Lesson 4

Identifying Social Engineering and Malware

CompTIA

Topic 4A

Compare and Contrast Social Engineering Techniques

Syllabus Objectives Covered

- 1.1 Compare and contrast different types of social engineering techniques

Social Engineering

- “Hacking the human”
- Purposes of social engineering
  - Reconnaissance and eliciting information
  - Intrusion and gaining unauthorized access
- Many possible scenarios
  - Persuade a user to run a malicious file
  - Contact a help desk and solicit information
  - Gain access to premises and install a monitoring device

Social Engineering Principles

- Reasons for effectiveness
- Familiarity/liking
  - Establish trust
  - Make request seem reasonable and natural
- Consensus/social proof
  - Exploit polite behaviors
  - Establish spoofed testimonials or contacts
- Authority and intimidation
  - Make the target afraid to refuse
  - Exploit lack of knowledge or awareness
- Scarcity and urgency
  - Rush the target into a decision

Impersonation and Trust

- Impersonation
  - Pretend to be someone else
  - Use the persona to charm or to intimidate
  - Exploit situations where identity-proofing is difficult
- Pretexting
  - Using a scenario with convincing additional detail
- Trust
  - Obtain or spoof data that supports the identity claim

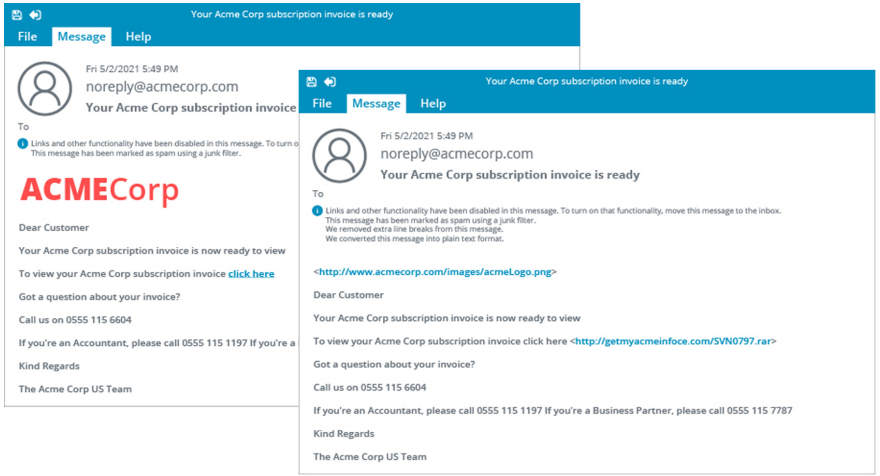
Dumpster Diving and Tailgating

- Dumpster diving
  - Steal documents and media from trash
- Tailgating
  - Access premises covertly
  - Follow someone else through a door
- Piggy backing
  - Access premises without authorization, but with the knowledge of an employee
  - Get someone to hold a door open

Identity Fraud and Invoice Scams

- Identity fraud
  - Impersonation with convincing detail and stolen or spoofed proofs
  - Identity fraud versus identity theft
- Invoice scams
  - Spoofing supplier details to submit invoices with false account details
- Credential theft and misuse
  - Credential harvesting
  - Shoulder surfing
  - Lunchtime attack

Phishing, Whaling, and Vishing



- Trick target into using a malicious resource
- Spoof legitimate communications and sites
- Spear phishing
  - Highly targeted/tailored attack
- Whaling
  - Targeting senior management
- Vishing
  - Using a voice channel
- SMiShing
  - Using text messaging

Spam, Hoaxes, and Prepending

- Spam
  - Unsolicited email
  - Email address harvesting
  - Spam over Internet messaging (SPIM)
- Hoaxes
  - Delivered as spam or malvertising
  - Fake A-V to get user to install remote desktop software
  - Phone-based scams
- Prepending
  - Tagging email subject line
  - Can be used by threat actor as a consensus or urgency technique
  - Can be added by mail systems to warn users

Pharming and Credential Harvesting

- Passive techniques have less risk of detection
- Pharming
  - Redirection by DNS spoofing
- Typosquatting
  - Use cousin domains instead of redirection
  - Make phishing messages more convincing
- Watering hole
  - Target a third-party site
  - Customer, supplier, hobbies, social media…
- Credential harvesting
  - Attacks focused on obtaining credentials for sale rather than direct intrusion
  - Attacks focused on obtaining multiple credentials for single company

Influence Campaigns

- Sophisticated threat actors using multiple resources to change opinions on a mass scale
- Soft power
  - Leveraging diplomatic and cultural assets
- Hybrid warfare
  - Use of espionage, disinformation, and hacking
- Social media
  - Use of hacked accounts and bot accounts
  - Spread rumor and reinforce messaging

