OPEN
SECURITY

Cyberspace Trapping

The Offensive Defender

whoami

- Former Air Force
- Counterhacker
- Founder Open Security
- Instructor with the SANS Institute
- Author of the SEC460 Course

I Am Red

- Offensive Perspective is Critical for Defense
  - This is True for Defense Software Vendors as too!
- Targeting Threat Tactics Requires Intimate Understanding

Losing is Inevitable

Defense Needs to Be Successful 100%
Offense just Needs to Win Once

Losing is Inevitable

- The quickest way to lose is to cede victory
  - It stifles Creative Thinking
  - It’s the Easy Way Out
- If a catastrophic breach feels inevitable how can we change this?
- Military Science gives us parallels from which to Learn

Introspection

- Is your Defense at the Boundary or Behind it?
- Do you know how your Vendor Tools Work?
- Breaches Happen!
  - The Maginot Line Style of Defense is Outdated and Dangerous
  - It is Time to Invest and Empower People to Customize Defense

Fighting the Right Fight

Is your Defensive Strategy Targeted to Address True Threats?

Cyberspace Trapping

- It’s not **You** it’s **Me**
- Poison vs Venom

Cyberspace trapping is the practice of poisoning threat Tactics, Techniques, and Procedures in order to weaponize your environment

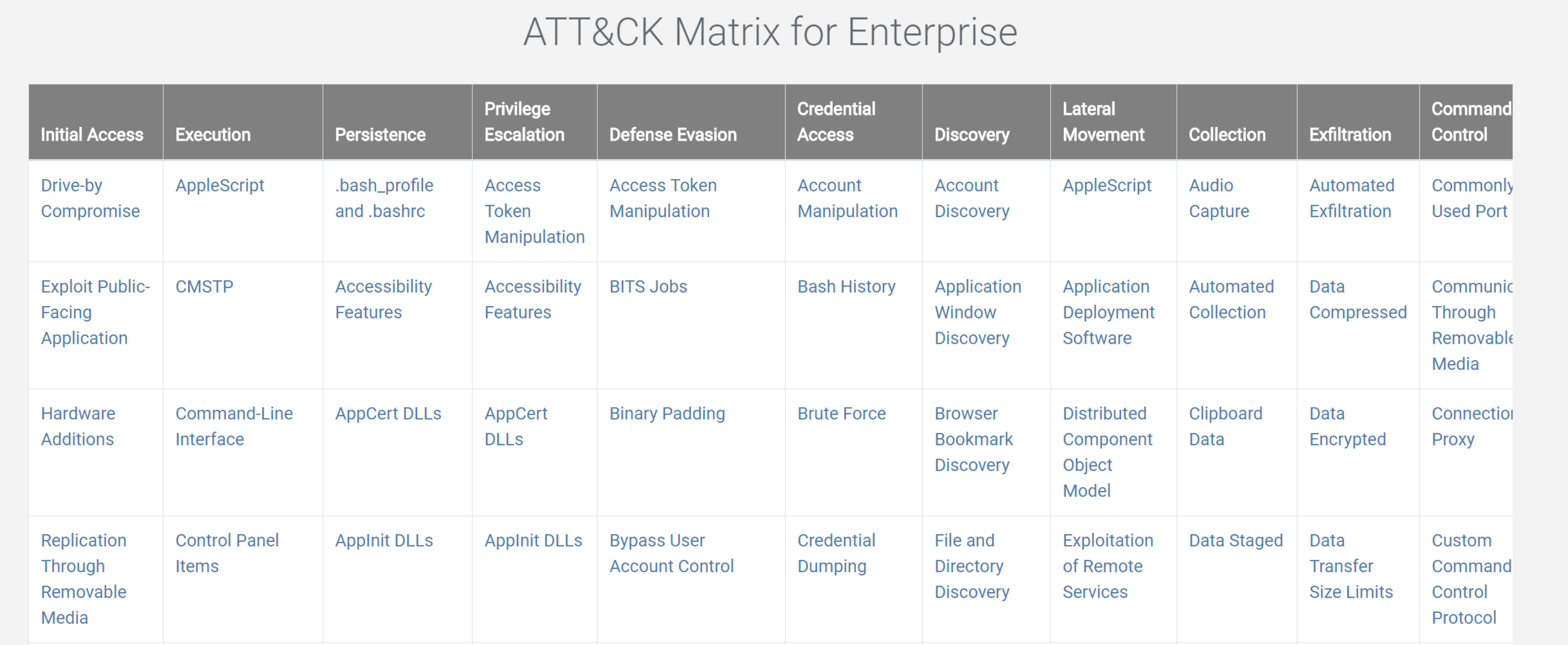
Tactics, Techniques, and Procedures (TTP)

- TTP is a widely used term in the information security community but many misuse or incorrectly delineate the term.
  - Tactics - "*The employment and ordered arrangement of forces in relation to each other.* See also procedures; techniques."
  - Techniques - "*Non-prescriptive ways or methods used to perform missions, functions, or tasks.* See also procedures; tactics."
  - Procedures - "*Standard, detailed steps that prescribe how to perform specific tasks.* See also tactics; techniques."

