

Keeping up with the changing ransomware landscape - blueAPACHE

Canonical: <https://www.blueapache.com/blog/keeping-up-with-the-changing-ransomware-landscape>

Details:

January 27, 2017

Ransomware is big business. The FBI estimated that in 2016 alone cybercriminals extorted nearly \$US1 billion from ransomware payoffs. An unsurprising fact considering more than 70% of businesses impacted by ransomware have admitted to paying ransom so as to regain access to business critical data and systems.

Ransomware is just another form of blackmail. But today, in its digital manifestation, it is more deadly, pervasive and easy to execute. From teenagers to organised hacker groups, ransomware is a very attractive concept for many online scammers. Not only is it notoriously difficult to track down perpetrators, but with disparate legal systems around the world, it is not easy to bring them to justice even when they are caught.

In its characteristic form, ransomware is an extortion technique where data on computers and other devices is encrypted and held for ransom until a specified amount of money, usually in the form of Bitcoins, is paid. While financial gain remains a major inducement for such crimes, there are no real boundaries to the inventiveness of cybercriminals, their motivations or even choice of ransom.

Here is a look at three new and unusual forms of ransomware that deviate from the typical formula.

Popcorn Time

A ransomware that unlocks your files for free if you infect others.

This malware, discovered by researchers at MalwareHunterTeam, gives victims a choice of ransom. They can choose to pay a ransom of 1.0 Bitcoin; the “fast and easy” way according to the ransom note, or they can choose the “nasty way” which involves sending the malicious link to two or more people.

To make this possible, the ransom note contains a URL pointing to a file located on the Popcorn Time's TOR server. If at least two people end up installing the Popcorn Time malware and paying the ransom, then the first victim's files are unlocked free of charge.

If the ransom is not received within seven days the decryption key, stored on a remote server owned by Popcorn Time's developers, is permanently deleted making it near impossible to retrieve the encrypted files.

It is unknown exactly how many devices have been infected with Popcorn Time but the spread appears to be worldwide and not limited to one particular region.

Koolova

A ransomware that unlocks your files for free if you read up on cybersecurity.

In this first of its kind approach, the Koolova ransomware does not ask for any Bitcoin payment. Instead, it will restore encrypted files for free if the victims educate themselves on ransomware by reading two articles.

Koolova encrypts a victim's files and displays a ransom note asking the user to read two blogposts – a Google security blog titled Stay safe while browsing and a BleepingComputer article on Jigsaw

ransomware .

Failure to read both articles before the countdown reaches zero results in the encrypted files being deleted. However, once the user reads both posts, the 'Decrypt My Files' button becomes available and clicking on it will retrieve the decryption key.

KillDisk

A ransomware that will not decrypt files even after ransom is paid.

A new variant of KillDisk ransomware has been found to encrypt Linux machines making them unbootable and demands 222 Bitcoins as ransom; possibly the largest ransom demand till date.

According to researchers, the files are encrypted using Triple-DES applied to 4096-byte file blocks, and each file on the computer is encrypted by a different set of 64-bit encryption keys.

The Linux variant differs from other ransomware in that it does not store the decryption key anywhere on disk or online. This means that regardless of the ransom being paid, there is no way to recover files once they have been encrypted.

Ransomware like KillDisk and Ranscam serve as reminders of the unpredictable nature of ransomware, making prevention the best form of defence against them.

The Takeaway

The threat of ransomware is going to remain, and quite likely grow, in the near future. Given its complexity and constant evolution, there is no 'silver bullet' security solution that can protect your organisation from all forms of attacks. However, organisations and individuals can implement measures to defend themselves and prevent these attacks before they occur.

Staff Education – It only takes one bad decision by a user to put your organisation at the mercy of a ransomware attack. When end users are aware of the type of threats to look out for, they can be your first, and most effective, layer of defence against ransomware.