Topic 4B

Analyze Indicators of Malware-based Attacks

Syllabus Objectives Covered

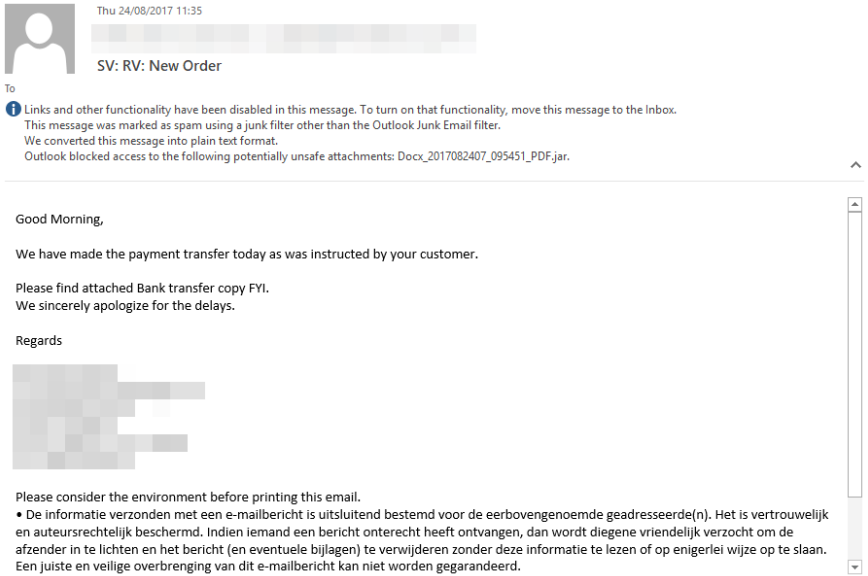
- 1.2 Given a scenario, analyze potential indicators to determine the type of attack
- 4.1 Given a scenario, use the appropriate tool to assess organizational security (Cuckoo only)

Malware Classification

- Classification by vector or infection method
- Viruses and worms
  - Spread within code without authorization
- Trojans
  - A malicious program concealed within a benign one
- Potentially unwanted programs/applications (PUPs/PAPs)
  - Pre-installed “bloatware” or installed alongside another app
  - Not completely concealed, but installation may be covert
  - Also called grayware
- Classification by payload

Computer Viruses

- Rely on some sort of host file or media
  - Non-resident/file infector
  - Memory resident
  - Boot
  - Script/macro
- Multipartite
- Polymorphic
- Vector for delivery

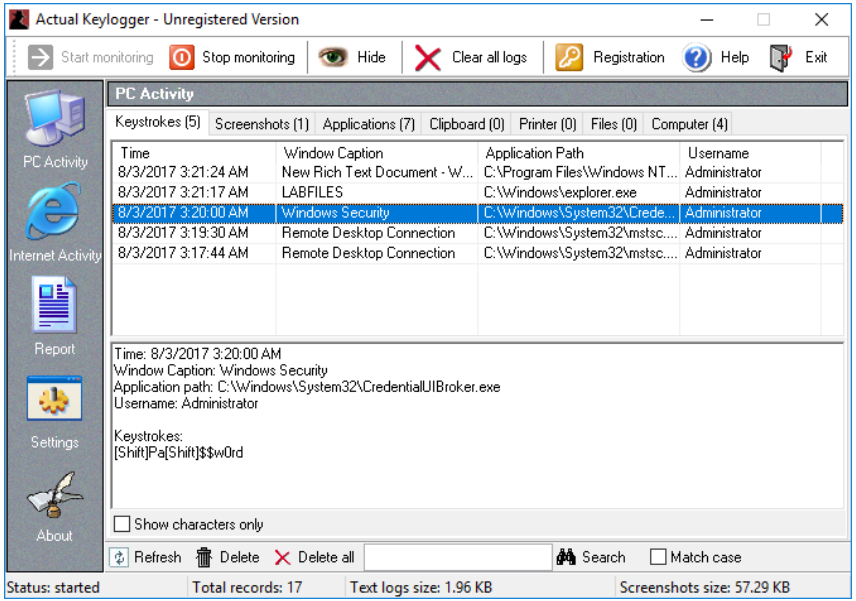


Screenshot used with permission from Microsoft.

Computer Worms and Fileless Malware

- Early computer worms
  - Propagate in memory/over network links
  - Consume bandwidth and crash process
- Fileless malware
  - Exploiting remote execution and memory residence to deliver payloads
  - May run from an initial script or Trojan
  - Persistence via the registry
  - Use of shellcode to create backdoors and download additional tools
  - "Living off the land" exploitation of built-in scripting tools
- Advanced persistent threat (APT)/advanced volatile threat (AVT)/ low observable characteristics (LOC)