Know thy self, know thy enemy. A thousand battles, a thousand victories

Finding Threat TTP

- Techniques grouped within a subset of overarching tactics
- Many listed techniques are in use by most threat groups

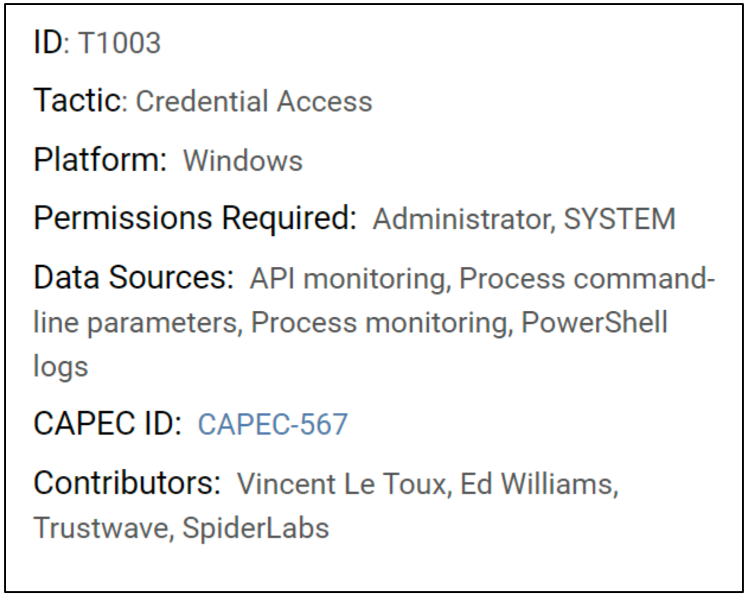


ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communic Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connectio Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command Control Protocol

Mimikatz and LSASS Passwords

- According to the NSA Red Team Mimikatz is the number one threat to US Government Environments



ID: T1003

Tactic: Credential Access

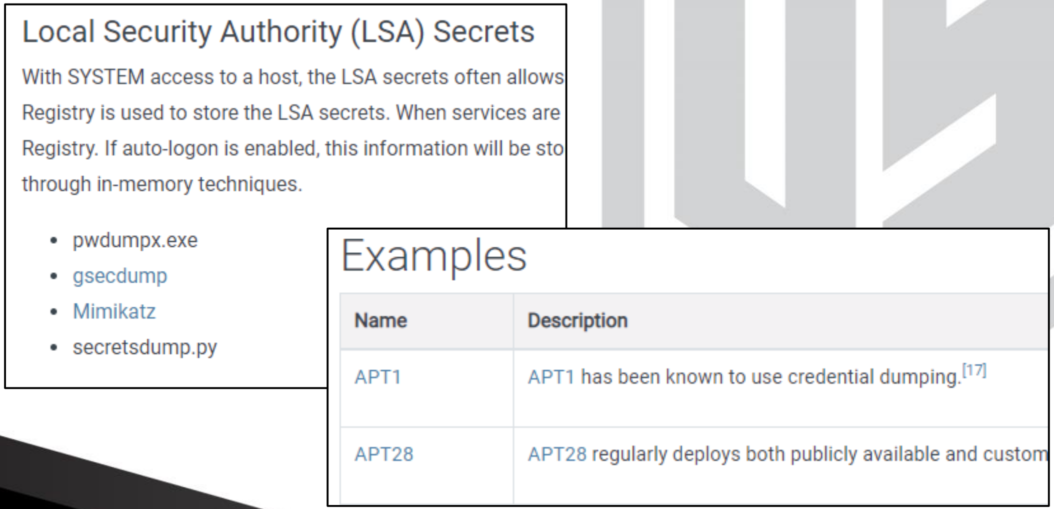
Platform: Windows

Permissions Required: Administrator, SYSTEM

Data Sources: API monitoring, Process command-line parameters, Process monitoring, PowerShell logs

