

Defending off the land: Agentless defenses available today

Jacob Torrey & Marco Slaviero
Black Hat EU 2024



The team



Jacob
Head of Labs



Casey
Sr. Sec Engineer



Pieter
Sr. Engineer



Leighton
Engineer



Roberto
Engineer



Marco
CTO

Agenda

- Background
- Defending Off the Land
- Primitives
- DoL Canarytokens
- What didn't pan out
- Caveats
- Future directions
- Takeaways

Defending off the land: Agentless defenses available today

Why should you care?

11+ techniques for detecting threat actors with no additional software.

This matters for places where EDR can't or won't.

Background

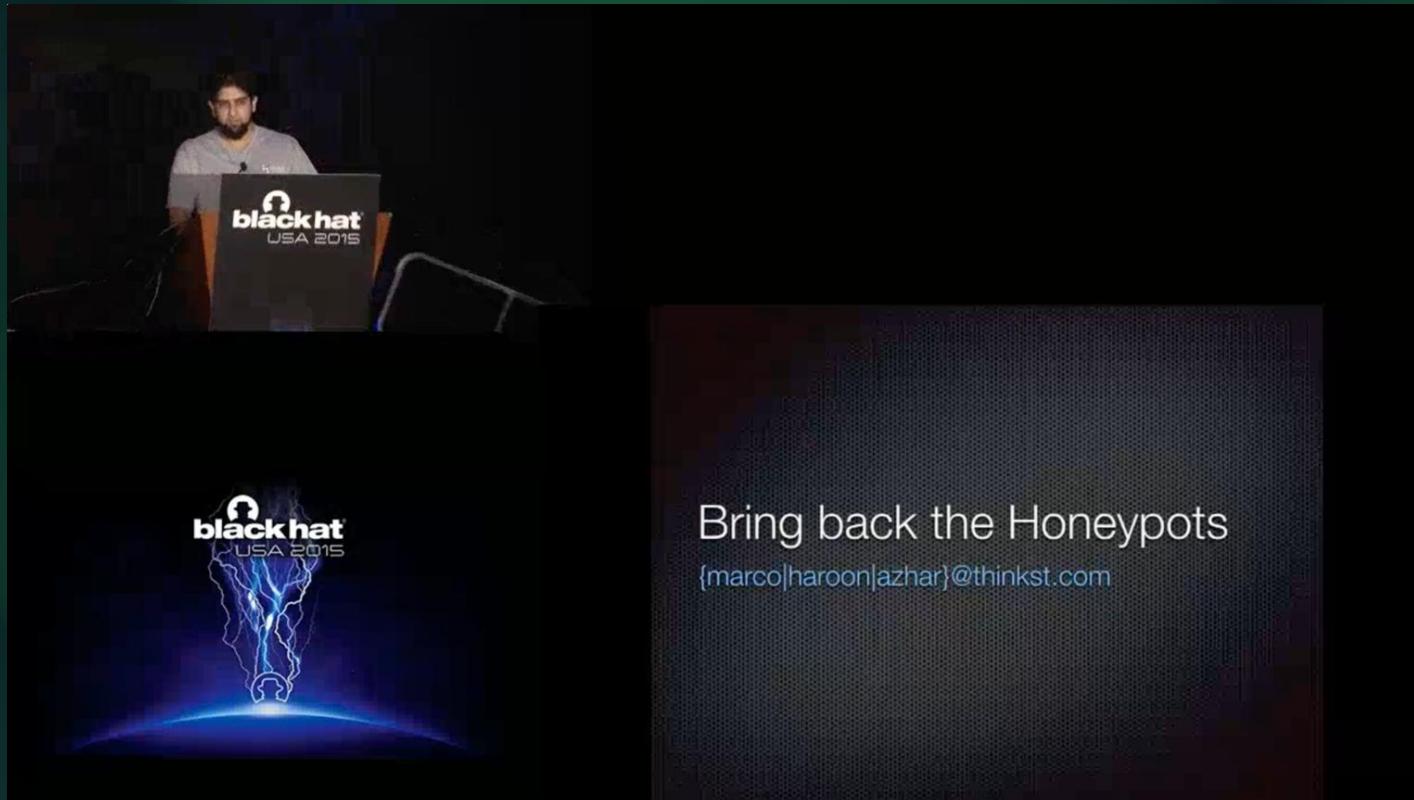
Bread and butter



THINKST
SCAPES

Q3 • 2024
<http://thinkst.com>

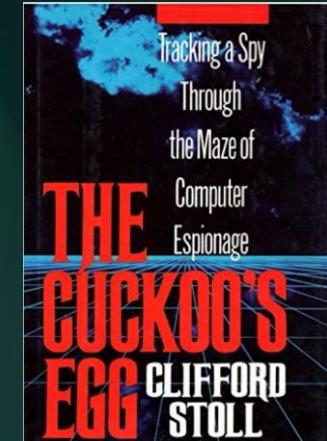
Deception is our game



Bring back the Honeypots
{marco|haroon|azhar}@thinkst.com

Honeypot aside

- Veteran idea
- Useful for breach detection
- Attacker research isn't useful (unless in volume)
- Parallel infrastructure



Canarytokens

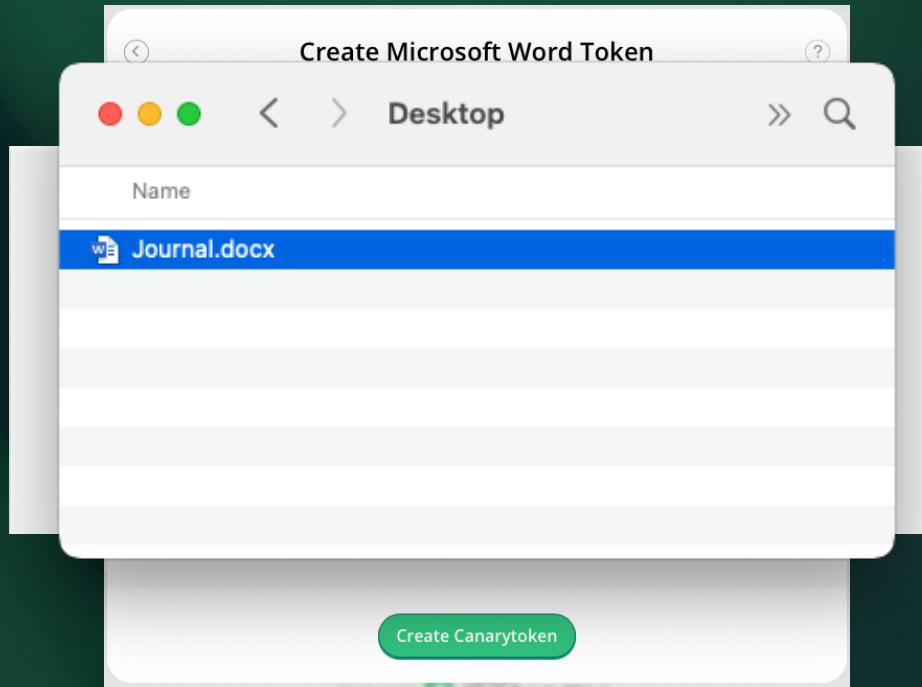
Canary tokens are simple

- Unique tags that can be embedded in a wide number of places.
 - Documents, emails, databases, file watchers, process watchers, LinkedIn, Bitcoin, Imgur
 - (And we've barely scratched the surface.)
- When that tag is triggered, you get an alert.



A screenshot of the Canarytokens website (canarytokens.org) displayed in a web browser. The page has a green header with the logo "CANARY TOKENS". Below the header, a large call-to-action button says "Create a Canarytoken. Deploy it somewhere." with the tagline "Know. When it matters." A search bar is present above two cards. The first card, titled "Web bug", shows an icon of a bug and text about getting an alert for URL visits. The second card, titled "DNS", shows an icon of a network graph and text about getting an alert for DNS resolution. A navigation menu with three horizontal bars is visible on the right side of the header.

Canarytokens example





Your Canarytoken was triggered

MS Word Canarytoken has been triggered by the Source IP



Reminder

Marco's desktop.

Canarytoken examples

 Your AWS keys Canarytoken is active!
Copy this credential pair to your clipboard to use as desired:

AWS token

```
[default]
aws_access_key_id = AKIAT4GVSAXZ00ZWBUMT
aws_secret_access_key = IH1uasukuILfr3an4z2w04vq+JPSRZyVc4Uh1XRh
output = json
region = us-east-2
```

This token is triggered when someone uses this credential pair to access AWS programmatically (through the API). The key is unique. i.e. There is no chance of somebody guessing these credentials.



