strain of *DetoxCrypto* malware is purposely trying to disguise itself as reputed security software Malwarebytes—albeit in an amateurish style, as the name of the poser software has typos: "Malwerbyte." So, beware what executables you install.

Unfortunately for the victims, this new wave of [ransomware] attacks goes far beyond the basics.

2. Works on Linux and Macs

As the world's leading operating system, Windows is a No. 1 target. Unix-like competitors have a reputation for offering better out-of-the-box security, but not even the best of them are spared in the ransomware onslaught. *LinuxEncode* gained a reputation as the first to target the Linux platform. It's also one of the easiest to defeat due to its amateur approach to encryption. Then there's *KeRanger*—some believe this is an updated version of LinuxEncode and the first ransomware launched on Mac OS X. KeRanger is distributed via BitTorrent client Transmission, suggesting that illegal downloads do in fact have a price.

3. Talks to You

You've heard of talking mobile apps. Now meet the talking malware. After encrypting the victim's files, the ransomware program known as *Cerber* delivers instructions on how to pay the ransom. The instructions are contained in TXT, HTML, and VBS files. The latter will recite the message in audio. Cerber demands an average ransom of $500 to $800 via anonymity network tunnel TOR. If you don't pay up, the amount doubles within two weeks.

4. Targets Mobile Phones, Tablets, and Smart TVs

Ransomware is primarily a computer-based threat. However, it rears its ugly head on other devices as well. Stealing security headlines in this category is *Fusob*, a Trojan that targets porn viewers by masquerading as an XXX video player. The mobile commerce revolution is in full swing, and the fact that victims can transfer funds in swipe and tap fashion has to be incredibly appealing to ransomware creators. This theory is fueled by a Blue Coat report proclaiming ransomware as the No. 1 one security threat on mobile devices.

The only thing scarier than ransomware on your phone is the kind that invades your home. *Franctic Locker*, or *FLocker*, originally started by targeting Android phones before eventually adopting capabilities that allowed it to attack Android-powdered smart TVs. FLocker locks your TV screen and alleges you've committed a crime—seeming to be a message from a law enforcement agency. The malware then demands $200 be paid in iTunes gift card credits.

5. Performs Full System Encryption

Most of the ransomware threats on our list operate by encrypting your files. Some, however, aim to paralyze you entirely by locking up your whole system. *Petya* was one of the first discovered to have full system encryption capabilities. Overwriting the MBR allows it to encrypt the hard drive, crash the OS, and present the ransomware note. A few months after its initial discovery, Petya returned—but it wasn't alone. The updated version came bundled with a second piece of malware (*Mischa*) that performed the ransomware duties in the event that the initial infection failed to gain the necessary admin privileges.

6. Deletes Your Files One by One

The classic ransomware infection blocks access to your files until you pay up. *Jigsaw* goes one step further. It encrypts your files and incrementally deletes them until you pay the ransom. Clearly the authors were heavily inspired by the horror movie franchise *Saw*. The ransom note is accompanied by an image of Billy, the creepy puppet that makes an appearance in each film, as well as a red digital clock that performs the countdown.

Clearly the [Jigsaw] authors were heavily inspired by the horror movie franchise "Saw."

7. Takes Your Money *and* Deletes Your Files

Some ransomware victims opt to simply pay the ransom to regain access to their mission-critical files as soon as possible. Sadly, giving in to the ransom demands can actually make matters worse. *RanScam*, an aptly named infection that presents itself as ransomware, will delete your files whether you pay the ransom or not. Ironically, this scheming malware is looked down upon by ransomware authors who realize that destroying files is a bad look for the community at large. After all, victims are not going to pay if they believe there's no chance they'll get the files back.

8. Encrypts Unmapped Drives

When ransomware first emerged on the scene, the attacks looked to encrypt files in the default drive before moving on to other mapped drives. However, evolved strains like *CryptoFortress*, *DMA Locker*, and *Locky* emerged. CryptoFortress was the first to show the ability to lock files whether they are mapped to a specific drive or not. This functionality has made it more important than ever for IT administrators to protect shared network folders with strong permissions.

According to some reports, ransomware even affects SQL databases, shutting down entire processes in order to encrypt files. New updates to Cerber have emerged that use a random extension and terminate a database process before attempting encryption.

9. Poses as a Windows Update

In order to slap the cuffs on unsuspecting users, ransomware authors must first gain system access, which means they need a clever disguise. It doesn't get any craftier than posing as something that all users need—critical system updates. *Fantom* targets business users by pretending to be a Windows update complete with a Microsoft copyright and familiar dialogue screen. But once you agree to the terms, the utility you think is updating your system is busy encrypting your files with AES encryption you couldn't crack with a virtual sledgehammer. This one is scary!

10. Encrypts Backup Copies

Next to prevention, a solid backup and disaster recovery plan has proven to be the most effective way to combat ransomware. Malware writers are trying to cripple the best defense mechanism, too. The FBI was the first to send word regarding *SAMAS*. This ransomware strain not only targets the infected system, but all connected systems and resources. Among those resources are backup copies victims can ordinarily rely on to restore their files and avoid paying ransom fees. Needless to say, SAMAS is one of the most dangerous ransomware villains we've seen to date.

Malware seems to grow more advanced by the day, and this extortion-driven threat is the worst possible example. Having an off-site backup is typically the best defense against ransomware. Nevertheless, a little common sense when browsing the internet helps, too.

Learn more about how to prevent ransomware and discourage data kidnappers.