CAPEC ID: CAPEC-567

Contributors: Vincent Le Toux, Ed Williams, Trustwave, SpiderLabs



Local Security Authority (LSA) Secrets

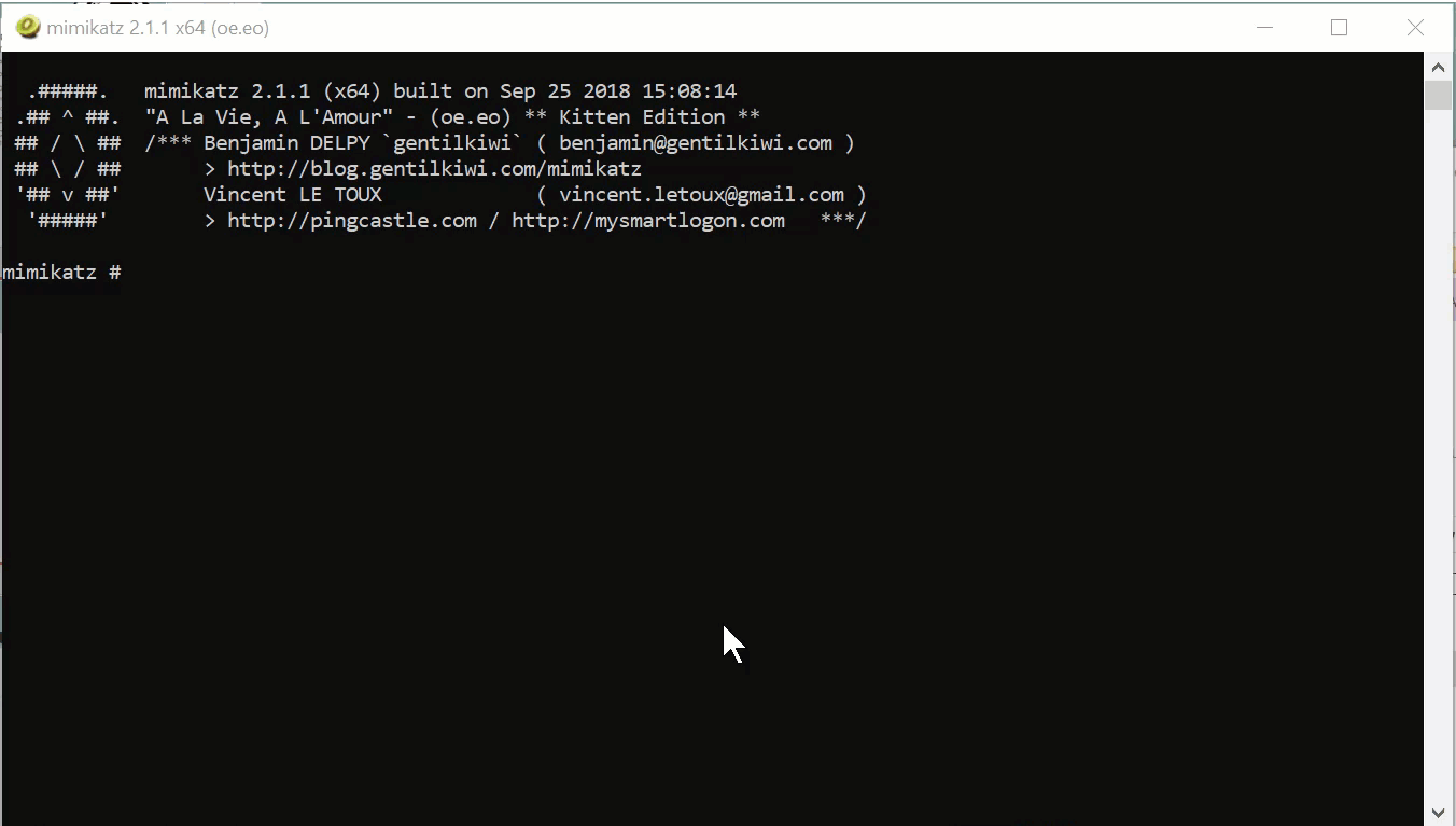
With SYSTEM access to a host, the LSA secrets often allows
Registry is used to store the LSA secrets. When services are
Registry. If auto-logon is enabled, this information will be sto
through in-memory techniques.

- pwdumpx.exe
- gsecdump
- Mimikatz
- secretsdump.py

Examples

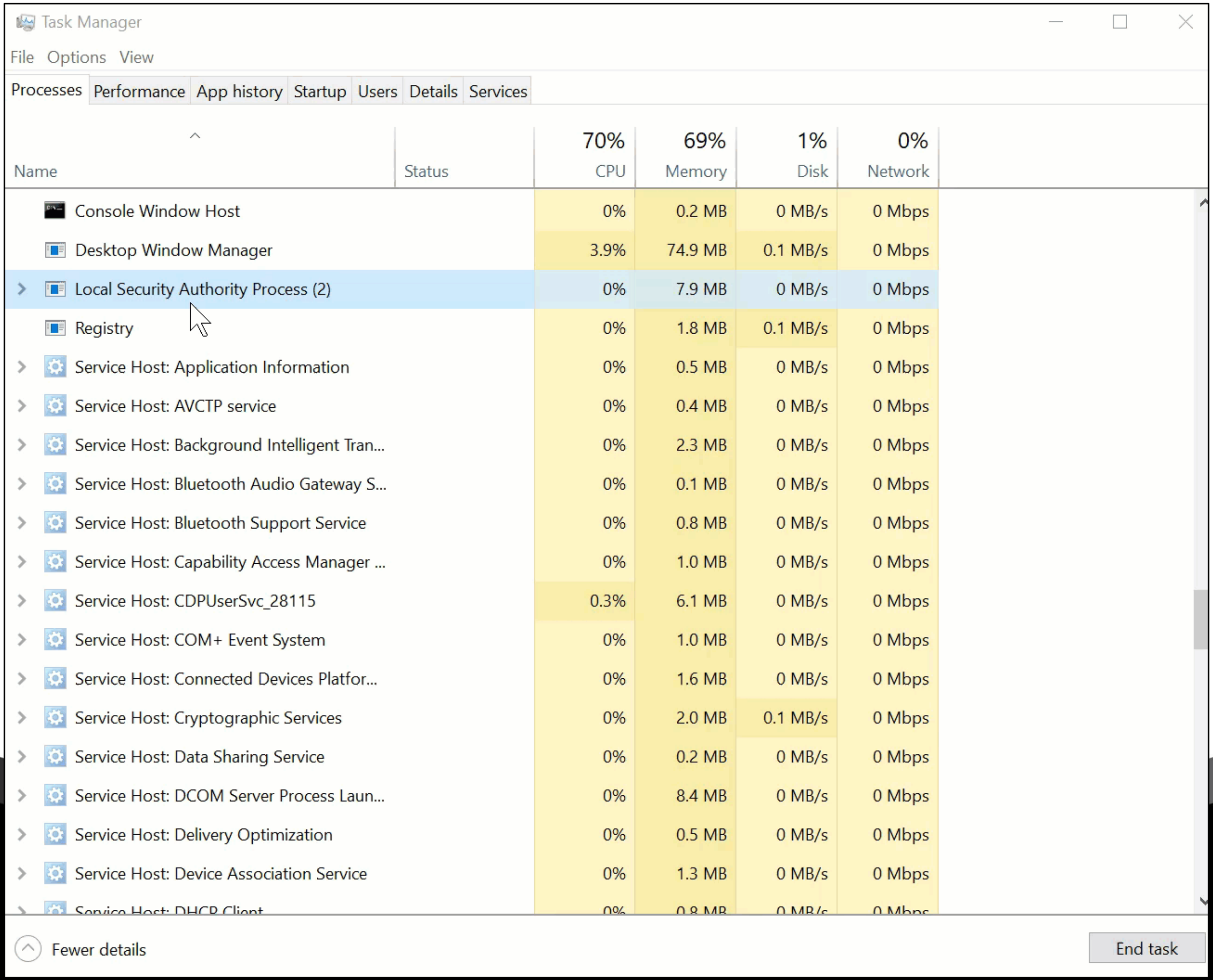
Name	Description
APT1	APT1 has been known to use credential dumping.[17]
APT28	APT28 regularly deploys both publicly available and custom