Meeting attackers where they are (not)

Early IPS:



```
$ tcpdump -X -s 0 -i eth0 | grep '%252E'
```

Just not feasible

Meeting attackers where they are



Dr. Anton Chuvakin @anton_chuvakin

...

Have you ever seen your **#SIEM** *detect* a real intrusion or an incident that became a full-on IR case (i.e. this was a real, non-trivial malicious attack)?

Yes

48.1%

No

51.9%

418 votes · 4 days left

8:39 PM · Dec 3, 2024 · 6,108 Views

Meeting attackers where they are

Dr. Anton Chuvakin

@anton.chuvakin

Have you ever seen your #SIEM *detect* a real intrusion or an incident that became a full-on IR case (i.e. this was a real, non-trivial malicious attack)?

Yes	48.1%
No	51.9%

418 votes · 4 days left

8:39 PM · Dec 3, 2024 · 6,108 Views

 **NexusFuzzy** 
@NexusFuzzy

No but [@ThinkstCanary](#) Canaries do

10:52 PM · Dec 3, 2024 · 999 Views

  2  8  

Meeting attackers where they are

- Malicious actors expect endpoint monitoring or telemetry
- EDR cannot be installed on every machine
 - Too old
 - Too weird
 - Not yours
 - Competing agents
 - Hybrid environment
- What then?



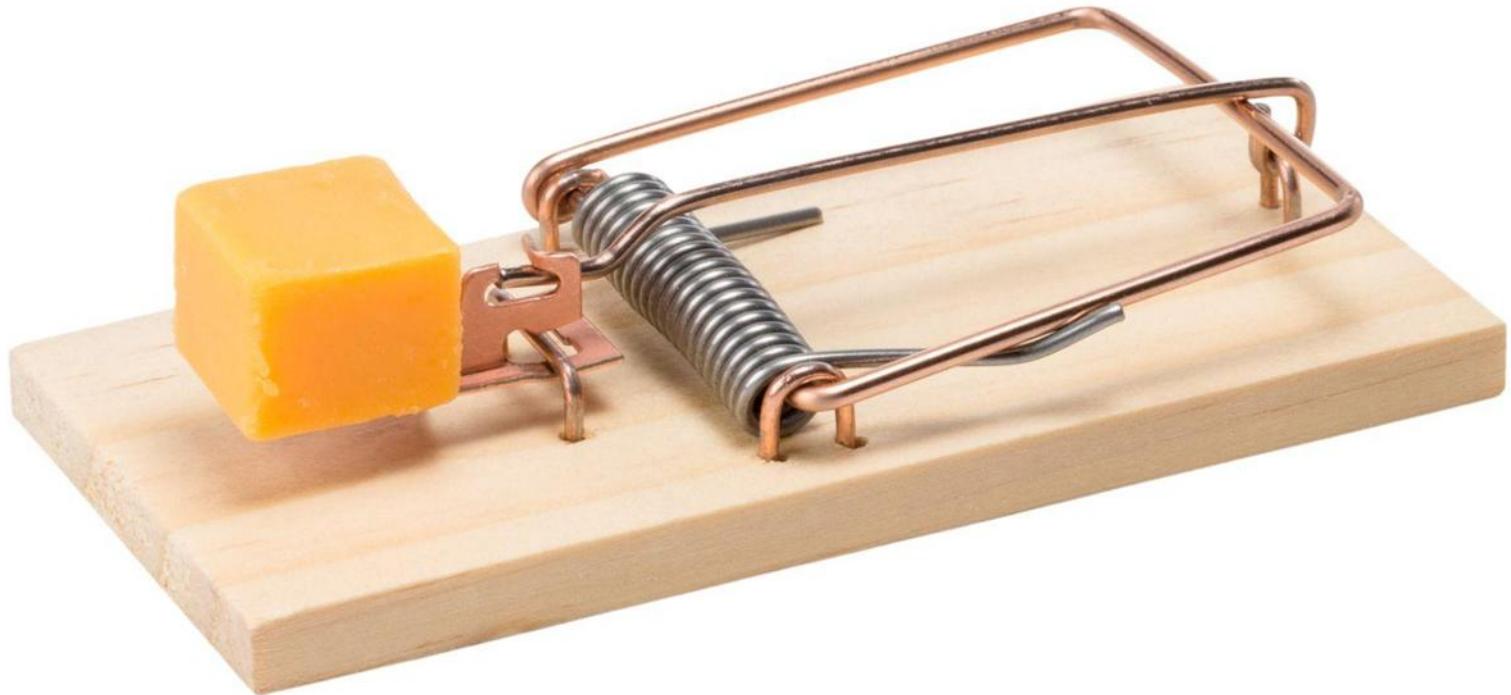
White House forms emergency team to deal with China espionage hack

The serious breach of telecommunications companies has now affected “about 10 or 12” firms, two people familiar with the investigation said.

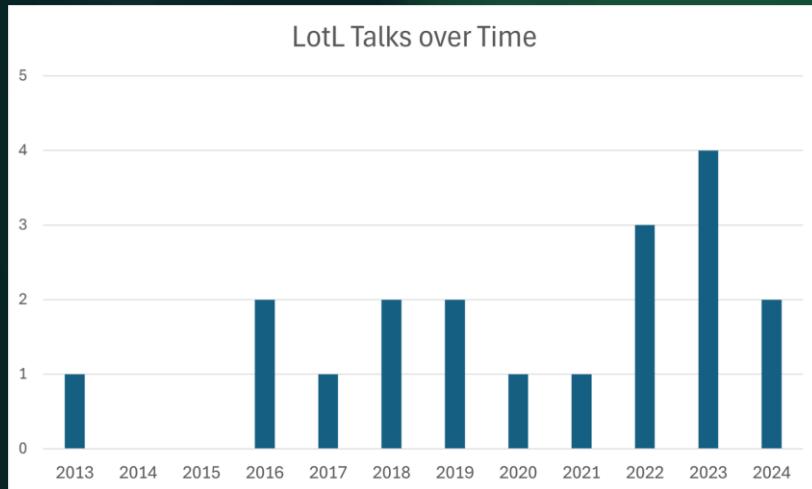
Exploiting the DRAM rowhammer bug to gain kernel privileges

How to cause and exploit
single bit errors

Mark Seaborn and Thomas Dullien



Attackers living off the land (LoL)



Windows 10

<https://citation.thinkst.com/>

Attacker LoL 1

```
"C:\Windows\system32\netsh.exe" interface portproxy add  
v4tov4 listenport=3390 listenaddress=REDACTED  
connectport=3389 connectaddress=REDACTED  
  
netsh advfirewall firewall add rule name="forwarded"  
protocol=TCP dir=in localip=REDACTED localport=3390  
action=allow  
  
Test-NetConnection -ComputerName REDACTED -Port 3390  
  
"C:\Windows\system32\netsh.exe" interface portproxy show all
```

Attacker LoL 2

```
C:\Windows\system32\sc(tasks.exe, /Create, /RU, NT  
AUTHORITY\SYSTEM, /tn, aytpnzc, /tr, regsvr32.exe -s  
"c:\Users\[REDACTED]\Desktop\7611346142\c2ba065654f13612ae63b  
ca7f972ea91c6fe97291caeaaa3a28a180fb1912b3a.dll", /SC, ONCE,  
/Z, /ST, 15:21, /ET, 15:33
```

A screenshot of an AP News article. The header features the AP logo and a navigation bar with links to World, U.S., Election 2024, Politics, Sports, Entertainment, Business, Science, Fact Check, Oddities, and Be Well. Below the header, the word "SCIENCE" is written in small capital letters. The main headline is "A faster spinning Earth may cause timekeepers to subtract a second from world clocks".

AP

WORLD U.S. ELECTION 2024 POLITICS SPORTS ENTERTAINMENT BUSINESS SCIENCE FACT CHECK ODDITIES BE WELL

SCIENCE

A faster spinning Earth may cause timekeepers to subtract a second from world clocks

QBOT, <https://www.elastic.co/security-labs/exploring-the-qbot-attack-pattern>

Attacker LoL 3

T1218.011

Rundll32

Rundll32 was back in the top 10 in 2023 as an attractive target for adversaries intent on blending in due to its necessity, capabilities, frequency of execution, and legitimacy.

