LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 10
Date: November 2, 2017

Attacking the InfoSec Supply Chain

Cisco Talos—CCLeaner Command and Control Causes Concern

- Full story links are in references below.
- CCLeaner, owned by Avast, is described as a computer security product, as it is designed to clean up the "crap" on computers, such as temporary files, history, cookies, super cookies, Autocomplete form history, and index.dat files. It also destroys the Windows recycle bin, lnk file, jumplists, memory dumps, and many log files.
- For those of us who work in forensics, we also categorize this as an "anti-forensics" tool, as the previous mentioned artifacts are many that we leverage when performing digital forensics
- Pro tip: Don't try to use CCLeaner to clean up your device before forensic analysis. It looks like a bull in a china shop, and it very obvious. We also know when and how many time you execute it (I digress).
- Cisco's Talos group disclosed on September 18th that CCLeaner version 5.33 was actually bundled with some malware that was actually digitally signed by PiriForm (CCLeaner developer), as was released on August 15, 2017.
- This 5.33 version was being downloaded from the legitimate Avast download servers as early as September 11, 2017.
- At the time, CCLeaner was boasting that they were adding 5 million users per week.
- Initial analysis determined that the malware simply gathered information, such as user rights, running processes, machine inventory, and some command and control communications.
- While the successful attack of the vendor and bundling of malware was successful without detection, the "payload," or intent, didn't really seem that severe.
- Talos was then able to obtain information from the command and control server information. I always smile when extremely smart people and groups just happen to "obtain" that type of information.
- The C&C had a second payload for specific technology companies that may have IP of value.
- According to Talos, tech corporations including HTC, Samsung, Sony, VMWare, Intel, Microsoft, Cisco, Linksys, Google, MSI, and many others are included in the list of targets.
- If you were on this list, there was an additional payload designed specifically for you that was much more feature-filled backdoor, as you were the intended target.

Takeaways

- Espionage from nation states, while not in the limelight as much of late, is back with attacks as sophisticated as this.
- What about the level of skill and patience needed to pull this off?
- Who would target these specific companies? We are all fairly certain we can guess. Agreements between countries or not, we have valuable intel that they seek.
- While this was very sophisticated, it is not the first time.
- Just a couple of months ago, the Netya ransomware worm was distributed through an updated form and accounting software firm that had a primary customer based in the Ukraine. After a couple of sophisticated cyber-attacks that took out power grids during times of conflict with Russia, many feel Russia was behind it. Links to more of this logical accusation are in the references below.
- In 2013, the popular whitelisting company Bit9 was also compromised in supply chain fashion, allowing malware to exist into environments they were deployed. This client list was very targeted, and this attack was attributed to China.
- In 2012, Adobe experienced a breach of one or more of their digital certificates so attackers could digitally sign malware. Some feel that China was involved in that one also.
- Probably the most infamous supply attack occurred in 2011 when RSA was attacked for the root seed for their SecureID multi-factor technology.
- For a patient and skilled adversary with a focus on IP espionage, supply chain attacks may become popular again.

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC's security services, he is also the practice lead for the organization's incident response, forensics, and litigation support practice.

References:

https://www.piriform.com/ccleaner/features

http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html

http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html

http://www.zdnet.com/article/ukraine-calls-out-russian-involvement-in-petya/

https://krebsonsecurity.com/2013/02/security-firm-bit9-hacked-used-to-spread-malware/

https://www.wired.com/2012/09/adobe-digital-cert-hacked/