Mimikatz



```
  .#####.   mimikatz 2.1.1 (x64) built on Sep 25 2018 15:08:14
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz #
```

Task Manager LSASS Dump



Name	Status	70% CPU	69% Memory	1% Disk	0% Network
Console Window Host		0%	0.2 MB	0 MB/s	0 Mbps
Desktop Window Manager		3.9%	74.9 MB	0.1 MB/s	0 Mbps
Local Security Authority Process (2)		0%	7.9 MB	0 MB/s	0 Mbps
Registry		0%	1.8 MB	0.1 MB/s	0 Mbps
Service Host: Application Information		0%	0.5 MB	0 MB/s	0 Mbps
Service Host: AVCTP service		0%	0.4 MB	0 MB/s	0 Mbps
Service Host: Background Intelligent Tran...		0%	2.3 MB	0 MB/s	0 Mbps
Service Host: Bluetooth Audio Gateway S...		0%	0.1 MB	0 MB/s	0 Mbps
Service Host: Bluetooth Support Service		0%	0.8 MB	0 MB/s	0 Mbps
Service Host: Capability Access Manager ...		0%	1.0 MB	0 MB/s	0 Mbps
Service Host: CDPUserSvc_28115		0.3%	6.1 MB	0 MB/s	0 Mbps
Service Host: COM+ Event System		0%	1.0 MB	0 MB/s	0 Mbps
Service Host: Connected Devices Platfor...		0%	1.6 MB	0 MB/s	0 Mbps
Service Host: Cryptographic Services		0%	2.0 MB	0.1 MB/s	0 Mbps
Service Host: Data Sharing Service		0%	0.2 MB	0 MB/s	0 Mbps
Service Host: DCOM Server Process Laun...		0%	8.4 MB	0 MB/s	0 Mbps
Service Host: Delivery Optimization		0%	0.5 MB	0 MB/s	0 Mbps
Service Host: Device Association Service		0%	1.3 MB	0 MB/s	0 Mbps
Service Host: DHCP Client		0%	0.8 MB	0 MB/s	0 Mbps