PAIRS WITH THIS SONG 



#8

OVERALL RANK

10.3%

CUSTOMERS AFFECTED

326

THREATS DETECTED

Attacker LoL 4

BLEEPINGCOMPUTER

[NEWS ▾](#) [TUTORIALS ▾](#) [VIRUS REMOVAL GUIDES ▾](#) [DOWNLOADS ▾](#) [DEALS ▾](#) [VPN](#)

[Search Site](#)

Home > News > Microsoft > Microsoft-signed malicious Windows drivers used in ransomware attacks

Microsoft-signed malicious Windows drivers used in ransomware attacks

By [Lawrence Abrams](#)  December 13, 2022  06:10 PM  1

<https://www.bleepingcomputer.com/news/microsoft/microsoft-signed-malicious-windows-drivers-used-in-ransomware-attacks/>

LoL: Sysadmin + malicious intent = Threat actor

```
$ echo '%sudo ALL=(ALL) NOPASSWD: ALL' >> /etc/sudoers  
C:\> icacls C:\* /grant Everyone:(R) /t /c /q
```

Manage access

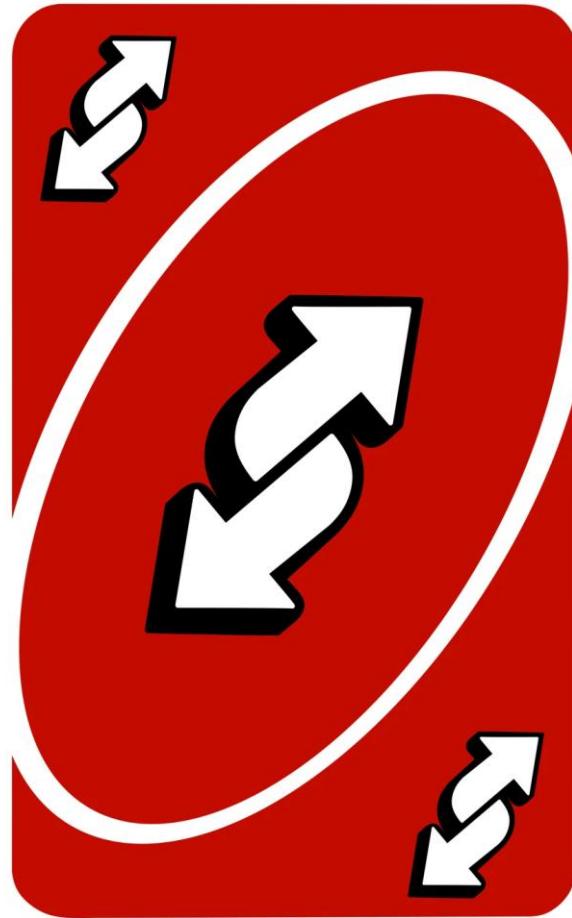
Create team Add people Add teams

Direct access Organization access

Access Type	Members	Role	Action
Direct access	2 members	Role: admin	
Organization access	4 members	Role: admin	
Organization access	3 members	Role: admin	

The screenshot shows a user interface for managing access. It has tabs for 'Direct access' and 'Organization access'. Under 'Organization access', there are three entries, each with a checkbox, a user icon, a blurred email address, and a member count. To the right of each entry is a box containing 'Role: admin' and a red delete icon. The third entry's row is highlighted with a red rectangle.

Defending off the land (DoL)



What is defending off the land?

- Lightweight and built-in
- Agentless detection techniques leveraging already present tools
 - I.e. no installs
- Can be deployed to systems where EDR can't be
 - Appliances / 3rd party vendor systems / non-enterprise assets
- Free and extensible
- Includes much deception, a bit of scripting
- Is it new?



briankrebs ✅
@briankrebs

...

Pro tip for the "but how do we protect ourselves?" folks. DarkSide ransomware, like many other strains, will not install on systems where certain Cyrillic keyboard and other scripts are already installed. So, install the Russian keyboard. You don't have to use it.

7:01 PM · May 11, 2021

Russian / GoRussian.reg □



cgytoder Update GoRussian.reg

Code

Blame

8 lines (6 loc) · 193 Bytes

```
1 Windows Registry Editor Version 5.00
2
3 [HKEY_LOCAL_MACHINE\SYSTEM\Keyboard Layout\Preload]
4 "1"="00000419"
5
6 [HKEY_USERS\.DEFAULT\Keyboard Layout\Preload]
7 "1"="00000409"
8 "2"="00000419"
```

This sounds like work

- Yes, products won't save you
- An empowered experienced sysadmin is worth their weight in gold

Why Windows only?

- Lots of baked-in features
- Most targeted platform
- Certainly options for other platforms, but we don't go there

Where do we get ideas from?



John Lambert
@JohnLaTwC

If you shame attack research, you misjudge its contribution. Offense and defense aren't peers.
Defense is offense's child.

1:35 PM · Mar 9, 2014 · Twitter Web Client

- DFIR reports (especially <https://thedefirreport.com/>)
- Papers (<https://citation.thinkst.com>)
- Visibility gaps

Background is done

The Map

1. **Primitives**
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise

Primitives

DNS & HTTP Web bugs

- Most Canarytokens are built on a unique hostname or URL
 - If they are accessed/resolved, someone is snooping

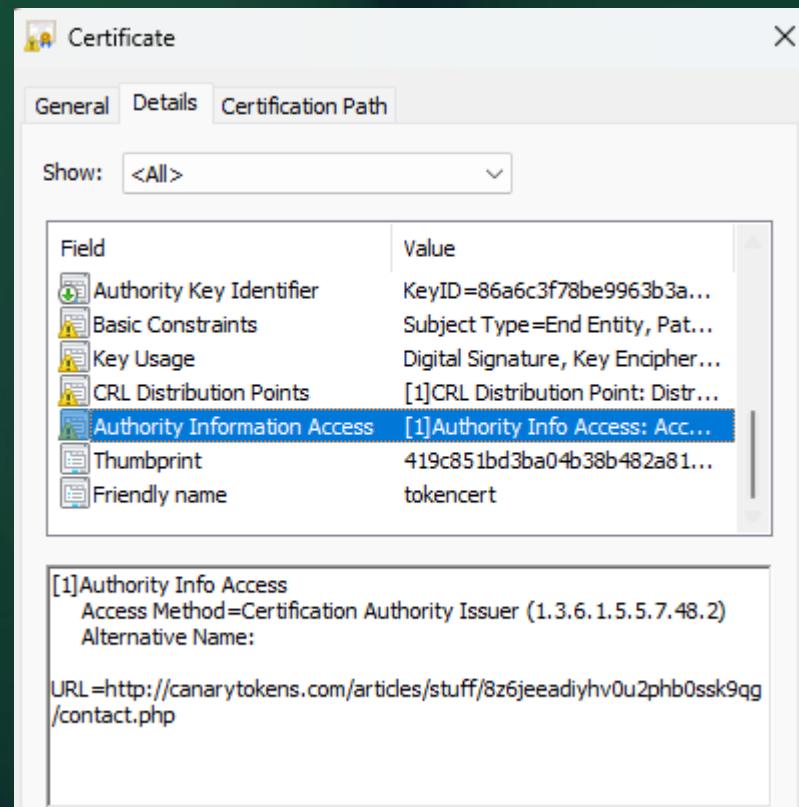
The screenshot shows a web-based configuration interface for generating a Canarytoken. It consists of two main sections:

- Canarytoken URL:** This section contains a text input field with the URL `http://canarytokens.com/feedback/about/traffic/w84gfc2p87z1mjp8ojyiixp6o/su`. To the right of the input is a green circular icon with a white clipboard symbol.
- Remember, it gets triggered whenever someone requests the URL.** This is a descriptive note below the URL input.
- Canarytoken hostname:** This section contains a text input field with the hostname `u2p8usnx77i5635tdcuaijb1m.canarytokens.com`. To the right of the input is a green circular icon with a white clipboard symbol.
- Remember, it gets triggered whenever someone performs a DNS lookup of the hostname.** This is a descriptive note below the hostname input. At the end of this note is a link labeled [Need more tips?](#) in green text.

