TERREF.COM
Computer Consulting Inc.
631-586-5811

What is ransomware?

Type:Trojan Infection Length:Varies - Systems Affected: Windows / Mac

How Ransomware Works

There are several ways that ransomware can infect your computer or your company's network. Sometimes the attack can stem from visiting an infected website. Occasionally a hacker will use a brute force attack to break in. But the most common means is through a phishing email.

A phishing email usually includes a link that will allow the malware that will carry out the ransomware to enter your system. Sometimes it will include a request for login credentials or other private information. If you provide those credentials, then the hacker can attack your computer or your network directly.

Computer Malware Attack
GETTY
However the malware gets into your system, it follows a series of steps. First it finds somewhere on your hard disk to hide, sometimes it mimics a system file and sometimes it installs itself into the master boot record, but either way removing it is difficult.

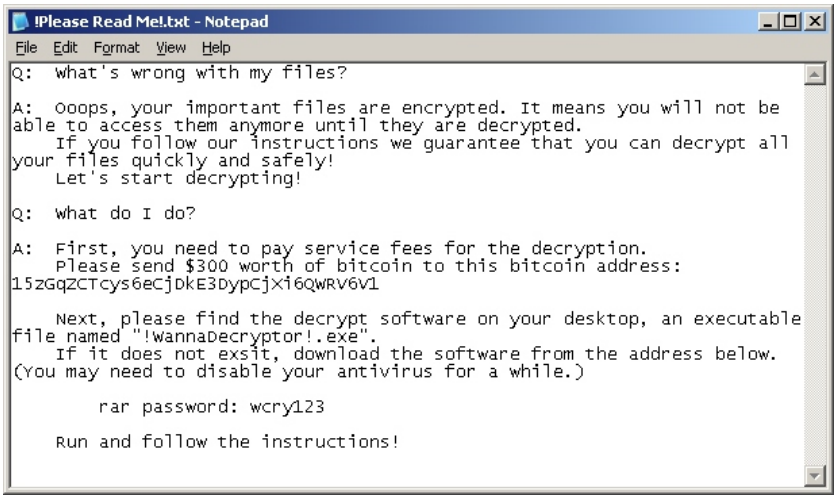
The second step is to locate any backups that are visible to your computer. These may be on an attached external hard disk or on a networked hard disk. When it finds them they will either be erased or encrypted.

The third step is to encrypt the data on your hard disk, although it may allow some system files to survive so that you can use your computer to pay the ransom.

Finally, the ransomware will announce itself and display instructions as to how the ransom should be paid. Normally you're given an amount in Bitcoins and given a deadline, after which the decryption key and instructions will be provided.

Ransom Screen

It also drops a file named !Please Read Me!.txt which contains the ransom note.



Who is impacted?

A number of organizations globally have been affected, the majority of which are in Europe.

Is this a targeted attack?
No, this is not believed to be a targeted attack at this time. Ransomware campaigns are typically indiscriminate.

Why is it causing so many problems for organizations?

WannaCry has the ability to spread itself within corporate networks, without user interaction, by exploiting a known vulnerability in Microsoft Windows. Computers which do not have the latest Windows security updates applied are at risk of infection.

Can I recover the encrypted files?

Decryption is not available at this time but Terref.com is investigating.
Terref.com does not recommend paying the ransom.
Encrypted files should be restored from back-ups where possible.

What are best practices for protecting against ransomware?

New ransomware variants appear on a regular basis. Always keep your Eset software up to date to protect yourself against them.
Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attackers.
Email is one of the main infection methods. Be wary of unexpected emails especially if they contain links and/or attachments.
Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.
Backing up important data is the single most effective way of combating ransomware infection. Attackers have leverage over their victims by encrypting valuable files and leaving the minaccessible. If the victim has backup copies, they can restore their files once the infection has been cleaned up. However organizations should ensure that back-ups are appropriately protected or stored off-line so that attackers can't delete them.
Using Terref.com cloud services could help mitigate ransomware infection, since Terref.com retain previous versions of files, allowing you to "roll back" to the unencrypted form.

The Smart and Easy Way to Protect Your Data

You can either tear out your hair when disaster strikes, or you can prepare for it.
Terref.com Online backup services are one of the best ways to protect yourself against loss of precious computer data, whether it's a result of a crashed hard drive or an unintentional ransomware attack.

Hard drive crashes and editing mishaps aren't the only things online backup can protect you from: There are also more traditional disasters such as fires, floods, and earthquakes, which can spell the end of your digital media and documents. Even if you're among the very few of us who diligently perform backups at regular intervals, those calamities can still result in data loss if you didn't store backups off-site. That's a good reason why an Terref.com online backup service may be the best way to protect your irreplaceable digital goods.

Call Now For Terref.com online Back Service and E-Set Endpoint Anti-virus Security 631-586-5811