Other Mimikatz Implementations

- PowerShell
- Cobalt Strike
- C#
- Metasploit
- Many Many Others

Poisoning LSASS

Tactic

- Escalate privileges to domain admin using stolen credentials

Technique

- Use Mimikatz to retrieve credentials from LSASS memory

Procedures

- Steps to accomplish the techniques mentioned above

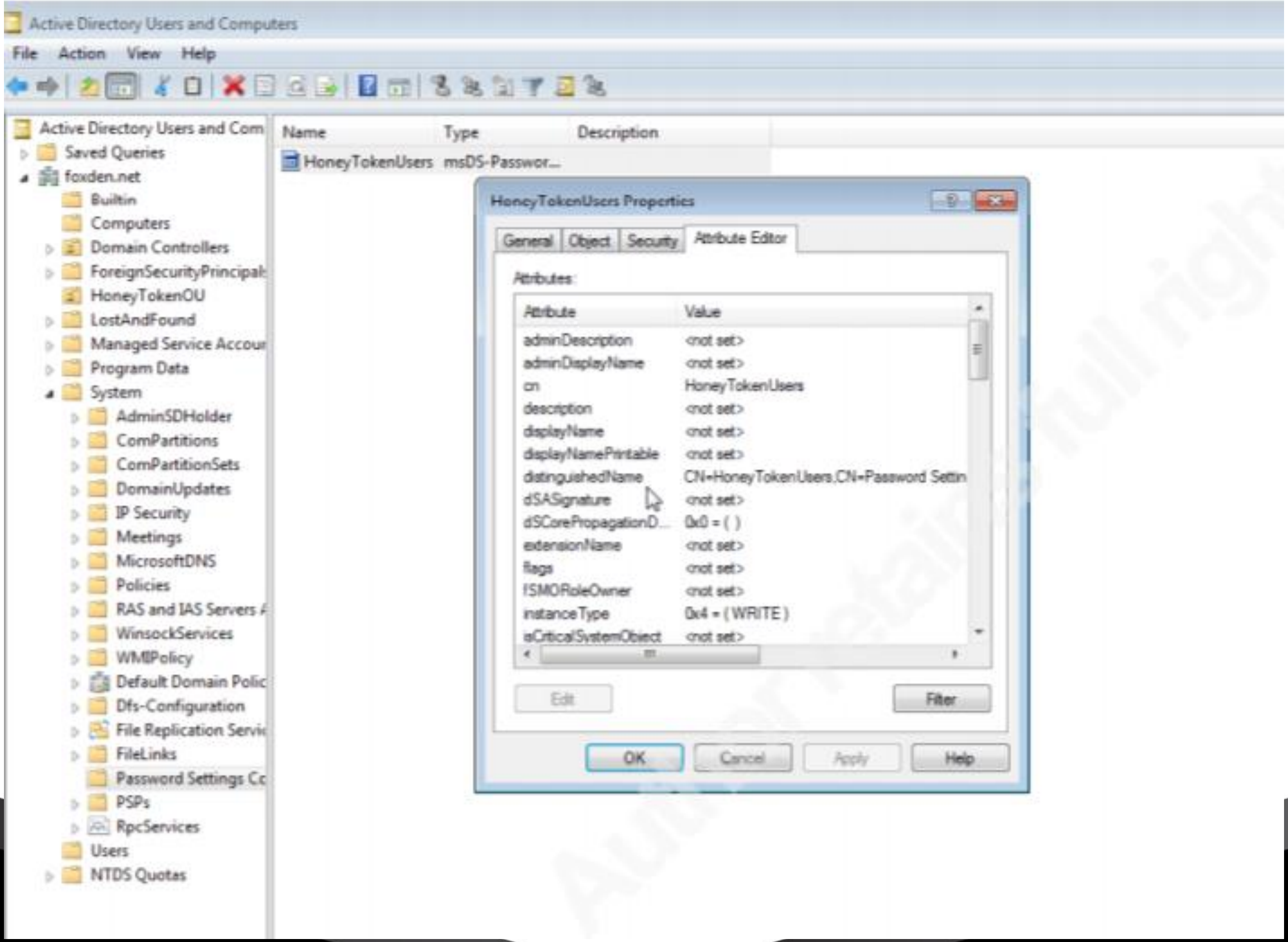
Traditional Defense

1. Do more user awareness training
2. Write a Mimikatz signature and pray

Cyberspace Trapping

- Create fake accounts configured to lockout after one failed attempt
  - Use RunAs to seed LSASS with fake creds

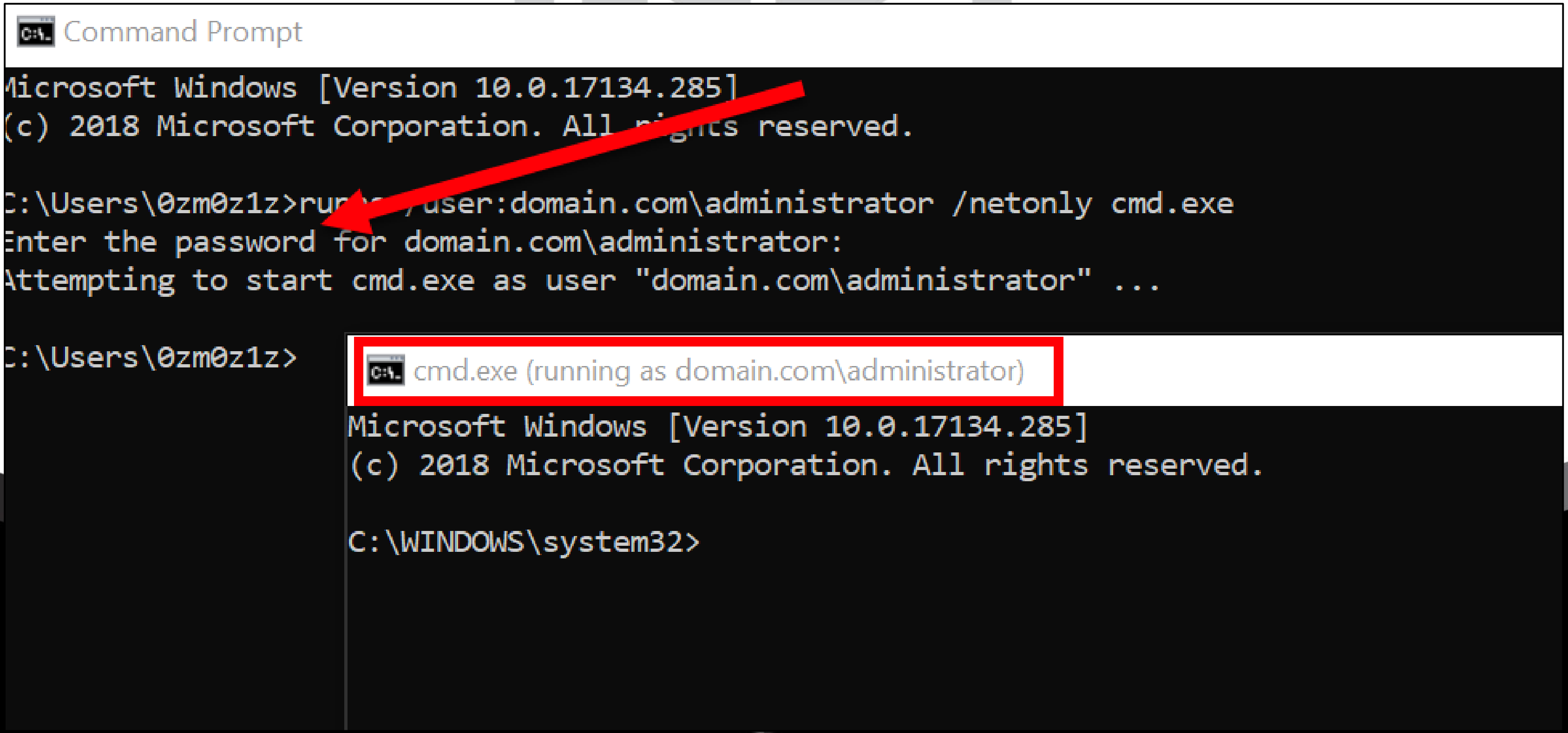
Configuring Fine-Grained Password Policies