- Simple way to add alerting is to embed DNS/HTTP token into script or action that triggers with additional information

Certificate AIA & CryptoAPI

- Authority Information Access is an x.509 field with a URL to the parent certificate authority
- In order to validate an unknown leaf certificate, Windows CryptoAPI fetches the URL
- Create a TLS certificate with an AIA of a web Canarytoken URL!



Scripting & dynamic compilation

- PowerShell allows for accessing Win32 and .NET APIs
- It also allows for running a string containing C#
 - Compiled into memory as a new type from dynamically-generated string
- Allows for very powerful capabilities to be deployed as a PS script
 - No explicit compilation step
 - No compiler suite needed

Windows Events and Event Triggers

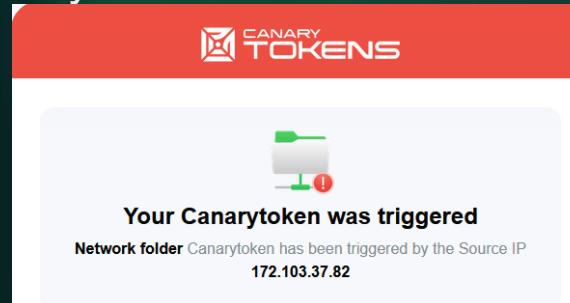
- Windows tracks 1000s of events across OS and user-space
 - Many must be enabled
- Task Scheduler can use Event as Trigger
 - Provides Event XML as argument to task Action

Alerting primitives

- PowerShell can pop toast/balloon notifications for local alerting



- Canarytokens.org is a handy site to handle the “downstream” aspects of alerts
 - Robust listeners
 - Good reputation email
 - Webhook support
 - Affordable ;)



In the capabilities we present here, we use a combination of the above

DoL Canarytokens

We'll go through these quickly

The Map

1. Primitives
2. Local threat actor detections
 - a. **Sensitive command detection**
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise

Sensitive command token

- Alerts on execution of a sensitive command (e.g., klist)
 - Rarely used benignly
 - DFIR reports show they are frequently used by attackers to orient themselves
 - Command doesn't have to exist at deployment time
- Registry key that sets PowerShell script to be run with target process
- Resolves a token domain that also encodes the computer and user names
 - Can be pushed out broadly via GPO

```
PS C:\Users\casey\Desktop> reg import .\canarytoken.reg  
The operation completed successfully.  
PS C:\Users\casey\Desktop> |
```

```
PS C:\Users\casey\Desktop> nltest.exe /?  
Usage: nltest [/OPTIONS]  
  
/SERVER:<ServerName> - Specify <ServerName>  
  
/QUERY - Query <ServerName> netlogon service  
/REPL - Force partial sync on <ServerName> BDC  
/SYNC - Force full sync on <ServerName> BDC  
/PDC_REPL - Force UAS change message from <ServerName> PDC  
  
/SC_QUERY:<DomainName> - Query secure channel for <Domain> on <ServerName>  
/SC_RESET:<DomainName>[\<DcName>] - Reset secure channel for <Domain> on <ServerName> to <DcName>  
/SC_VERIFY:<DomainName> - Verify secure channel for <Domain> on <ServerName>  
/SC_CHANGE_PWD:<DomainName> - Change a secure channel password for <Domain> on <ServerName>  
/DCLIST:<DomainName> - Get list of DC's for <DomainName>  
/DCNAME:<DomainName> - Get the PDC name for <DomainName>  
/DSGETDC:<DomainName> - Call DsGetDcName /PDC /DS /DSP /GC /KDC  
    /TIMESERV /GTIMESERV /WS /NETBIOS /DNS /IP /FORCE /WRITABLE /AVOIDSELF /LDAPONLY /BACKG /DS_6 /DS_8 /DS_9 /DS_10  
    /KEYLIST /TRY_NEXT_CLOSEST_SITE /SITE:<SiteName> /ACCOUNT:<AccountName> /RET_DNS /RET_NETBIOS  
/DSGETDC:<DomainName> - Call DsGetDcOpen/Next/Close /PDC /GC  
    /KDC /WRITABLE /LDAPONLY /FORCE /SITESPEC  
/DSGETFTI:<DomainName> - Call DsGetForestTrustInformation  
    /UPDATE_TDO
```

Run nltest & alert us behind the scene, quick and easy :)

CASEYBCD8.UN.casey.CMD.pvd6nto02timeqnrp8675309.canarytokens.com

Canarytoken triggered

ALERT

A DNS Canarytoken has been triggered by the Source IP 192.168.16.1. Please note that the source IP refers to a DNS server, rather than the host that triggered the token.

Basic Details:

Channel	DNS
Time	2022-12-30 16:37:53 (UTC)
Canarytoken	0mpmy260rq80sillue12345
Token Reminder	Create Token to monitor for nltest.exe at branch offices. This should be a rare command (This token was created to monitor the execution of: nltest.exe)
Token Type	cmd
Source IP	192.168.16.1
Sensitive Command Information	User casey executed "nltest.exe" on the host caseyce69

Canarytoken Management Details:

The Map

1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. **Scheduled task monitor**
 - c. Registry monitor
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise



Scheduled task monitor

- Scheduled task that alerts on suspicious creation of new scheduled tasks
 - Running powershell.exe, cmd.exe, mshta.exe, .bat files, etc.
 - Process that is writable by the user
 - Arguments in user-writable user
- Scheduled task is triggered on Windows event 4698 (new scheduled task)

Attacker LoL 2

```
C:\Windows\system32\sctasks.exe, /Create, /RU, NT AUTHORITY\SYSTEM, /tn, ayttpnzc, /tr, regsvr32.exe -s "c:\Users\[REDACTED]\Desktop\7611346142\c2ba065654f13612ae63b ca7f972ea91c6fe97291caeaaa3a28a180fb1912b3a.dll", /SC, ONCE, /Z, /ST, 15:21, /ET, 15:33
```

A faster spinning Earth may cause timekeepers to subtract a second from world clocks

QBOT, <https://www.elastic.co/security-table/exploring-the-qbot-attack-pattern>



Scheduled tasks

- Scheduling tasks
 - Running tasks
 - Processing tasks
 - Arguing about tasks
- Scheduling tasks

YO DAWG I HEARD YOU LIKE SCHEDULED TASKS

SO I MADE A SCHEDULED TASK
TO MONITOR FOR NEW SCHEDULED TASKS

imgflip.com

```
cs.exe, /Create, /RU, NT
cpnzc, /tr, regsvr32.exe -s
bp\7611346142\c2ba065654f13612ae63b
9a28a180fb1912b3a.dll", /SC, ONCE,
```

A faster spinning Earth may cause
timekeepers to subtract a second from
world clocks

Administrator: Windows PowerShell

```
PS C:\Users\JacobTorrey> |
```

The Map

1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. **Registry monitor**
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise



Registry monitor

- Registry is a common feature for LotL
 - Persistence with/without files
 - Disable security protections
 - Enable remote access
- Monitor the ~80 most security-sensitive keys for changes
 - Alert when they change
 - Local balloon notification or via canarytokens.org
 - Drawn from Elastic's detection rules
- PowerShell script to access the Registry
 - Can be automatically run periodically

	Name	Type	Data
	(Default)	REG_SZ	(value not set)
	{3D644C9B-1FB8-4f30-9B45-...	REG_EXPAND_SZ	%PUBLIC%\Downloads
	Common AppData	REG_EXPAND_SZ	%ProgramData%
	Common Desktop	REG_EXPAND_SZ	%PUBLIC%\Desktop
	Common Documents	REG_EXPAND_SZ	%PUBLIC%\Documents
	Common Programs	REG_EXPAND_SZ	%ProgramData%\Microsoft\Windows\Start Menu...
	Common Start Menu	REG_EXPAND_SZ	%ProgramData%\Microsoft\Windows\Start Menu...
	Common Startup	REG_EXPAND_SZ	%ProgramData%\Microsoft\Windows\Start Menu...
	Common Templates	REG_EXPAND_SZ	%ProgramData%\Microsoft\Windows\Templates
	CommonMusic	REG_EXPAND_SZ	%PUBLIC%\Music
	CommonPictures	REG_EXPAND_SZ	%PUBLIC%\Pictures
	CommonVideo	REG_EXPAND_SZ	%PUBLIC%\Videos

The Map

1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. **Service monitor**
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise



Windows Service token

- A common post-exploitation technique is to disable security and backup services (ATT&CK T1489)
- Create shell services that alert on stopping
- PowerShell that dynamically creates Service and registers a pipe to PowerShell
 - Once started, it will auto-start on boot
 - If stopped, it will trigger an alert

Sign in

Alerts History

https://canarytokens.org/nest/history/06ff17b6024cabb44b5274de4a553640/b9mjavxydfjcpk3fcu12dd1t2

CANARY TOKENS

NEW CANARYTOKEN ALERTS HISTORY MANAGE DOCUMENTATION THINKST CANARY

Alerts History



Web bug Canarytoken ID: b9mjavxydfjcpk3fcu12dd1t2

Alerts list

There are no alerts for this Canarytoken.



