Malware Behavior & Implementation Strategies:

Forms of Malware Attacks & Their Effects

Andrew L. Ramirez

East Carolina University

Prepared for Professor Ping Li

Forms of Malware & Their Effects

The fight against the latest malware on both client and server side attacks hasn't ever been as crucial as it is today. Nowadays, the malware we encounter and are actively seeing in our networks and computers are becoming more and more sophisticated and are adapting to the counter measures that are being taken against them. Malware comes in many forms that all affect systems differently. In recent events, IBM Security recently warned banks and their commercial customers that hackers are using a variant of Dyre, christened "The Dyre Wolf." To attack online banking systems (Kitten, 2015). This particular form of malware targets banking institutions but more specifically their back-end systems and online-banking platforms.

How it accomplishes this is the Dyre variant is programmed to monitor hundreds of online banking sites, so it's able to launch a convincing spoofed page when a user tries to log into their account and online banking system. The victim is greeted with a page that is supposedly experiencing issues and provides a number which says the victim should call to receive further assistance. Once the victim calls they are tricked into revealing their confidential information which includes login information and security questions; by doing so they allow wire transfers to take place. According to John Kuhn, IBM senior threat researcher, "We have seen over 200 banks and over 500 URLs from those banks listed in the Dyre malware code. These are the banks and the URLs that it is tracking. So, we know the attackers are aware of these banking websites and how they run, they are very aware of changes that banks put in place to prevent Dyre infections, and they are spending a lot of time researching these sites to know how they work and how wire transfers are conducted."(Kitten, 2015). To date, IBM is not aware of any institution or business that has recovered stolen funds or stopped fraudulently wires that were linked to a Dyre Wolf attack.

Dyre is one example of a form of malware that is delivered via phishing attacks but there are plenty of other forms of malware that cause equal havoc to businesses and countries around the world. In recent years, there has been a form of malware that has cost users and businesses billions of dollars per year. This kind of malware is called, Ransomware. Ransomware can reach systems from desktops to companies to hospitals and just about anything that is connected to the Internet. How this form of malicious code works is very similar how Dyre works, it can be in a form of a phishing scheme for example, the end user receives an email that appears to be from their boss or the end user opens a browser window and directs the user to a website that seems legitimate and that is where the infection begins. Figure 1 below illustrates the flow or process that ransomware takes.

Figure 1 (Carbon Black)

Unlike Malware that likes to hide in different directories and change its extension and mask itself as a legitimate process; ransomware makes its presence known to the end user or victim but only

when it has completed everything it was set out to do. As the user activates the malware and it infiltrates their computer and or network the ransomware runs as an executable or at least attempts to. It then spawns child processes, including vssadmin.exe which is a shadow copy and it deletes existing shadows on the victim's machine and the malware creates new entries to hide in. The code then creates a powershell executable to propagate copies of itself throughout the filesystem, in this step the executable also searches the filesystem for files of specific extensions and begins to encrypt those files. The powershell executable child process creates three copies of the originating malware binary. First in the AppData directory, next in the Start directory, and lastly in the root C:\ directory. After encrypting the victim's files, the malware sends the encryption key and other host-specific information back to the command-and-control server where the attacker gathers all the information that has been sent (Johnson, 2016). The final step in the phase is where the ransomware note is delivered to the unsuspecting victim and this is usually when people realize what has transpired; they find they can't access any of their files on their computer and are now being told to pay the ransom or risk losing all their data.

As troubling as it may seem to have your personal computer become infected with this horrible malware it hardly compares to when an entire network is compromised and all business/services must be put on hold for an undetermined amount of time and that's exactly what happened with the San Francisco's Municipal Railway (Muni). Per Stephen Hilt and William Sanchez, IT security researchers at Trend Micro, the attackers deployed the HDDCryptor malware; this malware differs from others seen because HDDCryptor not only targets resources in network shares such as drives, folders, files, printers, and serial ports via Server Message Block (SMB), but it also locks the drive. Such a damaging routine makes this particular ransomware a very serious and credible threat not only to home users but also to

enterprises (Hilt & Sanchez, 2016). The attackers demanded 100 bitcoins (around $73,000) for the decryption key. The San Francisco Municipal Transport Agency (SFMTA) confirmed that several payment systems were taken offline. They reported, around 900 computers seem to have been infected, including office desktops, CAD workstations, email and print servers, laptops, payroll systems, SQL databases, lost & found property terminals and station kiosk PCs. Muni also reported they were forced to open several fare gates on its system, effectively allowing many people to ride for free. The company estimated that it will have lost $50,000 in fares during the weekend in which its systems were down (Renaud & Tankard, 2016).