Attribute	Value
adminDescription	<not set>
adminDisplayName	<not set>
cn	HoneyTokenUsers
description	<not set>
displayName	<not set>
displayNamePrintable	<not set>
distinguishedName	CN=HoneyTokenUsers,CN=Password Settin
dSASignature	<not set>
dSCorePropagationD...	0x0 = ( )
extensionName	<not set>
flags	<not set>
fSMORoleOwner	<not set>
instanceType	0x4 = (WRITE)
isCriticalSystemObject	<not set>

Sneaking Fake Credentials into LSASS

```
runas /user:domain.com\admin /netonly cmd.exe
```

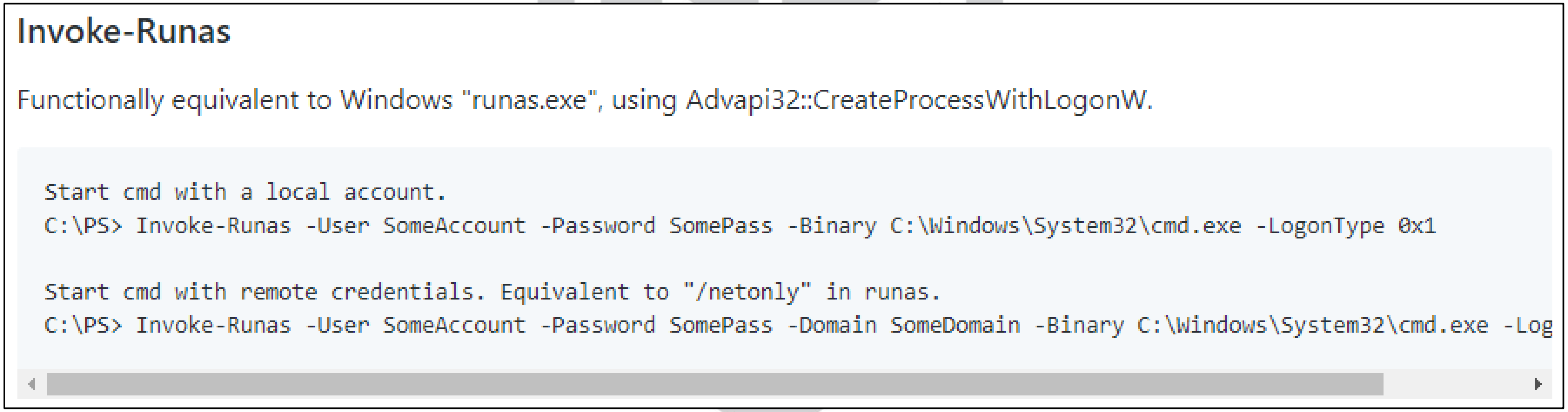


```
Microsoft Windows [Version 10.0.17134.285]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\0zm0z1z>runas /user:domain.com\administrator /netonly cmd.exe
Enter the password for domain.com\administrator:
Attempting to start cmd.exe as user "domain.com\administrator" ...

C:\Users\0zm0z1z>
```

```
Microsoft Windows [Version 10.0.17134.285]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

Sneaking Fake Credentials into LSASS

https://github.com/FuzzySecurity/PowerShell-Suite



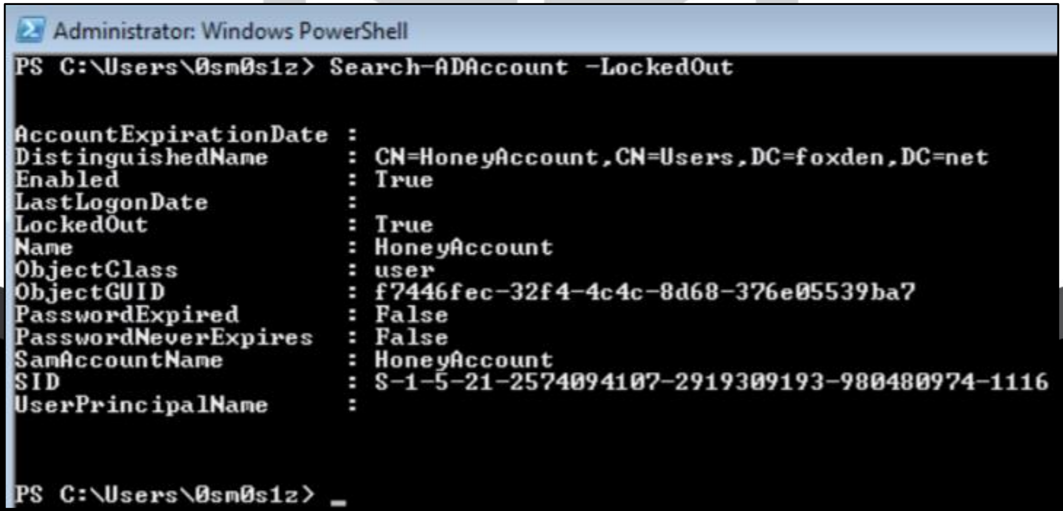
Invoke-Runas

Functionally equivalent to Windows "runas.exe", using Advapi32::CreateProcessWithLogonW.