Name	Description	Status	Startup Type	Log
Internet Connection Sharin...	Provides ne...	Running	Manual (Trig...	Loc
Inventory and Compatibilit...	This service ...	Running	Manual	Loc
IP Helper	Provides tu...	Running	Automatic	Loc
IP Translation Configuratio...	Configures ...	Manual (Trig...	Loc	
IPsec Policy Agent	Internet Pro...	Manual (Trig...	Net	
Kerberos Local Key Distribut...	This service ...	Manual	Loc	
KtmRm for Distributed Trans...	Coordinates...	Manual (Trig...	Net	
Language Experience Service	Provides inf...	Manual	Loc	
Link-Layer Topology Discov...	Creates a N...	Manual	Loc	
Local Profile Assistant Service	This service ...	Manual (Trig...	Loc	
Local Session Manager	Core Windo...	Running	Automatic	Loc
MalwareBytes Anti-Malware	Helps prote...	Running	Automatic	Loc
McpManagementService	Universal Pr...	Manual	Loc	
MessagingService_1047c6	Service sup...	Manual (Trig...	Loc	
Microsoft Account Sign-in ...	Enables use...	Manual (Trig...	Loc	
Microsoft App-V Client	Manages A...	Disabled	Loc	
Microsoft Cloud Identity Se...	Supports int...	Manual	Net	
Microsoft Cloud Managed ...	Microsoft C...	Running	Automatic (D...	Loc
Microsoft Defender Antiviru...	Helps guard...	Running	Manual	Loc
Microsoft Defender Antiviru...	Helps prote...	Running	Automatic	Loc
Microsoft Defender Core Se...	Monitors th...	Running	Automatic	Loc

#Ad

Did you know some of the best security teams in the world run Thinkst Canary?

Find out →

The Map

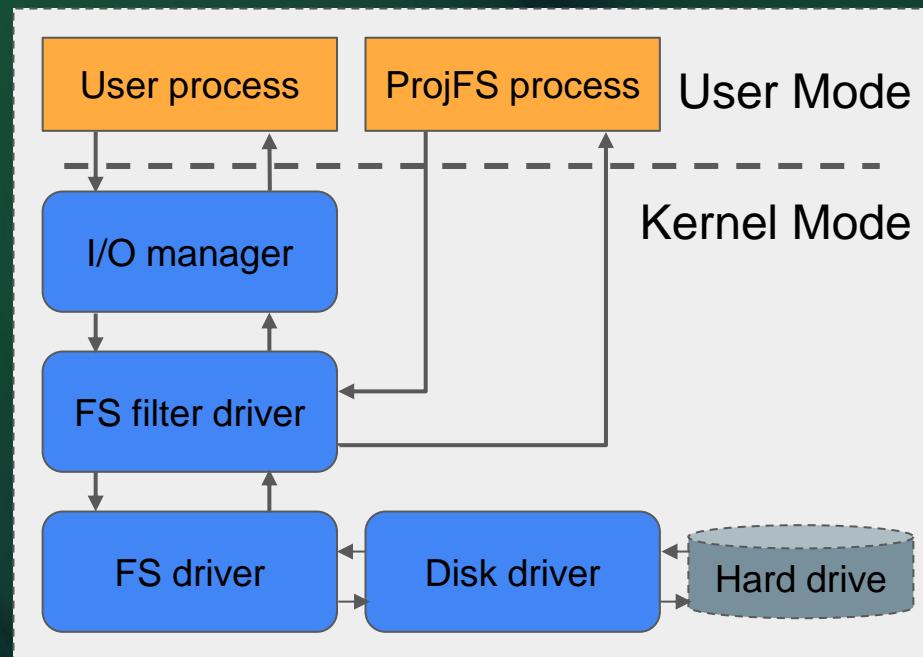
1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. Service monitor
 - e. **File access monitoring (ProjFS)**
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise

Monitoring file access

OS Feature	Implementation	Performance impact	File content monitoring	Scalability
ProjFS	User mode & MS driver	Low	Yes	High
File System Watcher	User mode	Moderate	No	Limited
Object Auditing / SACLs	OS subsystem	High	Yes	Fair
Controlled Folder Access	OS-\$\$ / MSFT Defender	Low	Low	High

Windows Projected File System

- ~FUSE for Windows
- API to manipulate the file system
 - Non-admin
 - User mode
 - C#, Python, or even PS
- Used to create file structures on-demand
 - RegistryFS
 - Git
- Even used for file tar pits!



We've made this easy to use and effective



Get an alert when a attacker accesses a file in the fake file system.

Create Canarytoken

Create Windows Fake File System Token



Canarytoken Settings

Where will this directory be placed?
C:\Secrets

Create (fake) files for the following Industry/Sector
Home Network

Mail me here when the alert fires
alert@example.com

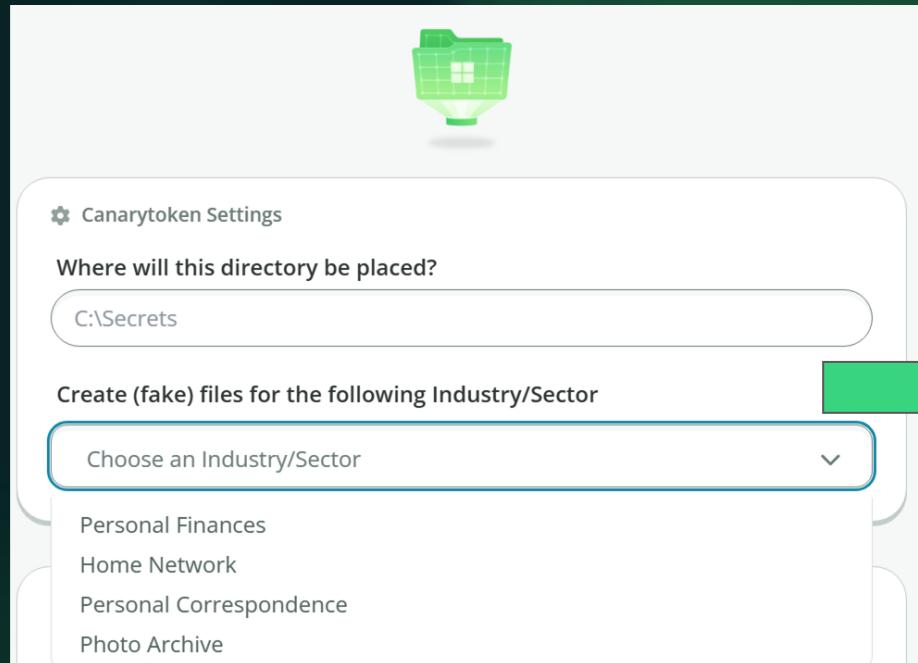
Remind me of this when the alert fires
Testing ProFS

Notify me here when the alert fires
<http://your-webhook-url.com>

Add Webhook Notification

Create Canarytoken

We provide some files to start you off, easy to change



A large green arrow points from the right side of the user interface towards the file list on the right.