The healthcare industry is the number one most hit industry by ransomware and a lot of hospitals aren't adequately taking the necessary steps to protect themselves and their patients from being another victim to these kinds of attacks. A Presbyterian hospital in Hollywood became a victim to ransomware and it had the entire hospital and board of directors desperately looking for help as the cybercriminals asked for $3.4 million dollars as payment but the demand was later reduced to $17,000. (Kelpsas & Nelson, 2016). There have been reports of other big hospitals also being hit like MedStar Health, a Washington, DC-based hospital chain. The hospital chain had to turn patients away because important medical records were out of reach for the staff. The attackers in this case asked for 45 bitcoins which roughly translates to $19,000 US dollars – in exchange for the decryption key that would allow the hospital to open their documents and update patient information which is what they could not do (Cox, 2016). According to a cybersecurity firm, NTT group says, "A likely reason we are seeing so many attacks on hospitals is that their Chief Information Officer has designed a flawed disaster recovery plan (DRP) and are not equipped to deal with these kinds of attacks." (Kelpsas & Nelson, 2016).

Attacks like the San Francisco Municipal Railway and Hollywood Presbyterian Hospital experienced are becoming more frequent and they are as unexpected and dangerous as one could imagine, a recent Malwarebytes-sponsored global survey of IT executives demonstrates the scale of the business threat. Thirty-nine percent of the organizations surveyed had been impacted by a ransomware attack during the previous 12 months. Across the various industries surveyed, ransomware attacks were most common in the healthcare and financial services-related industries, including banking and insurance. The rate of ransomware attacks in the US is escalating. The FBI received complaints for nearly 2,500 ransomware attacks in 2015, which cost victims $24 million (Malwarebytes, 2017). The reason why cybercriminals choose ransomware is simple: it's profitable & provides them with instant gratification. Their preferred payment method is usually in cryptocurrencies because they are anonymous and virtually impossible to trace. A troubling fact is, ransomware is becoming more easy to use. Ransomware developed by experienced criminals is finding its way into an online marketplace, offering ransomware as a service (RaaS) for less technically adept scammers also called script kiddies. Cybercriminals are also choosing ransomware because it is difficult defending against it. According to Malwarebytes-sponsored survey of executives in IT-related roles, U.S respondents were most concerned about malware infiltration through email and browsing (Malwarebytes, 2017). As explained before, once this malware enters the system and it has successfully run all its services it is impossible to remove the malware while still retaining all the information in the hard drive without the decryption key. In my opinion, I feel this type of malware will remain and continue to wreak havoc as it is unless companies like Malwarebytes and Kaspersky labs develop more advanced methods of combatting this type of malware before it strikes.

References

Cox, J. W. (2016, 03 29). *MedStar Health turns away patients after likely ransomware cyberattack*. Retrieved from The Washington Post: https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html?utm_term=.9b9950913ed4

Hilt, S., & Sanchez, W. G. (2016, 09 14). *BkSoD by Ransomware: HDDCryptor Uses Commerical Tools to Encrypt Network Shares and Lock HDDs*. Retrieved from Trend Micro: http://blog.trendmicro.com/trendlabs-security-intelligence/bksod-by-ransomware-hddcryptor-uses-commercial-tools-to-encrypt-network-shares-and-lock-hdds/

Johnson, B. (2016, 09 19). *Ransomeware on the Rise*. Retrieved from Carbon Black: https://www.carbonblack.com/2016/09/19/how-ransomware-works/

Kelpsas, B., & Nelson, A. (2016). Ransomware in Hospitals: What Providers Will Inevitably Face When Attacked. *The Journal of Medical Practice Management*, 67-70. *

Kitten, T. (2015, April 6). *New Malware Attacks Prey on Banks*. Retrieved from Bank Info Security: http://www.bankinfosecurity.com/dyre-malware-a-8076

Malwarebytes. (2017). Malwarebytes Endpoint Security vs Ransomware. *Malwarebytes White Paper*, 4.*

Renaud, K., & Tankard, C. (2016). Ransomware claims more victims. *Network Security*, 2.*