Ransomware

A history and the current status

About the Speaker

20 books (Including 3 on forensics, 5 on computer security, 1 on cryptology)

40 industry certifications

Member and Diplomat of the American College of Forensic Examiners

Chair of the cyber forensics board for the American College of forensic Examiners

2 Masters degrees

7 Computer science related patents

Over 25 years experience, over 15 years teaching/training, over 12 years of litigation support

Helped create CompTIA Security+, Linux+, Server+. Helped revise CEH v8. Created OSForensics certification.

Frequent consultant/expert witness

www.chuckeasttom.com

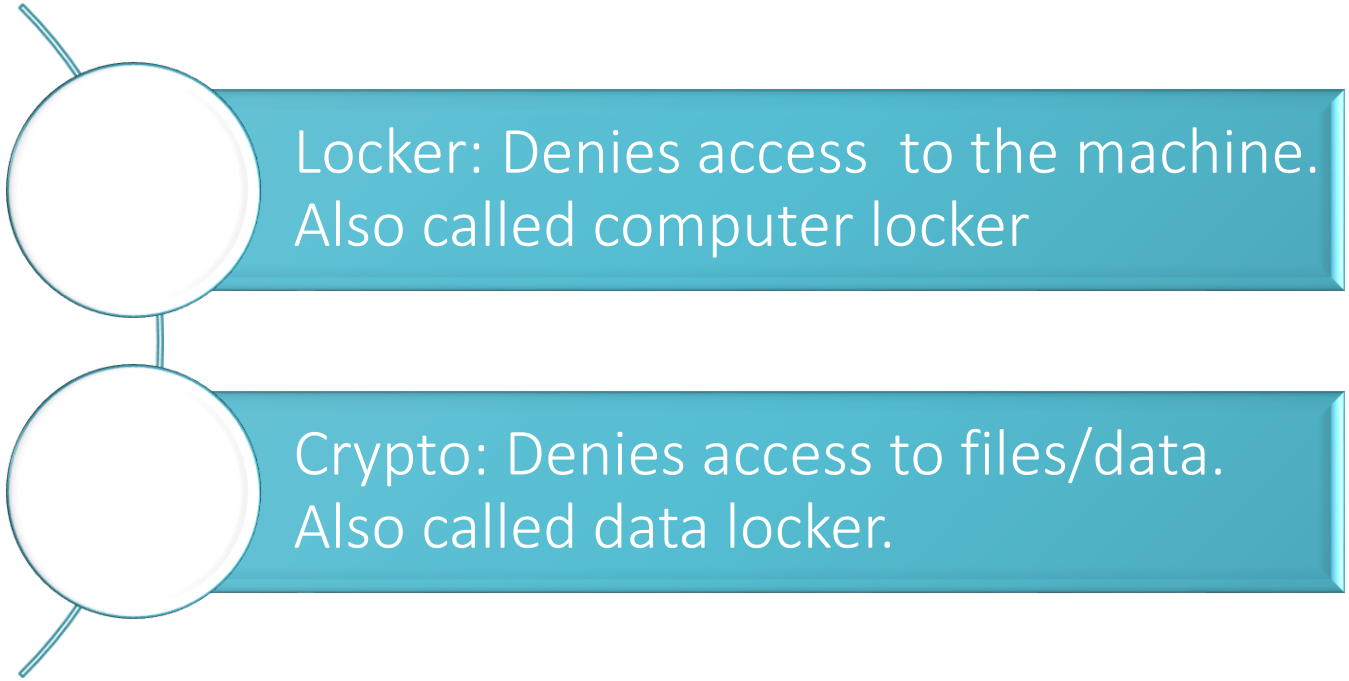
chuck@chuckeasttom.com

Ransomware

Works as a worm then either disables system services or encrypts user files. Then one demands a Ransom to release those files/service.

Ransomware

According to Symantec (2015), ransomware comes in two forms:.



Ransomware

- The first known ransomware was the 1989 PC Cyborg Trojan, which only encrypted filenames with a weak symmetric cipher. The notion of using public key cryptography for these attacks was introduced by Young and Yung in 1996
- In 2013 McAfee claimed they had collected over a quarter million examples of ransomware in the first 3 months of the year.
- In 2016 “Almost two-fifths of businesses in the U.S., Canada, the U.K., and Germany have been hit in the last year by a ransomware attack, according to a survey by security firm Malwarebytes.” – Fortune Magazine August 3, 2016

Ransomware – It is a problem for Africa as well

- Over the last 12 months, there has been a 16% increase in ransomare attacks, a Data Breach Investigation Report by Verizon, has revealed - http://www.itnewsafrica.com/2016/05/ransomware-african-businesses-continue-to-be-at-high-risk/

- Ransomware is increasingly becoming a problem in SA and local companies are not reporting incidents for fear of reputational damage, says a security company. “Statistics in South Africa remain vague as organizations are reluctant to reveal the extent to which they have been targeted by ransomware," security firm Panda Security said in a statement to Fin24.

Ransomware

“The modern-day ransomware has evolved considerably since its origins 26 years ago with the appearance of the AIDS Trojan. The AIDS Trojan was released into the unsuspecting world through snail mail using 5¼” floppy disks in 1989. Despite the public being unprepared for this new type of threat all those years ago, the AIDSTrojan was ultimately unsuccessful due to a number of factors. Back then, few people used personal computers, the World Wide Web was just an idea, and the internet was mostly used by experts in the field of science and technology. The availability and strength of encryption technology was also somewhat limited at the time. Along with this, international payments were harder to process than they are today.”

