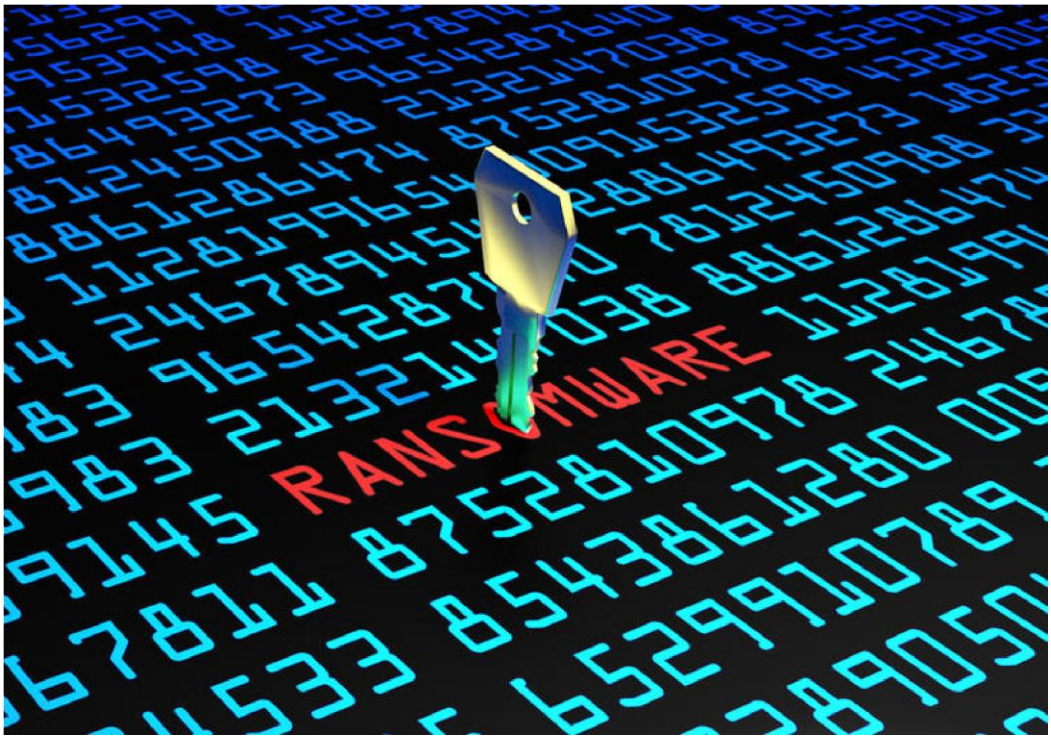


Ransomware: The smart person's guide (5 Mins. Read).

www.techrepublic.com

This guide covers the history of ransomware, the systems being targeted in ransomware attacks, and what you can do to avoid paying a ransom in the event of an attack.

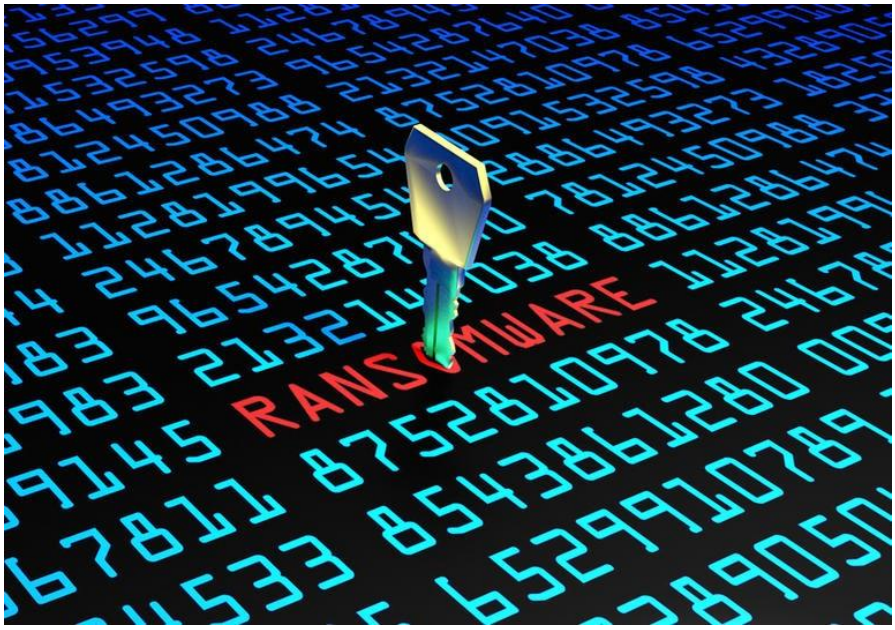
In the past, security threats often involved scraping information from systems that could be used for other crimes such as identity theft.
Now, criminal organizations have proceeded to directly demanding stream type money from victims by holding their devices—and data—hostage.

This type of attack in which data is encrypted and victims are prompted to pay for the key, called ransomware, has grown rapidly since 2013.
TechRepublic's smart person's guide about ransomware is a quick introduction to this security threat, as well as a "living" guide that will be updated periodically as new exploits and defenses are developed.

