Secfence TECHNOLOGIES

Cyber Espionage, Infiltration and Combating Techniques

-By Atul Agarwal & CERT-IN

What is Cyber Espionage, Infiltration

- Cyber spying or Cyber espionage is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage

- Wikipedia

Secfence TECHNOLOGIES

How?

- Done using exploitation methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware.

- Wikipedia

Secfence TECHNOLOGIES

Attacking techniques

While targeting the end users, the following attack techniques are commonly seen:

- Phishing
- Exploits
  - Drive-by downloads
  - Attachments
- Social Engineering
  - USB Drive
  - Trojan horses / backdoored software

Secfence TECHNOLOGIES

Attack Types : By motive

- Generally, cyber attacks could be categorized into two groups:
  - Mass attacks – Cyber Crime
    - Main motive is financial gains
  - Targeted attacks – Espionage
    - Motive is Intelligence gathering.

Secfence TECHNOLOGIES

Modus Operandi : Cybercrimes

- Highly organized
- Outsourced to specialist
- Use off the shelf malware
  - Zeus, SpyEye
- Use off the shelf exploit kits
  - BlackHole, CrimePack etc.

Secfence TECHNOLOGIES

Modus Operandi : Espionage

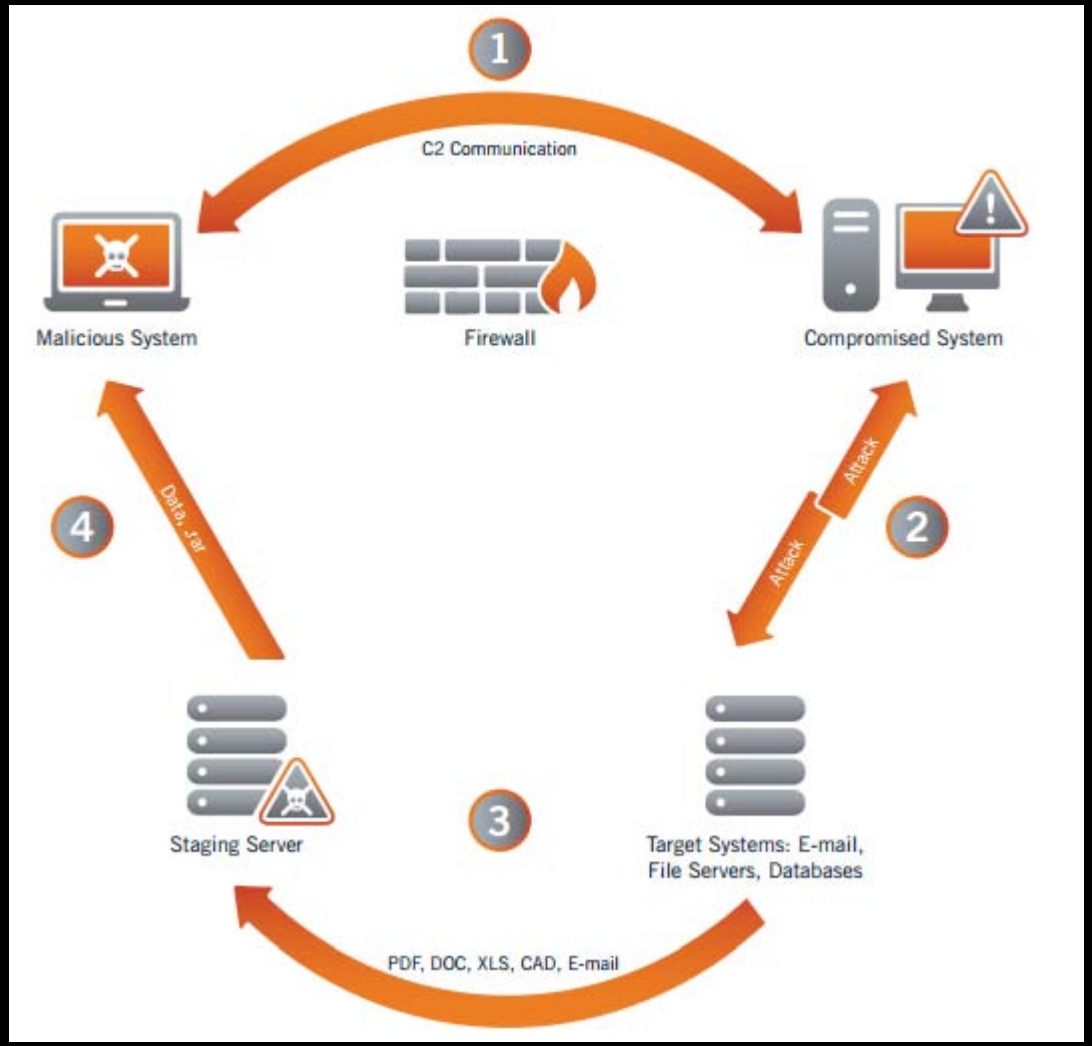
- State backed / Corporate backed
- Motive is exfiltration of national secrets / corporate secrets.
- APT – Advanced Persistent Threats

Secfence TECHNOLOGIES

APT

- **Advanced** – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques such as telephone-interception technologies and satellite imaging.
- **Persistent** – Operators give priority to a specific task, rather than opportunistically seeking information for financial or other gain. This distinction implies that the attackers are guided by external entities.
- **Threat** – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code.

