RSA®Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SPO-W06

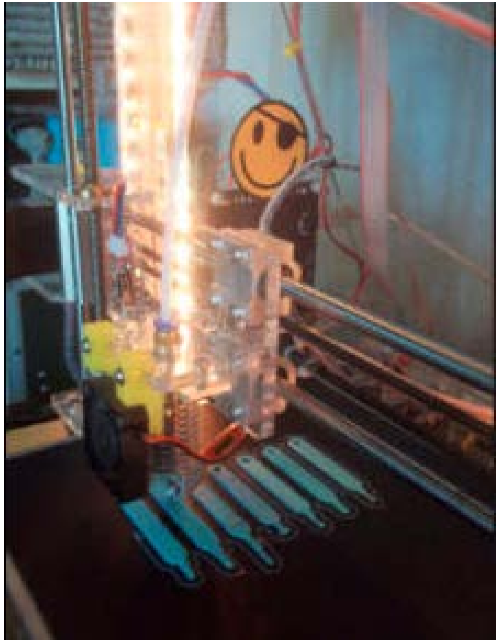
BADMIN:
(Ab)using legitimate sysadmin tools for offensive purposes

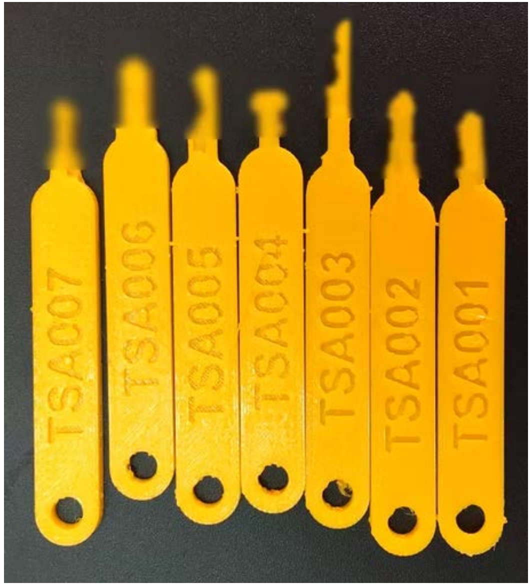
Andre Derek Protas

Technical Director
CyberPoint International
@tacticalRCE

Tools and Access Used for Defense

Tools and Access Used for OFFENSE





Introduction

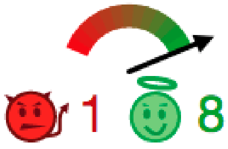
- Adversaries don’t always use flashy Trojans to pillage your network
- Administrative tools can be plenty to roam and gain a long-term foothold in your network
- Administrative tools give adversary many advantages:
  - Typically well-tested, supported software
  - Most AV/HIPS/NIPS overtly white-list their actions
  - Tend to be available across all platforms for stability
  - Plausible deniability

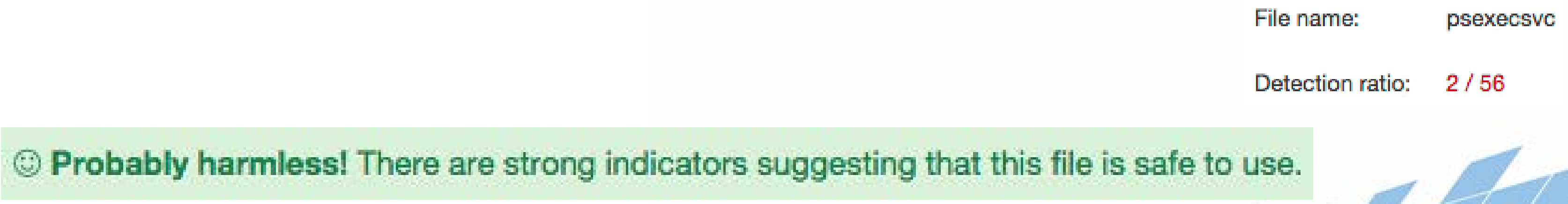
Disclaimer

- We are not discussing any vulnerabilities; this is ***expected behavior***
- Focus is on Windows, but other platforms are susceptible to the same concept
  - e.g., provisioning, batch automation, network booting, etc.)
- Tools / code / examples exist for all topics in the public and have been used in activate attacks or tests
- These are only a few examples to drive the point home, not an exhaustive list

Tool Example: PSEXEC

- Legit Purpose: run commands on remote windows hosts
- Malicious Purpose: HIPS evasion with MSFT-signed executable
- Used in advanced “skeleton key” compromises
- Detection?: Monitor for “BAD” psexec executions
  - Very difficult to know what “BAD” is, unless any execution is bad



