IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

A Study on Zero Day Malware Attack

Abhay Pratap Singh

Department of CSE, Manav Rachana International University, Faridabad

Abstract: A popular class of threats known as zero day malware has drawn increasing attention from researchers primarily from the organization sector. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. In order for the vendor to rectify the vulnerability, the software company must release a patch. Traditional based antivirus are unable to detect these kind of threats,For cybercriminals, unpatched vulnerabilities in popular software, such as Microsoft Office or Adobe Flash, represent a free pass to any target they might want to attack,so its better to keep update your software feature as well.In this paper our prime focus on getting information new kind of malware and what are the ways we can avoid that kind of threat as well.

Keywords: Zero day malware,Antivirus Evasion techniques,Zero day attack,Spear phishing.

1. INTRODUCTİON

A zero-day attack poses a serious threat to the Internet security as it exploits zero-day vulnerabilities in the computer systems. Attackers take advantage of the unknown nature of zero-day exploits and use them in conjunction with highly sophisticated and targeted attacks to achieve stealthiness with respect to standard intrusion detection techniques. Thus, it's difficult to defend against such attacks. These zero-day attacks can take the form of polymorphic worms, viruses, Trojans, and other malware. There are some effective attacks that avoid detection are blended attacks, polymorphic worms which show distinct behaviors, this includes complex mutation to evade defenses, multi-vulnerability scanning to identify potential targets, targeted exploitation that launches directed attacks against vulnerable hosts, remote shells that open arbitrary ports on compromised hosts to connect at later time.

Traditional security tools rely on malware binary signatures or the reputation of outside urls and servers. By definition these defenses identify only known, confirmed threats. Code morphing and obfuscation techniques generate new malware variants faster than traditional security firms can generate new signatures. And spam filters will not stop low volume, targeted spear-phishing attacks.

At the same time, operating system-level protection such as Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) are becoming less effective.

2. CURRENT DETECTION SYSTEM

Statistical based detection: - The statistical based approach to detecting zero day exploits in real time relies on attack profiles built off historical data. This approach does not usually adapt well to changes in zero day exploit patterns. Any changes in a zero day exploits pattern would require a new profile to be learned by the system.

Signature based detection: - The main requirement of the system is to have an update database of all the signature files of the malware. The accuracy is totally dependent on the signature database of the system. Signature based detection system cannot detect a new virus since the database will not have any information about the new virus, although this method of intrusion detection is fast and accurate since the chances of false alarms are very low in this system.

Anomaly based detection: - Anomaly based detection system monitor the processes on a host machine for any abnormal activity. If any abnormal activity is identified, the system raises an alarm signaling the possible presence of malware. In this detection technique, the system uses the collected heuristics to categorize an activity as normal or malicious. Even though chances of false alarm are relatively higher in this method, it is more reliable because it is also capable of detecting new viruses.

3. ANTİVİRUS EVASİON TECHNİQUES

There are some popular techniques by which attacker can easily bypass antivirus, with the help of these techniques to bypass antivirus protection to install virus, backdoors, boots etc in the target computers. Some of the techniques we will be discussing here:

1- Binding and splitting
2- Converting exe to executable client side script
3- Code obfuscation/code morphing
4- Code injecting
5- Cryptography
6- Polymorphic generator

4. SOME WAYS TO AVOİD ZERO DAY ATTACK

There are some important ways which we can protect ourself from that kind of threat.

DOI 10.17148/IJARCCE.2017.6179

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

1.1 Use a Top-Notch Antivirus.

The first thing you can do is get yourself an excellent antivirus. Make sure the antivirus you choose doesn't just protect against known threats, since zero-day attacks are, by definitions, attacks that were not known just one day earlier. So when you choose your antivirus software, make sure it protects you from both known and unknown attacks. At ZoneAlarm, we call this process Threat Emulation, and it means email attachments and downloads are tested for threats in a safe, cloud-based environment before being allowed to enter your computer.

1.2 Use Only Updated Browsers.

Firefox, Chrome and Internet Explorer all push out automatic updates of their browsers on a regular basis. These updates, which often include patches to newly discovered vulnerabilities, generally take place in the background. The updates are installed when you close and reopen your browser, and won't disturb your use of the browser at all.

1.3 Update Your Software.

Another important way of protecting yourself against zero-day attacks is to make sure that you use the most updated version of your software. If software you trust sends you a notice to update your version, do it. If the software update explains that this a critical update (it may be referred to as a "critical security release" or similar), believe them. The update may include a patch to a recently discovered vulnerability. By updating your software, you immunize yourself against possible future infections through that vulnerability.

Many software vendors automatically update your software for you. Windows, for example, automatically installs important and recommended updates to your Windows software. While it is possible to turn off these automatic updates, it is highly recommended that you don't, as they protect you from potentially dangerous security and reliability issues.

5. CONCLUSION

Zero day malware are very sophisticated,now a days attackers become so smart they used various obfuscation techniques,so that it becomes difficult to identify the nature of virus,even though some intrusion detection system (IDS) can detect but not so much reliable because sometimes they give false positive results also. İn this paper we provided introduction part of zero day malware attcak,still the reserach is going on that kind of threat.

REFERENCES

[1] P. Szor, "The Art of Computer Virus Defense and Research," Symantec Press.
[2] Defenses zero day exploit various sized organization from SANS institute.
[3] R. Kaur and M. Singh ," A Survey on Zero day Polymorphic worm detection techniques", in IEEE Communications Surveys & Tutorials, vol .16,no.3 ,pp.1520-1549,March 2014.