Notes Nov 8, 2018

Malware

* NIST 800-83 defines malware as:

Table 6.1 Malware Terminology

* Advanced persistent threat
  + Cybercrime directed at business and political targets, using a wide variety of intrusion technology.

Classification of Malware

* Classified into two broad categories
  + Based first on how it spreads or propagates to reach the desired targets
  + Then on the actions or payloads it performs once a target is reached.
* Also classified by:
  + Those that need a host program (parasitic code such as viruses)
  + Those that are independent self-contained programs (worms, trojans, and bots)

Types of Malicious Software (Malware)

* Propagation mechanisms include:
  + Infection of existing content by viruses that is subsequently spread to other systems.
  + Exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
  + Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks.
* Payload actions performed by malware once it reaches a target system can include:
  + Corruption of system or data files
  + Theft of service/make the system a zombie agent of attack as part of a botnet
  + Theft of information from the system/keylogging
  + Stealthing/hiding its presence on the system.

Attack Kits

* Initially the development and deployment of malware required considerable technical skill by software authors
  + The development of virus-creation toolkits in the early 1990s and then more general attack kits in the 2000s greatly assisted in the development and deployment of malware

Toolkits are often known as “crimeware”

* Include a variety of propagation mechanisms and payload modules that even novices can deploy
* Variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them.

Examples are:

* Zeus
* Angler

Attack Sources

* Another significant malware development is the change from attackers being individuals often motivated to demonstrate their technical competence to their peers to more organized and dangerous attack sources such as:
  + Politically motivated attackers
  + Criminals

Advanced Persistent Threats (APTs)

* Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
* Typically attributed to state-sponsored

APT Characteristics

* Advanced
  + Used by the attackers of a wide variety of intrusion technologies and malware including the development of custom malware if required
  + The individual components may not necessarily be technically advanced but are carefully selected to suit the chosen target.
* Persistent
  + Determined application of the attacks over an extended period against the chosen target in order to maximize the chance of success.
  + A variety of attacks may be progressively applied until the target is compromised.
* Threats
  + Threats to the

APT Attacks

* Aim:
  + Varies from theft of intellectual property or security and infrastructure related data to the physical disruption of infrastructure
* Techniques used:
  + Social engineering
  + Spear-phishing email
  + Drive-by-downloads from selected compromised websites likely to be visited by personnel in the target organization
* Intent:
  + To infect the target with sophisticated malware with multiple

Viruses

* Piece of software that infects programs
  + Modifies them to include a copy of the virus
  + Replicates and goes on to infect other content
  + Easily spread through network environments
* When attached to an executable program a virus can do anything that the program is permitted to do
  + Executes secretly when the host program is run
* Specific to operating system and hardware
  + Takes advantage of their details and weaknesses

Virus Components

* Infection mechanism
  + Means by which a virus spreads or propagates
  + Also referred to as the infection vector
* Trigger
  + Event or condition that determines when the payload is activated or delivered
  + Sometimes known as a logic bomb
* Payload
  + What the virus does (besides spreading)
  + May involve damage or benign but noticeable activity

Virus Phases

* Dormant phase
  + Virus is idle
  + Will eventually be activated by some event
  + Not all viruses have this stage
* Triggering phase
  + Virus is activated to perform the function

Macro and Scripting Viruses

* NISTIR 7298 defines a macro virus as:
  + “a virus that attaches itself to documents and uses the macro programming capabilities of the document’s application to execute and propagate”
* Macro viruses infect scripting code used to support active content in a variety of user document types
* Are threatening for a number of reasons:
  + Is platform independent
  + Infect documents, not executable portions of code
  + Are easily spread
  + Because they infect user documents rather than system programs, traditional file system access controls are of limited use in preventing their spread.

Virus Classifications

* Classification by target
  + Boot sector infector