-Savage, K., Coogan, P., Lau, H. (2015). The Evolution of Ransomware. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Reveton (2012)

This was a Trojan that was based on the Citadel Trojan which was in turn based on the Zeus Trojan. This was interesting because it spread by popping up a window claiming to be from some law enforcement agency. It would claim you had done something illegal and the user needs to pay a fine. It would display the users IP address, and in some cases a brief clip from the victims web cam.

Cryptolocker (2013)

One of the most widely known examples of ransomeware is the infamous CryptoLocker. It was first discovered in 2013. CryptoLocker utilized asymmetric encryption to lock the user's files. Several varieties of CryptoLocker have been detected.

.

CryptoWall (2014/2015)

CryptoWall is a variant of CryptoLocker first found in August of 2014. It looked and behaved much like CryptoLocker. In addition to encrypting sensitive files it would communicate with a command and control server, and even take a screenshot of the infected machine. By March of 2015 a variation of CryptoWall had been discovered which is bundled with the spyware TSPY_FAREIT.YOI and actually steals credentials from the infected system, in addition to holding files for ransom. It spread by both malicious file attachments to email messages and via the Gameover Zeus botnet.

Also known as: CryptoLocker.F and TorrentLock

CTB-Locker (2015)

CTB-Locker is downloaded and installed on a system by a separate trojan-downloader program. It is spread as an attachment to spam e-mail. That attachment is often a zip file. Sometimes it was a zip file inside a zip file. The ultimate file had an .SCR extension so users would think it was a screen saver, when it was in fact the Trojan-Downloader:W32/Dalexis. That Trojan would then go to a list of compromised sites and download an encrypted copy of CTP-Locker, decrypt and run it. It encrypted files and appended a randomly generated 7-character extension, then displayed a ransom notice to the user.

Hitler Ransomware (2016)

Displays a lock screen featuring Hitler, together with a message that warns users that files have been encrypted. The ransomware requests the payment of only 25 euros, in the form of a Vodafone cash card. The lock screen features a misspelling "Ransonware." First spotted by the malware analyst Jakub Kroustek from AVG. The malware will remove the extension for all of the files under various directories, display a lock screen, and then show a one hour countdown. After that hour it will crash the victim's computer, and on reboot, delete all of the files under the %UserProfile% of the victim

Hidden Tear Ransomware (2016)

Michael Gillespie found this malware. It impersonates a PokemonGo application for Windows and targets Arabic users.

It scans the drive for sensitive files (anything document, spreadsheet, image, or database) and encryptes it with AES, appending the .locked extension to the file. The victim is then instructed to email me.blackhat20152015@mt2015.com to get payment instructions. It also adds a backdoor Windows account, spreading the executable to other drives, and creating network shares.

It then hides this account from being seen on the Windows login screen by configuring the following Windows registry key:KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList "Hack3r" = 0.

It also addes a network share on the infected computer. It is not yet known what this share is for.

http://www.bleepingcomputer.com/news/security/pokemongo-ransomware-installs-backdoor-accounts-and-spreads-to-other-drives/

%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\[random].exe PokemonGo.exe

Hidden Tear Ransomware (2016)

This is the executable %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\[random].exe
PokemonGo.exe

Thermostats held ransom (2016)

On August 7, 2016, the first ever ransomware for smart thermostats was reported (http://motherboard.vice.com/read/internet-of-things-ransomware-smart-thermostat)

In this case, fortunately, this was not ransomware found in the wild, but rather the creation of two security researchers, designed to illustrate a flaw in smart home technology. They demonstrated their proof of concept ad this years Defcon conference in Las Vegas.

ransomware-as-a-service

Cerber, a crypto ransomware tool has hit victims in Korea, US, China, Taiwan, and other countries.

"It is a model that allows individuals with very little technical know-how to buy readymade ransomware kits for use against targets of their choice. Often, the developers of the malware allow the so-called affiliates to even specify the ransom amount they want from victims."
http://www.darkreading.com/attacks-breaches/cerber-ransomware-could-net-$2-million-its-first-year-/d/d-id/1326644?

McAffee has reported TOX Ransomware as a service as early as 2015. The site is free to use, but they keep 20% of all ransom that is collected.

Remediation - Cisco

- Improve network hygiene, by monitoring the network; deploying patches and upgrades on time; segmenting the network; implementing defenses at the edge, including email and web security, Next-Generation Firewalls and Next-Generation IPS.
- Integrate defenses, by leveraging an architectural approach to security versus deploying niche products. Measure time to detection, insist on fastest time available to uncover threats then mitigate against them immediately.
- Make metrics part of organizational security policy going forward. Protect your users everywhere they are and wherever they work, not just the systems they interact with and when they are on the corporate network.
- Back up critical data, and routinely test their effectiveness while confirming that back-ups are not susceptible to compromise.

Source: http://www.biztechafrica.com/article/cisco-report-predicts-next-generation-ransomware/11584/#.V7NQ4qK-HEQ

Resources

No More Ransom portal
http://allafrica.com/stories/201607280983.html

.