Data backup – Nothing can help take the edge off a ransomware attack than the ability to instantly restore data from secure business continuity backups. The importance of maintaining regular backup routines and ensuring that the backups are secure cannot be overstated. The best backup strategies always include regular testing to verify data integrity and usability in case of emergency.

Multi-layered defences – Endpoint security alone cannot offer total protection against the constantly changing variants of ransomwares. Additional defences such as firewalls and policy restrictions can better secure your environment. Always ensure that your systems are running the latest version of software, including operating systems and antivirus software with up to date malware definitions.

For more information on how to better secure your business, contact our security team .

News

How much money did the FBI estimate cybercriminals extorted from ransomware payoffs in 2016?

The FBI estimated that in 2016 alone cybercriminals extorted nearly \$US1 billion from ransomware payoffs.

What percentage of businesses impacted by ransomware admitted to paying the ransom?

more than 70% of businesses impacted by ransomware have admitted to paying ransom so as to regain access to business critical data and systems.

What is Popcorn Time ransomware and what unusual ransom options does it offer?

Popcorn Time is a ransomware discovered by researchers at MalwareHunterTeam that gives victims a choice of ransom: they can pay 1.0 Bitcoin (the 'fast and easy' way) or take the 'nasty way,' which involves sending the malicious link to two or more people. If at least two people install the malware and pay the ransom, the first victim's files are unlocked free of charge. If the ransom is not received within seven days, the decryption key is permanently deleted, making it near impossible to retrieve the encrypted files.

How does Koolova ransomware differ from typical ransomware?

Koolova ransomware does not ask for any Bitcoin payment. Instead, it restores encrypted files for free if victims educate themselves on ransomware by reading two articles—a Google security blog titled 'Stay safe while browsing' and a BleepingComputer article on Jigsaw ransomware. Failure to read both articles before the countdown reaches zero results in the encrypted files being deleted; once both are read, a 'Decrypt My Files' button becomes available to retrieve the decryption key.

What makes the KillDisk ransomware variant especially dangerous?

A new variant of KillDisk ransomware encrypts Linux machines, making them unbootable, and demands 222 Bitcoins as ransom—possibly the largest ransom demand to date. The files are encrypted using Triple-DES applied to 4096-byte file blocks, with each file encrypted by a different set of 64-bit encryption keys. Unlike other ransomware, this Linux variant does not store the decryption key anywhere on disk or online, meaning files cannot be recovered even if the ransom is paid.

What three measures do you recommend organizations implement to defend against ransomware?

We recommend: (1) Staff Education, so end users can recognize threats and act as the first layer of defence; (2) Data backup, maintaining regular, secure backup routines with regular testing to verify data integrity and usability; and (3) Multi-layered defences, including firewalls, policy restrictions, and keeping systems and antivirus software up to date, since endpoint security alone cannot offer total protection against constantly changing ransomware variants.

How does Endpoint Detection and Response (EDR) help defend against ransomware, according to you?

Our MDR material illustrates how endpoint detection and response can detect suspicious activity and support investigation and containment, including stopping a payload before encryption in the illustrated scenario. Detection and prevention depend on coverage, configuration and the attack; EDR does not guarantee that every ransomware payload is stopped.

What is your emPOWER MDR service and what does it provide?

Our emPOWER Managed Detection and Response (MDR) service combines EDR with continuous monitoring, advanced analytics, and threat intelligence to provide 24/7 protection against ransomware

and other threats, including rapid triage, containment, and remediation capabilities designed to minimize the impact of successful attacks.

Why is human risk management important in defending against ransomware?

The article highlights staff education because ransomware can spread through malicious attachments and links. It recommends combining awareness with secure, tested backups and multiple technical defences. This supports addressing human risk without assigning an unsupported percentage to all breaches.

How can someone get more information about securing their business against ransomware from you?

The blog post advises contacting our security team via the site's contact page for more information on how to better secure a business against ransomware.