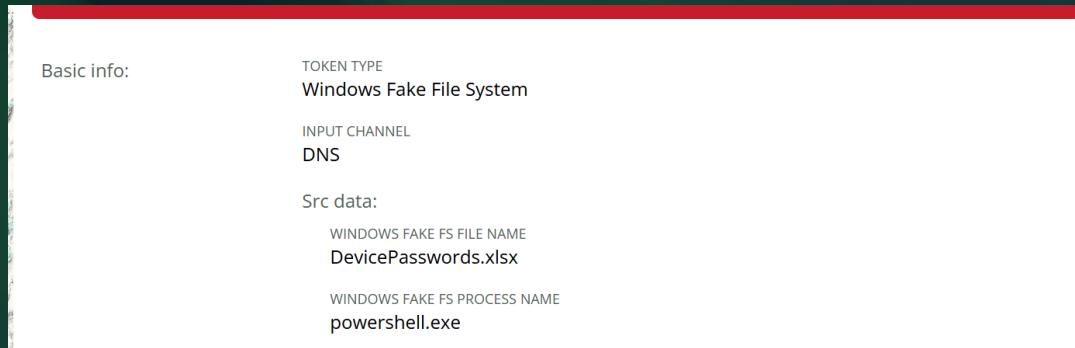
This PC > Local Disk (C:) > Secrets > HomeNetwork	
Name	Date modified
ISP	5/15/2024 3:04 PM
NetworkDevices	11/22/2024 5:04 PM
NetworkDiagram	4/30/2024 10:04 PM
Security	8/18/2024 9:04 PM

Alert on file open or copy

```
Directory: C:\Secrets\HomeNetwork\Security

Mode          LastWriteTime      Length Name
----          -----          ---- 
----          7/25/2024 3:04 AM        1652 DevicePasswords.xlsx
----          11/10/2024 1:04 PM       30926 FirewallRules.docx
----          3/2/2024  9:04 PM       41708 SecurityChecklist.pdf

PS C:\Secrets\HomeNetwork\Security> cat .\DevicePasswords.xlsx
This is the content of DevicePasswords.xlsx
PS C:\Secrets\HomeNetwork\Security> |
```





SMB remote sessions - on remote open | copy

```
PS C:\Users\casey\Documents> .\CanaryFs-SMB.exe c:\SecretShare $(Get-Content test_file.csv -Raw) x4ka4j8my0326k2as7u7b6ej8.canarytokens.com true FakeFSShare
```

The screenshot illustrates a workflow for managing SMB shares on a Windows system and interacting with them via a macOS application.

Windows Computer Management:

- Left pane:** Shows the navigation tree with "Computer Management (Local)" selected, followed by "System Tools" and "Shared Folders". Under "Shared Folders", "Shares" and "Sessions" are listed.
- Right pane:** A table listing shares. The "FakeFSShare" row is highlighted with a blue background. The table columns are: Share Name, Folder Path, Type, # Client Connections, and Description. The "FakeFSShare" entry has the following details:
 - Share Name: FakeFSShare
 - Folder Path: c:\SecretShare
 - Type: Windows
 - # Client Connections: 0
 - Description: Created by SmbManager
- Actions pane:** Shows "Shares" and "FakeFSShare" with "More Action..." buttons.

MacOS Finder:

- Left sidebar:** Shows the file system structure with "FakeFSShare" mounted at the root, "Macintosh HD", and "Network".
- Central pane:** Shows a "Project" folder containing subfolders: assets, docs, secrets, src, and tests. The "secrets" folder is selected and highlighted with a blue background.
- Right pane:** Shows additional subfolders: cloud_keys, passwords, and ssh_keys.

Green arrows point from the "FakeFSShare" entry in the Windows Computer Management table to the "FakeFSShare" mount point in the macOS Finder sidebar, and from the "secrets" folder in the macOS Finder central pane back to the "FakeFSShare" entry in the Windows Computer Management table.

Testing results

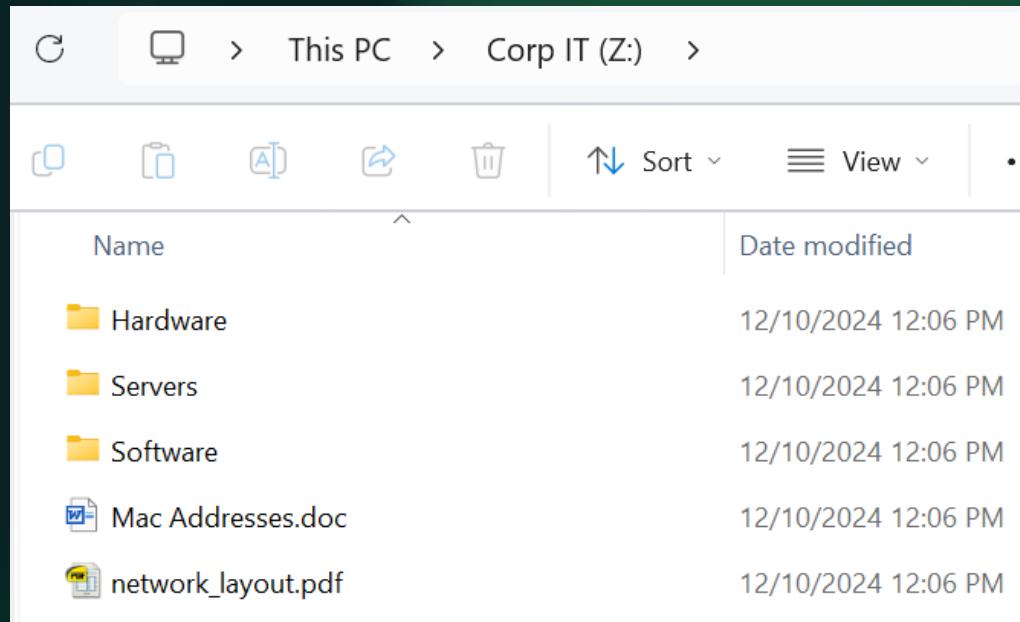
<u>Tool Name</u>	<u>Allows Enumeration</u>	<u>Detects on File Open/Copy</u>
ShareFinder	✓	✓
FRansom	✓	✓
Snaffler	✓	✓
Get-FileHash		✓
Compress (7z/Zip)		✓
Full AV scan	✓	✓
Windows Search indexer	✓	✓

The Map

1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. **File access monitoring (WebDAV)**
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise

Network mount token

- Network drives are common
 - Z: → internal file share
- We built a lightweight WebDAV server in Cloudflare workers
 - Fast responses
- Users map a drive to a WebDAV URL with custom credentials
- If the drive contents are accessed, you get an alert



Your Canarytoken was triggered

Network folder Canarytoken has been triggered by the Source IP
165.225.10.148

Reminder
Framework network mount

Source IP
165.225.10.148

Date 2024/12/06 **Time** 21:59 UTC

File Path /network_layout.pdf

WebDAV Client User-Agent Microsoft-WebDAV-MiniRedir/10.0.26100

The Map

1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. **RDP access**
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise



RDP token

- Windows ships with RDP service, catch people attempting to login with RDP
 - Popular lateral movement technique
 - Client is also built-in
- Enable RDP service and configure with a TLS certificate that points to a token URL
- Add all users to a group that is denied access to RDP sessions
- Clients verify TLS certificate, trigger alert, and even with credentials are not given a session

