Ransomware

Osamah Alabry

Danny Henriquez

Christopher Leotis

Joshua Link

Alec Zec

Professor Regan

GBA 327

Business Information System and Analytics

Saint Leo University

3, December 2015

Ransomware is a nasty computer virus that infiltrates your computer after you visit suspicious websites, and arrives through different means such as, “drive-by downloads, stealth downloads or through a user clicking on an infected advert” (Norton 2015). It has also been acquired from distribution through email. Ransomware first emerged in “Russia and Eastern Europe in 2009” (Norton 2015), after which it has spread to many other countries including Western Europe, the US. This spread has caused increased infestation rates and a great deal of frustration for many computer users. Ransomware works by using malware to disable a computer until the user pays a ransom to restore access. Cybercriminals often use tricks, such as displaying phony messages clamming to be from law enforcement, such as the FBI to convince victims to pay up.

Furthermore, the growing global cyberwar with threats on malware, breaches and distributed denial of service attacks. Because messages are evolving over time and the “global cyberwar with treats on malware, breaches and distributed denial of service attacks” (Gewirtz, 2014), it has become easier for cybercriminals to use different methods to defraud users. Early variants of Ransomware used a locked screen containing “pornographic images to shame users into paying the fine, and are now using law enforcement logos” (Norton 2015). Their techniques have become more sophisticated with code built into the programs, to tailor messages to the right language and local law enforcement logo. Even if a person does pay the ransom, the cybercriminals often do not restore functionality. An example of how devastating Ransomware can be, is the case of the “Durham Police Department in New Hampshire, which was attacked by CryptoWall” (NewCombe, 2014).

Now users can make their computers safer by installing comprehensive security software, such as Norton Securities and Symantec Connect. These security software will help protect

against cybercriminals, who will take advantage of vulnerabilities found in user's software to install their malware. By keeping your operating systems and software up-to-date you can also increase your computer's safety. It's safer to regularly back up any files stored on your computer, just to in case you do acquire malware, so after treats like ransomware are removed from your device, your files can be restored. Just like on computers, you also must be cautious on mobile devices. Try to avoid "downloading apps from unfamiliar sites and only install apps from trusted sources" (Power, 2015). Back up everything on your mobile, which I know ITunes does this automatically for users once you plug your phone into your computer. This precaution ensures that if a mobile device does become infected, you can always restore everything from the backup. It's also a good idea to install a "security app, such as Norton Mobile Security" (Power, 2015), these actions will help protect your devices.

To conclude, people use electronic devices on a daily basis. This leaves their computers, smartphones and tablets valuable to treats like Ransomware. Its ever growing popularity leads to cybercriminals have multiple opportunities to invade our computers, smartphones, tablets and other devices. But, we do have one reliable way to restore functionality to our devices is to remove the malware which allowed ransomware to infiltrate the user's computer in the first place.

Works Cited

Gewirtz, David, Journal of Counterterrorism & Homeland Security International. Summer2014, Vol. 20 Issue 2, p8-9. 2p.

Newcombe, Tod, Government Technology, Oct2014, Vol. 27 Issue 8, p46-48, 3p, 1 Color Photograph Color Photograph; found on p46 part. 1 (Incomplete)

Norton. (2015). Retrieved from Ransomeware on the rise: Norton tips on how to prevent getting infected: http://us.norton.com/ransomware/article

Power, J. -P. (2015, Feburary 09). *Symantec Connect*. Retrieved from Ransomware: How to stay safe: http://www.symantec.com/connect/blogs/ransomware-how-stay-safe