Abstract

Malwares i.e. malicious code/softwares poses prevalent threat to businesses and network across distributed systems. Like it is said in order to catch criminals, we have to think like a criminal, likewise in order to catch cyber criminals/terrorists, we have to think like a cyber-criminal. Malware campaigns have been the driving engines for cyber-warfare being used by cyber criminals & black hat hackers to target organizations, various governments, and financial institutions for leverage & selfish profits, since early decade. In the recent trends of past years, the sophistication of malware campaigns have grown more complex to perform targeted successful attacks and bypass the prevailing & evolving defense mechanisms out there. Our approach is motivated by the factor that malwares breed on the vulnerability of the software applications running across the web. Idea behind pervasive malware propagation mechanism is to provide insight towards various exploitable scenarios based on vulnerabilities and software coding flaws in the software system, its architecture and over the network. Understanding the control flow structure of malware propagation into the system & over the network provides greater insight into how vulnerabilities are being exploited, how target surface
identification is being carried out by the attackers, how exactly the exploits are being delivered using the payloads & what mechanism is being used to maintain the access to the exploited victim over the network. Eventually some suggestions as precautionary mitigation mechanisms to stop the malware propagation.

References

1. Shui Yu, Song Guo, and Ivan Stojmenovic, Fool Me If You Can: Mimicking Attacks and Anti-attacks in Cyberspace, IEEE Transactions on Computers, 139-151, http://dx.doi.org/10.1109/TC.2013.191

Index Terms
Keywords

Pervasive, Malware Propagation Mechanism, Vulnerability, Exploitation, Threat Surfaces, Vulnerability Identification, Payload, Software Flaw, Coding Flaw, Vulnerability Patching, Exploit kit, botnet, command & control center, attack surfaces, Malicious code, Advanced attack.