Secfence TECHNOLOGIES



Secfence
TECHNOLOGIES

Cases Studies

- Operation Aurora
  - Began in mid-2009 and continued through December 2009
  - Targets
    - Google
    - Adobe Systems
    - Juniper Networks
    - Rackspace
    - Yahoo
    - Symantec
    - Northrop Grumman
    - Morgan Stanley
    - Dow Chemical
  - Internet Explorer Zero Day used

Stuxnet

- Exploits four unpatched Microsoft vulnerabilities, two for self-replication and two for escalation of privilege
- Contact a command and control server (to download and execute code)
- Contains a Windows rootkit that hide its binaries
- Attempts to bypass security products
- Two valid certificates: Realtek and
- JMicron, both companies based in the same building in Taiwan

Secfence TECHNOLOGIES

Stuxnet

- Fingerprints a specific industrial control system and modifies code on the Siemens
- PLCs to potentially sabotage the system
- Hides modified code on PLCs, essentially a rootkit for PLCs
- Copies itself into Step 7 projects in such a way that it automatically executes when the Step 7 project is loaded
- Updates itself through a peer-to-peer mechanism within a LAN
- Airgaps not safe! (USB was vector here)

Secfence TECHNOLOGIES

More APTs

- Shadows in the cloud
- Operation Shady RAT
- Red October
- Operation Hangover
- And more..

Secfence TECHNOLOGIES

Zero day Market

- Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits : Forbes

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Secfence TECHNOLOGIES

Sources

- zero day black market
  - forums
- zero day legitimate market
  - "penetration testing" software
  - advanced exploit packs
  - exploit-kits
  - VUPEN
  - Defence contractors

Secfence TECHNOLOGIES

Anonymous Infra

- “BulletProof” Servers
- PasteBin / Free hosting etc.
- VPN/Proxy
- Anonymous Mass Emailing

Secfence TECHNOLOGIES

Anonymous Money

- Liberty Reserve
- Paypal
- Other E-currencies
- Bitcoin
- Hawala?

Secfence TECHNOLOGIES

Mitigations / Problems

- Two Factor Authentications
- IP Whitelisting

Secfence TECHNOLOGIES

Basic Malware Analysis and Identification

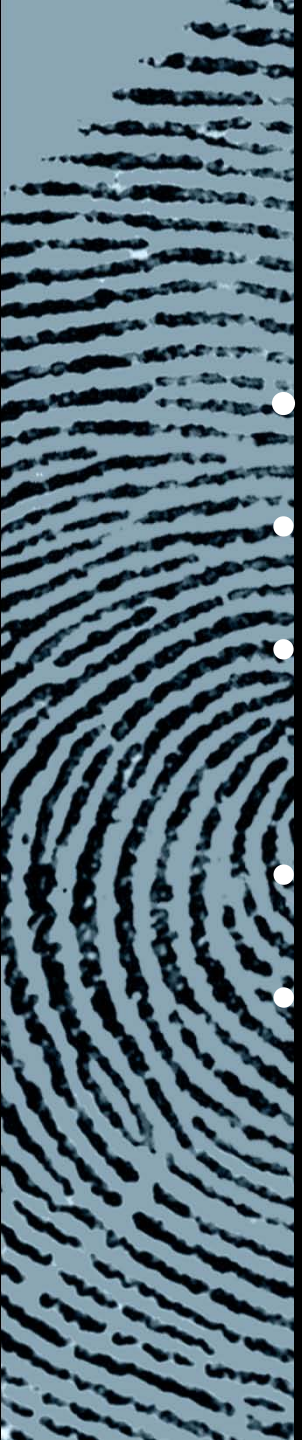
- Using Online Scanners
- Malware - Virustotal.com
- Malware - NoVirusThanks.com (Private Samples)
- PDF's, Flash, URL's – Wepawet
- Malware Analysis report - Anubis

Secfence TECHNOLOGIES

Basic Malware Analysis and Identification

- Verifying integrity of executables
- MD5, SHA Hashes and hash generation too
- Crosschecking Whitelist hash db (http://isc.sans.org/tools/hashsearch.html)
- Virustotal Hash
- Tripwire

Secfence TECHNOLOGIES



Basic Malware Analysis and Identification

- Virtualization and Sandboxing
- About Virtualization and Sandboxing
- Analyzing & using unknown binaries in Virtual Environments and Sandboxes
- Using sandboxed browsers
- Using Snapshots, non-persistant drives to stay safe

Secfence TECHNOLOGIES

Best Practices

- Disabling Autorun
- Using Email Safely
- Using online document readers
- Using safe document readers (Sumatra, OpenOffice)
- Disable Javascript on PDF Readers
- Using safe browsers + NoScript
- Using OpenDNS
- Identifying Phishing (Phishtank)
- Identifying Executable extensions

Secfence TECHNOLOGIES