Spyware, Adware, and Keyloggers



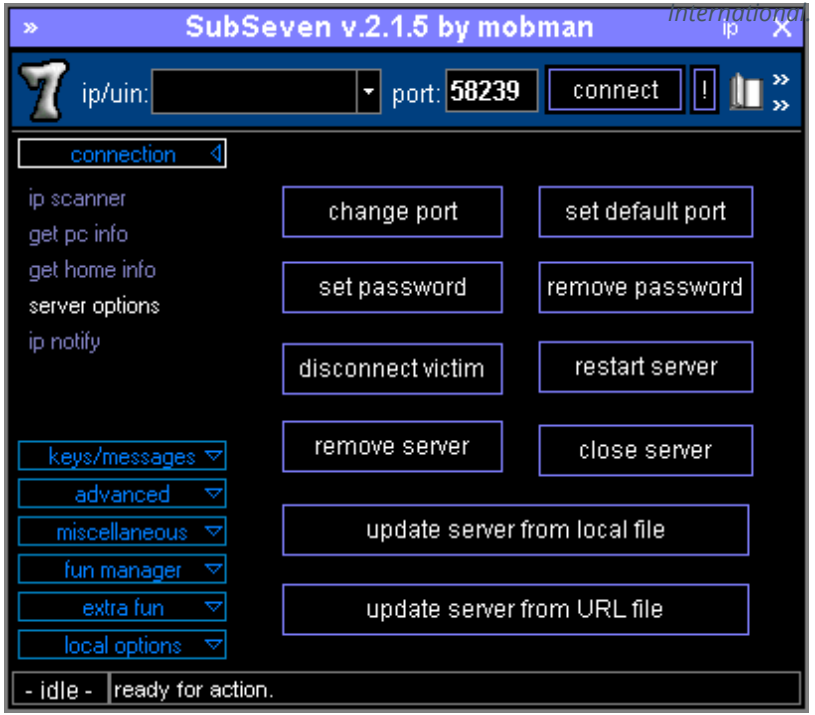
Screenshot used with permission from ActualKeylogger.com.

- Tracking cookies
- Adware (PUP/grayware)
  - Changes to browser settings
- Spyware (malware)
  - Log all local activity
  - Use of recording devices and screenshots
  - Redirection
- Keylogger
  - Software and hardware

Backdoors and Remote Access Trojans

- Backdoor malware
- Remote access trojan (RAT)
- Bots and botnets
- Command & control (C2 or C&C)
- Backdoors from misconfiguration and unauthorized software

Screenshot used with permission from Wikimedia Commons by CCAS4.0 International.



Rootkits

- Local administrator versus SYSTEM/root privileges
- Replace key system files and utilities
- Purge log files
- Firmware rootkits

Ransomware, Crypto-Malware, and Logic Bombs

- Ransomware
  - Nuisance (lock out user by replacing shell)
- Crypto-malware
  - High impact ransomware (encrypt data files or drives)
- Cryptomining/crypojacking
  - Hijack resources to mine cryptocurrency
- Logic bombs

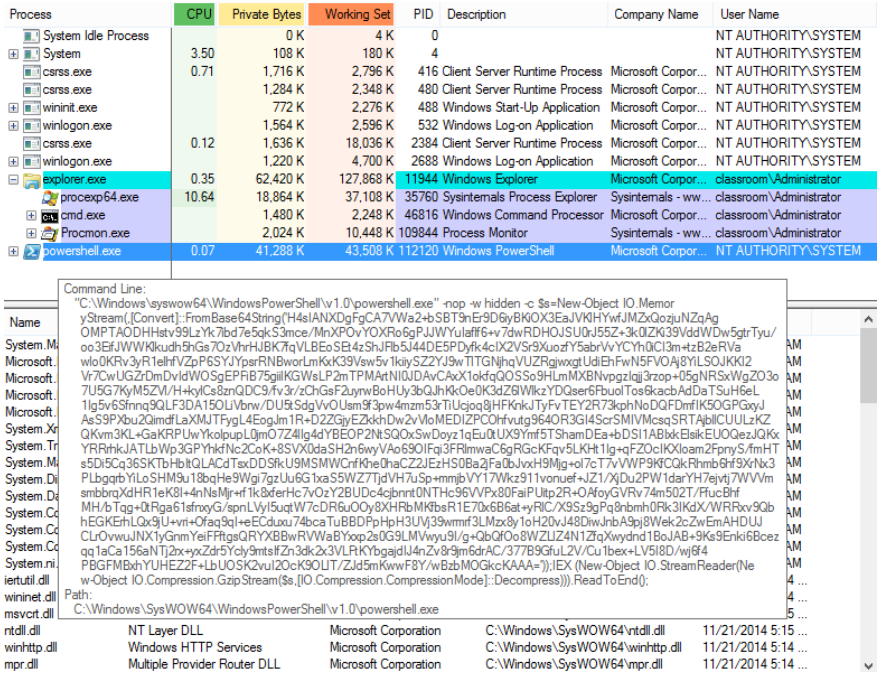
Image by Wikimedia Commons.

Malware Indicators

- Browser changes or overt ransomware notification
- Anti-virus notifications
  - Endpoint protection platforms and next-gen A-V
  - Behavior-based analysis
- Sandbox execution
  - Cuckoo
- Resource utilization/consumption
  - Task Manager and top
- File system changes
  - Registry
  - Temp files

Process Analysis

Screenshot: Process Explorer docs.microsoft.com/en-us/sysinternals.



- Signature-based detection is failing to identify modern APT-style tools
- Network and host behavior anomalies drive detection methods
- Running process analysis
  - Process Explorer
- Logging activity
  - System Monitor
- Network activity

Lesson 4

Summary