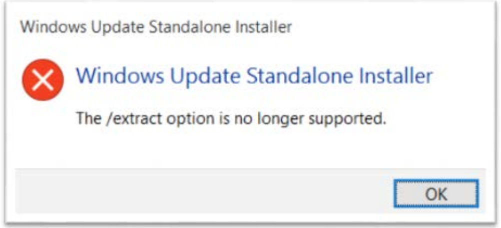

File name: psexecsvc

Detection ratio: 2 / 56

☺ **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

Tool Example: WUSA

- Legit Purpose: make Windows installer packages
- Malicious Purpose: evade UAC and file restrictions
- Allows arbitrary file writing to directories that normal require UAC prompts
- A “feature” of the /extract switch, removed in Windows 10
- Detection?: Monitor for bad WUSA processes



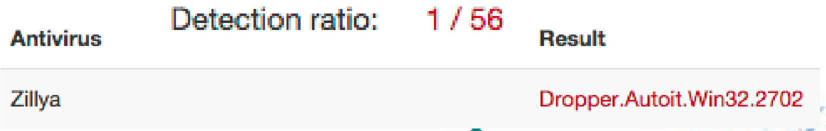
Windows Update Standalone Installer

Windows Update Standalone Installer

The /extract option is no longer supported.

Tool Example: AutoIT

- Legit Purpose: windows automation / provisioning toolset
- Malicious Purpose: evade anti-virus
- Very simple scripting language to learn (intended for administrators, not developers)
- Very easy framework to use to perform malicious actions as “AutoIT” and not as a stand-alone piece of malware
- Used in many modern day attacks as a first-stage “dropper” to validate endpoint prior to dropping real malicious payload
- Detection?: Hope your AV runtime picks up payload



Detection ratio: 1 / 56

Antivirus	Result
Zillya	Dropper.Autoit.Win32.2702

Tool Example: WSUS

Windows Server
Update Services

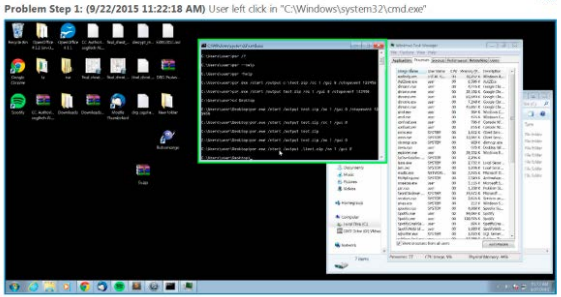
- Legit Purpose: patch distribution for enterprise
- Malicious Purpose: malicious binary distribution across enterprise
- Requires limited modifications to deploy non-MSFT binaries
- Non-SSL deployments are especially susceptible to MITM attacks
- Detection?: Look for rogue packages in WSUS repository
- Prevention?: SSL enabled (not default)

Tool Example: AD Security Support Providers

- Legit Purpose: support extended authentication schemes
- Malicious Purpose: inspect/forward credentials in plaintext
- Very simple automated tools to deploy SSP as part of MetaSploit framework
- Has been seen in the wild in multiple campaigns
- Detection?: Look for new SSPs in DC registry
  - HKLM: System\CurrentControlSet\Control\Lsa\Security Packages

Tool Example: Problem Steps Recorder

- Legit Purpose: helps users show their problems to admins with screenshots, keystrokes, etc.
- Malicious Purpose: native CLI for recording user actions
  - Bonus: Report is delivered as MHT file (***great*** phishing opportunity)
- Detection?: if psr.exe isn’t needed, any execution of it should be considered suspicious



Problem Step 1: (9/22/2015 11:22:18 AM) User left click in "C:\Windows\system32\cmd.exe"

Tool Example: Powershell

- Legit Purpose: automation and programming
- Malicious Purpose: programming malicious actions
  - Obfuscating malicious payloads in memory
  - Powershell Empire: fully functional, powershell-only backdoor
  - Powershell Service? Now we have SSH for Windows >=]
- Detection?:
  - Event logs and reporting
  - Persistent location monitoring
  - Forensics (memory, prefetch)

Tool Example: WMI

- Legit Purpose: administration and system querying
- Malicious Purpose: code execution and reconnaissance
  - Allows for simple and effective persistence
  - Can connect and query / execute arbitrary code on remote systems
- Detection?:
  - Use WMI to query your hosts ;-]

Summary

- Many administrative tools can be used for good or bad purposes
- There’s a good chance these tools are already being used by your administrators on your network
- Smart, advanced adversaries understand the advantages of using administrative tools and leverage them in their campaigns
- These tools and techniques can be tested easily to verify your posture

Apply Slide

- Run Red/Blue Scenarios ***Constantly***
  - Dedicated teams with metrics
  - How would your AV / HIPS / NIPS deal with these threats?
- ***Challenge*** your security vendors
  - It’s ok to ask them specifics about if/how they detect a threat
  - “Zero-Day Protection” wasn’t discussed today
- Weigh the pros and cons of ***automation***
  - Harder to find a malicious administrative tool action if it’s commonly used in your environment
- ***PROTECT YOUR ADMINS!***
  - If they are compromised, everything is compromised

Q&A / Contact

Thank You for Attending!

Are There Any Questions?

CONTACT

Web: www.cyberpointllc.com

Email: aprotas@cyberpointllc.com

Twitter: @tacticalRCE