Executive summary

- What is it? Ransomware is malware. The hackers demand payment, often via Bitcoin or prepaid credit card, from victims in order to regain access to an infected device and the data stored on it.
- Why does it matter? Because of the ease of deploying ransomware, criminal organizations are increasingly relying on such attacks to generate profits.
- Who does this affect? While home users have traditionally been the targets, healthcare and the public sector have been targeted with increasing frequency. Enterprises are more likely to have deep pockets from which to extract a ransom.
- When is this happening? Ransomware has been an active and ongoing threat since September 2013.
- How do I protect myself from a ransomware? attack? A variety of tools developed in collaboration with law enforcement and security firms are available to decrypt your computer.

This Guide is provided by BTPS – www.btpsonline.com
Published by TechRepublic. www.techrepublic.com



What is ransomware?

Ransomware is a subclass of malware that is characterized by holding device control—and therefore locally stored data—for a ransom, which is typically paid using virtual currencies such as Bitcoin, though often premium SMS messaging and prepaid credit cards are alternative options. Sophisticated ransomware attacks employ disk or file-level encryption, making it impossible to recover files without paying the ransom demanded by the hackers.

Historically, ransomware has invoked the image of law enforcement to coerce victims into paying—displaying warnings such as the FBI logo and a message indicating that illegal file sharing has been detected. More recently, the authors of ransomware payloads clearly indicate that a device has simply been hacked.

Ransomware attacks are typically propagated through file-sharing networks, but have also been distributed as part of a malvertising campaign on the Zedo ad network, as well as through phishing emails that disguise the payload as maliciously crafted images or as executables attached to emails. WannaCry, perhaps the most well-known single ransomware attack, uses a flaw in Microsoft's SMB protocol, leaving any unpatched, internet-connected computer vulnerable to attack.

Why does ransomware matter?

For criminal organizations, the use of ransomware provides a very straight line from development to profit, as the comparatively manual labor of identity theft requires more resources. As such, the burgeoning growth of ransomware can be attributed to the ease of deployment, and a high rate of return relative to the amount of effort put forth.

Many ransomware attacks leverage known vulnerabilities, so original research is not required of attackers. The WannaCry attack is a special case—it leverages two exploits named EternalBlue and DoublePulsar. These exploits were discovered and used by the NSA, and the existence of these vulnerabilities was disclosed by The Shadow Brokers, a group attempting to sell access to a cache of vulnerabilities and hacking tools developed by the US government.

For IT professionals, the risk of ransomware extends beyond desktops and notebook workstations, but has historically included smartphones and other connected computing devices, such as Synology NAS products and Android TV devices. While home users were traditionally the targets of ransomware, business networks have been increasingly targeted by criminals. Additionally, servers have become high-profile targets for ransomware attackers, as unpatched, internet-connected systems are easy targets.

Who does ransomware affect?

According to NTT Security's 2017 Global Threat Intelligence Report, 28% of ransomware attacks targeted businesses and professional service firms over the last year. 19% of attacks targeted government and public sector employees, with healthcare service providers accounting for 15% of ransomware attacks. Enterprises are particularly appealing targets for targeted attacks. While larger organizations have deeper pockets to pick from, they are more likely to have robust IT operations with recent backups to mitigate any damage and avoid paying the ransom.

Ransomware attacks are generally quite successful for criminal organizations, as victims often pay the ransom. Specifically targeted attacks may result in increasingly higher ransom demands, as attackers become more brazen in their attempts to extort money from victims.

However, "false" ransomware attacks—in which attackers demand a ransom, though files are deleted whether users pay or not—have also recently become widespread. Perhaps the most brazen (though unsuccessful) of these is a KillDisk variant that demands a $247,000 ransom, though the encryption key is not stored locally or remotely, making it impossible for files to be unlocked if anyone were to pay the ransom.

When is ransomware happening?

While the first rudimentary ransomware attack dates back to 1989, the first widespread encrypting ransomware attack was CryptoLocker, which was deployed in September 2013. Originally, victims of CryptoLocker were held to a strict deadline to recover their files, though the authors later created a web service that can decrypt systems for which the deadline has passed at the hefty price of 10 BTC (as of June 17, 2017, the USD equivalent of 10 Bitcoin, or BTC, is approximately $25,339).

While the original CryptoLocker authors are thought to have made about $3 million USD, imitators using the CryptoLocker name have appeared with increasing frequency. The FBI's Internet Crime Complaint Center estimates that between April 2014 and June 2015, victims of ransomware paid over $18 million USD to restore access to their devices.

The WannaCry attack, which started on May 12, 2017, was stopped three days later when a security researcher identified and registered a domain name used for command and control of the payload. The National Cyber Security Centre, a division of GCHQ, identified North Korea as the origin of the WannaCry attack.

How do I protect myself from a ransomware attack?

Ransomware is often spread in file-sharing networks or on websites that purport to provide direct downloads. Other traditional attack vectors have also been used, such as email attachments or malicious links. There are ways to protect against a potential infection. For enterprise workstation deployments, using Group Policy to prevent executing unknown programs is an effective security measure for ransomware and other types of malware.

Ensuring that all devices on your network receive regular and prompt security patches is the biggest defense against any hacking attempt, including ransomware. Additionally, a sane device lifecycle is also important for network security—outdated systems running unsupported operating systems such as Windows XP have no place on an internet-connected network. Despite this, due to the severity of WannaCry, Microsoft released a patch for Windows XP.

For those who have been infected, the No More Ransom project—a collaboration between Europol, the Dutch National Police, Kaspersky Lab, and Intel Security—provides decryption tools for many widespread ransomware types.