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Users\User> cd .\Documents\DOL\  
PS C:\Users\User\Documents\DOL> ./install.ps1  
This script will install the RDP Canarytoken to your system  
It will:  
- Install a tokened certificate into your certificate store  
- Configure the RDP service to use that certificate for RDP connections  
- Confirm if you want to disable RDP logins for all users  
- Enable the RDP service and open the RDP port on the local firewall
```

Install RDP Canarytoken
Would you like to continue and install the RDP Canarytoken?
[Y] Yes [N] No [?] Help (default is "N"): y
Installing the certificate...
Setting the RDP service to use that certificate
The operation completed successfully.

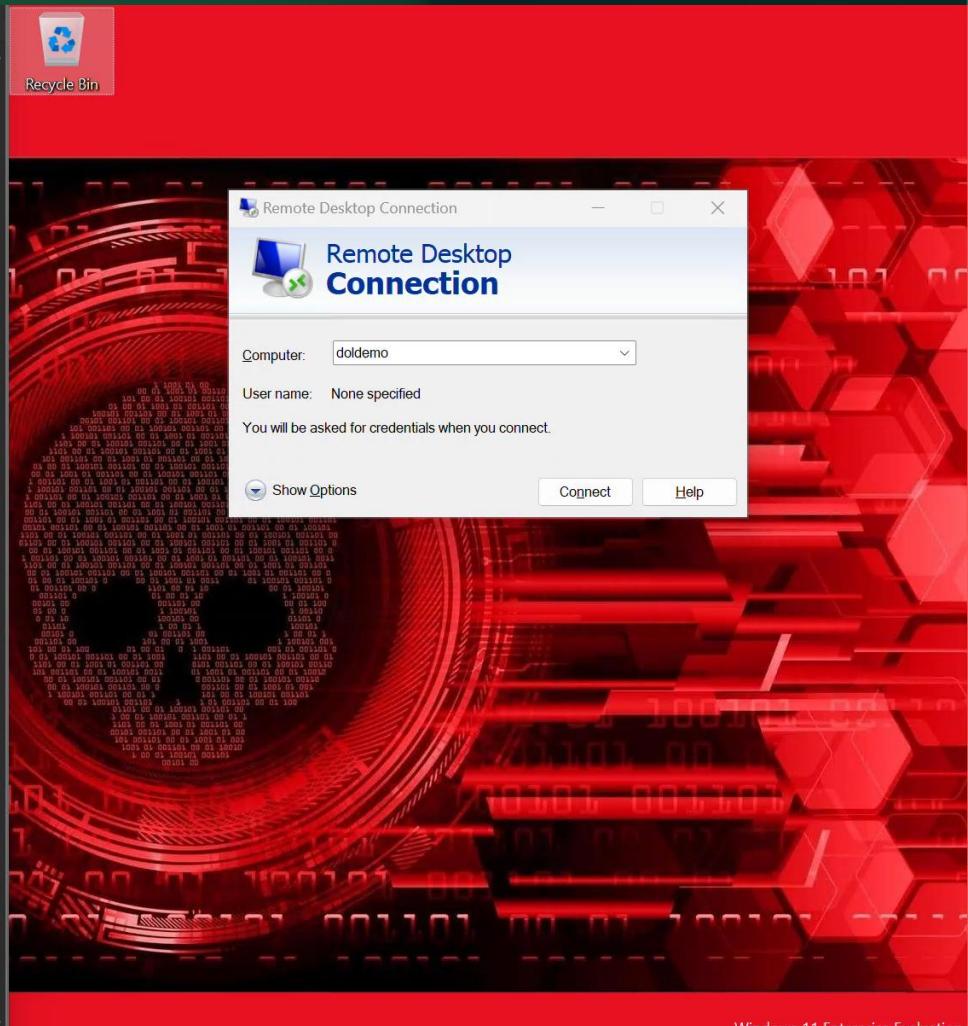
Disable RDP access for all users
This will prevent any non-local logins, skip this for VMs or cloud-based systems
[Y] Yes [N] No [?] Help (default is "N"): n
Updating policy...

Computer Policy update has completed successfully.

Enabling RDP service
The operation completed successfully.

Updated 3 rule(s).
Ok.

```
PS C:\Users\User\Documents\DOL> whoami  
doldemo\user  
PS C:\Users\User\Documents\DOL>
```



The Map

1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. **WinRM access**
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise



WinRM token

- Windows ships with a management service, WinRM
 - Popular lateral movement technique (PSRemoting)
 - Client is also built-in
- Enable HTTPS WinRM service and configure with a TLS certificate that points to a token URL
- Install a SDDL that denies WinRM logins
- Clients verify TLS certificate, trigger alert, and even with credentials are not given a session

```
Administrator: Windows Powx + v - o x
PS C:\Users\User\Documents\DOL> .\install-winrm.ps1
This script will install the WinRM Canarytoken to your system
It will:
- Install a tokened certificate into your certificate store
- Configure the WinRM service to use that certificate for HTTPS connections
- Disable WinRM logins for all users
- Enable the WinRM service and open the WinRM HTTPS port on the local firewall
all

Install WinRM Canarytoken
Would you like to continue and install the WinRM Canarytoken?
[Y] Yes [N] No [?] Help (default is "N"): y
Installing the certificate...
Setting the WinRM service to use that certificate
Enabling WinRM service
WinRM is not set up to receive requests on this machine.
The following changes must be made:

Start the WinRM service.
Set the WinRM service type to delayed auto start.

WinRM has been updated to receive requests.

WinRM service type changed successfully.
WinRM service started.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Enable the WinRM firewall exception.
Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

WinRM has been updated for remote management.

WinRM firewall exception enabled.
Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
ResourceCreated
    Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
```

```
Windows PowerShell x + v - o x
PS C:\Users\User> whoami
attackerdemo\user
PS C:\Users\User> winrs -r:https://doldemo:5986 -u:"Savvy Defender" -p:demodemo whoami


Windows 11 Enterprise Evaluation
```

The Map

1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. **Hyper-V honeypots**
 - d. AD logins
4. Cloud threat actor detections
 - a. IdP compromise



Local non-risky honeypots with Hyper-V

- Windows 11 includes Hyper-V by default¹
- Run a Linux honeypot VM on the machine
- Use Windows NAT to redirect incoming traffic to the honeypot
 - windows:22 -> honeypot:22 (fake that you're running SSH)
 - windows:80 -> honeypot:80 (run a fake "local" website)
 - windows:3389 -> honeypot:3389 (see when people try to login to your RDP)
- Honeypot communicates with a Windows monitoring script via Hyper-V KVPs to show alerts

¹ For Enterprise and Pro editions, on CPUs with VM extensions

Attacker LoL 1

```
"C:\Windows\system32\netsh.exe" interface portproxy add v4tov4 listenport=3390 listenaddress=REDACTED connectport=3389 connectaddress=REDACTED  
netsh advfirewall firewall add rule name="forwarded" protocol="TCP" dir="in" localip=REDACTED localport=3390 action=allow  
Test-NetConnection -ComputerName REDACTED -Port 3390  
"C:\Windows\system32\netsh.exe" interface portproxy show all
```

Ransomware Incident: <https://theadline-report.com/2024/04/29/ransomware-in-29-days/>

192.168.1.59

OpenCanary.ps1 X + ⚙

File Edit View

```
$vmNetmask = "24"
$vmIpAndNetmask = "$vmIp/$vmNetmask"
$vmGw = "172.16.10.254"
$vmDns = "8.8.8.8"
$canarySettings = '{
    "ssh.enabled": true,
    "ftp.enabled": true,
    "portscan.enabled": true,
    "redis.enabled": true,
    "mysql.enabled": true,
    "mssql.enabled": true,
    "telnet.enabled": true,
    "vnc.enabled": true
}'
$portMapping = @{
    21 = 21
    22 = 22
    23 = 23
    6379 = 6379
    5000 = 5000
    3306 = 3306
    1433 = 1433
}
$eventSource = "OpenCanary"

function AddKvpItem {
    [cmdletbinding()]
    Param (
        [string]
        $vmName,
        [string]
        $key,
        [string]
        $value
    )
}
```

Ln 27, Col 16 | 12,751 characters 100% Unix (LF) UTF-8

67°F Partly sunny

Search

6:07 AM 12/5/2024

The Map

1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. **AD logins**
4. Cloud threat actor detections
 - a. IdP compromise



AD login token

```
PS > type .\creds.txt
Username: Marcos
Password: OothaY8u
```

- Scheduled task that alerts on failed AD login attempts for token usernames
 - Make fake usernames
 - Drop their “credentials” in places
 - Alert upon usage

Attacker LoL 2