```
Start cmd with a local account.
C:\PS> Invoke-Runas -User SomeAccount -Password SomePass -Binary C:\Windows\System32\cmd.exe -LogonType 0x1

Start cmd with remote credentials. Equivalent to "/netonly" in runas.
C:\PS> Invoke-Runas -User SomeAccount -Password SomePass -Domain SomeDomain -Binary C:\Windows\System32\cmd.exe -Log
```

Monitoring and Scaling with PowerShell

- Tracking LockedOut Status Provides us with Additional Sensors within the Environment
- Correlating this Information with the IP Address of the system where the Trap is in Place Allows for Increased Reaction Speed



```
PS C:\Users\0sm0s1z> Search-ADAccount -LockedOut


AccountExpirationDate :
DistinguishedName     : CN=HoneyAccount,CN=Users,DC=foxden,DC=net
Enabled               : True
LastLogonDate         :
LockedOut             : True
Name                  : HoneyAccount
ObjectClass           : user
ObjectGUID            : f7446fec-32f4-4c4c-8d68-376e05539ba7
PasswordExpired       : False
PasswordNeverExpires  : False
SamAccountName        : HoneyAccount
SID                   : S-1-5-21-2574094107-2919309193-980480974-1116
UserPrincipalName     :



PS C:\Users\0sm0s1z> _
```

Other Implementations

- Passwords.txt Files
- Poisoned Password Managers
- Network Passwords
  - Telnet
  - FTP
  - HTTP

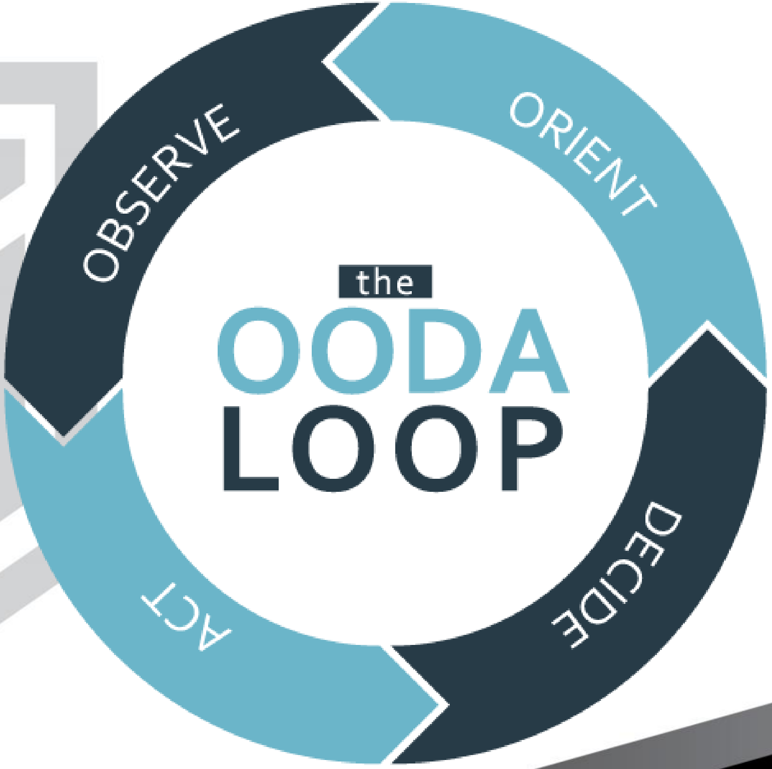
The threat actor can no longer know whether to trust the password gifts of careless users. They might just be poisoned.

Trap Master 101

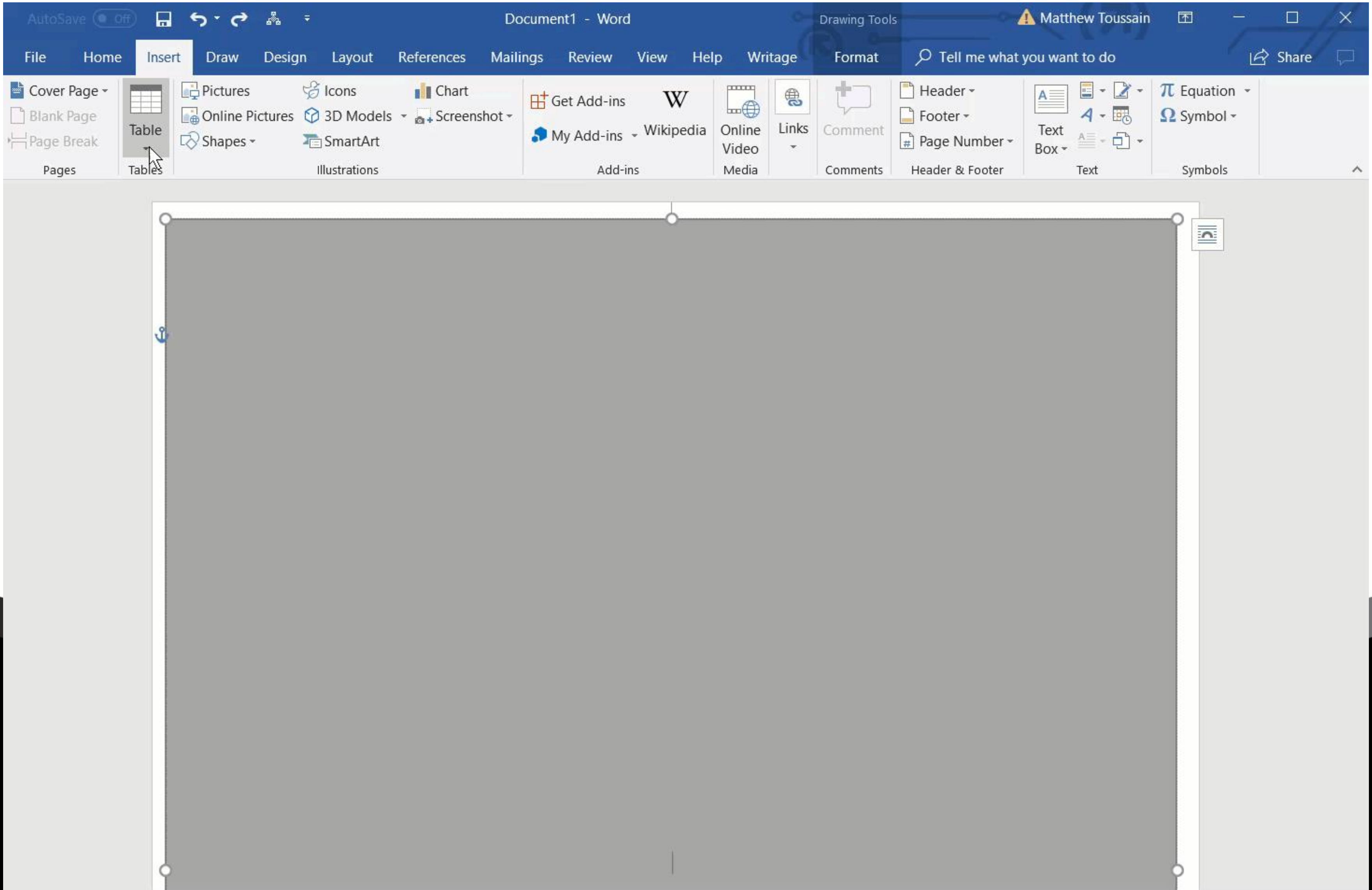
Pretend inferiority and encourage his arrogance.

The OODA Loop

- When the Threat can no Longer Trust their Own Tools Their ability to Decide has been Disrupted



Poisoning Documents



Other Traps

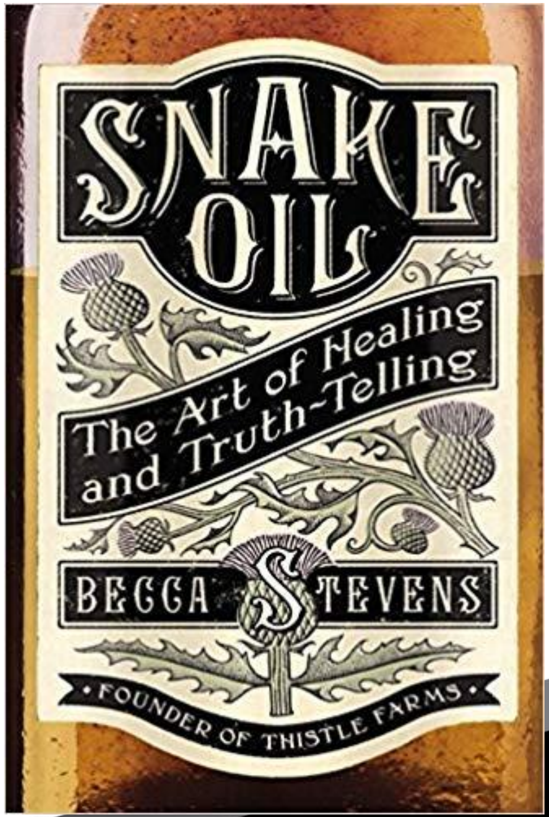
- Fake Login Portals
  - Site Cloning
- Robots.txt Disallowed References
- Port Traps
- Decoy Shared Drives
- Local Admin Access Group Traps
- Many More

Traps vs Honeypots

- Traps are Built to Poison Adversary Tactics to Produce Indicators of Compromise
  - Because the Trap is Based on Fake Information they are Difficult to Turn Against You
- Honeypots Collect Threat Intelligence by Providing a Low-Risk Target for Adversary Exploitation

Intel Gain/Loss

- Threat Intelligence is Vital, but Most Commercial Feeds are Pure Snake Oil
- Personalized Indicators of Compromise are the only Valid Ones
- In the Private Sector we are **Extremely** Quick to Burn our Threat Intelligence



Cyberspace Trapping

- Cyberspace Trapping is an aggressive strategy for defense
- The objective is not to block attacks
  - Blocking all attacks, you can see, leaves fewer options to identify the attacks you cannot
  - Poison the root of their methodology
  - Then follow the effects along the tree until you see fruit they are after and deny them.
- Engaging adversaries by tactic as opposed to tool is not a static, trivially bypass-able defense like AV signatures
- **When the opponent is uncertain they are vulnerable. When deceived they are weak. Cyberspace trapping about sowing confusion, disorder, and chaos along the attacker's path**

Questions?

Matthew Toussain | @0sm0s1z | http://github.com/0sm0s1z/CyberspaceTrapping