```
C:\Windows\system32\schtasks.exe, /Create, /RU, NT AUTHORITY\SYSTEM, /tn, ayttppnzc, /tr, regsvr32.exe -s "c:\Users\[REDACTED]\Desktop\7611346142\c2ba065654f13612ae63bca7f972ea91c6fe97291caeaaa3a28a180fb1912b3a.dll", /SC, ONCE, /Z, /ST, 15:21, /ET, 15:33
```

A faster spinning Earth may cause timekeepers to subtract a second from world clocks

QBOT, <http://www.elastic.co/security-table/exploring-the-qbot-attack-pattern>

Alerts History



Web bug Canarytoken ID: [REDACTED]

Alerts list

Download list

CSV

JSON

Date: December 7, 2024 at 1:26:23
PM
IP: [REDACTED]

Channel: HTTP

Date: December 7, 2024 at 1:26:23
PM
IP: [REDACTED]

Channel: HTTP

X

USER-AGENT

Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US)
WindowsPowerShell/3.0

Request args:

USERNAME

MarcoS

WORKSTATION NAME

WORKSTATION IP

RECORD ID

20916402

MACHINE NAME

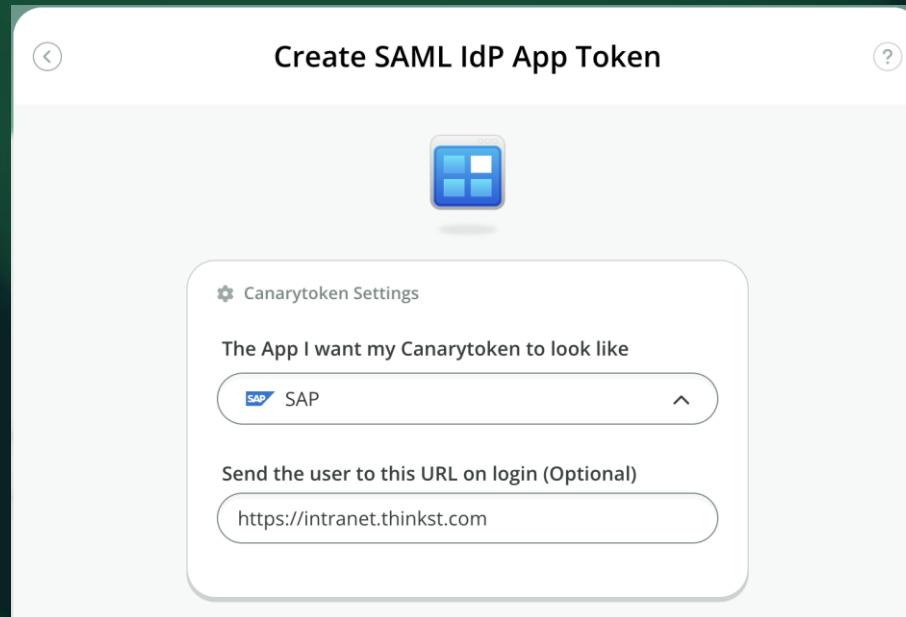
win2k19-domainsrv.corp.thinkst.com

The Map

1. Primitives
2. Local threat actor detections
 - a. Sensitive command detection
 - b. Scheduled task monitor
 - c. Registry monitor
 - d. Service monitor
 - e. File access monitoring (ProjFS)
 - f. File access monitoring (WebDAV)
3. Remote threat actor detections
 - a. RDP access
 - b. WinRM access
 - c. Hyper-V honeypots
 - d. AD logins
4. Cloud threat actor detections
 - a. **IdP compromise**

IdP token

- “Identity is the new {perimeter, attack surface, firewall}”
- Threat actors love SSO compromise
 - Hybrid AD means that local environments are part of cloud enterprise
- Detect when identities are compromised, with deception



okta



onelogin
by ONE IDENTITY

My Apps Dashboard | okta-de X +

https://okta.com/app/UserHome?fromAdmin=true

Search your apps

Admin

My Apps

Work

Add section +

Notifications 1

Add apps

Last sign in: 16 minutes ago

© 2024 Okta, Inc.

Privacy

Sort ▾

My Apps

Work

Azure

Outlook

MS Teams

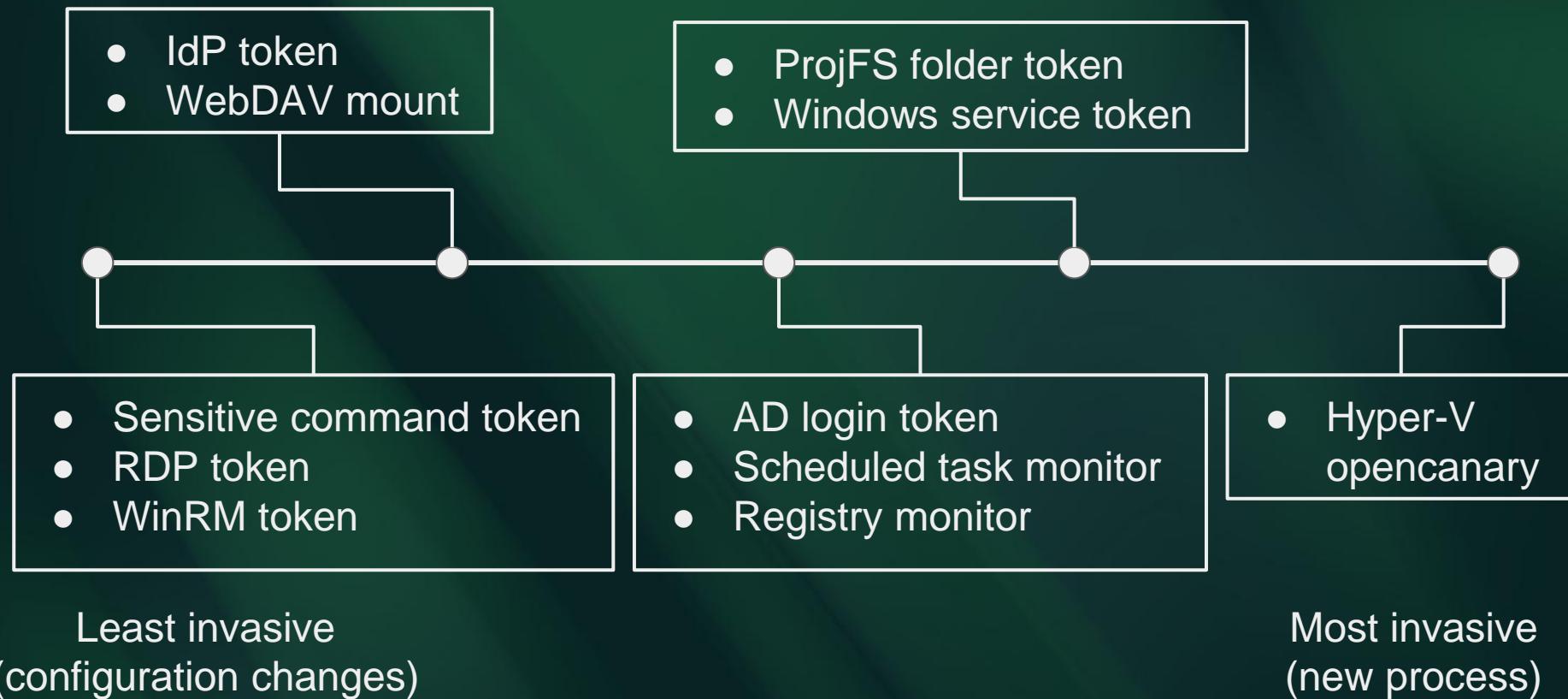
MS 365

SAP

+ Add section

</techniques>

Spectrum of capabilities



What didn't pan out

Fruitless directions

- Windows Sandbox
 - Spins up read-only Windows in VM
 - XML configuration for which application is run and if any state can be saved
 - Start-up times too high for dynamic usage
 - Long-running processes (e.g., browser) see less security benefit
- DPAPI as token
 - Useful for breadcrumbs, but doesn't provide sufficient auditing to token
 - Windows credential unprotect is not audit logged
 - Chrome and Edge protect all passwords with auditable credential
 - Cannot alert on specific password fill

Caveats

Caveats

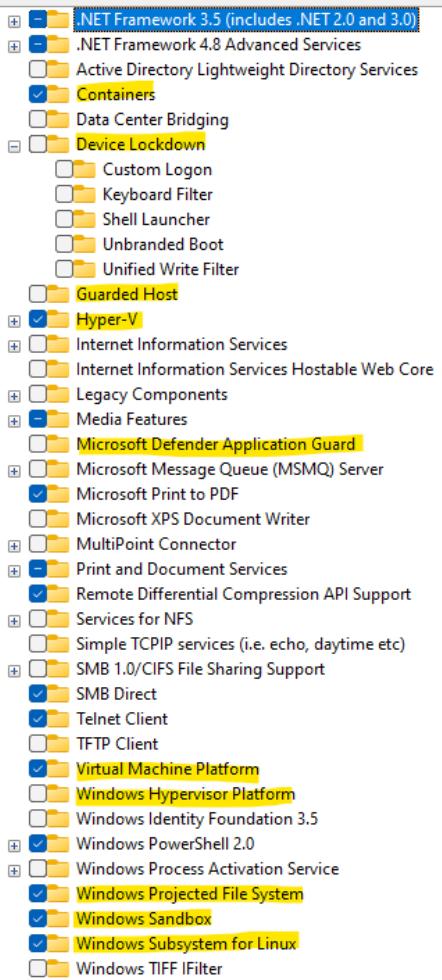
- PowerShell is restricted in many environments
 - Tension between allowing for unconstrained execution and improved defense
- Enabling visibility into audit events can reduce log retention
- Relying on existing functionality means that an update can change behavior
 - Managing version differences at scale is painful
 - Some features linger on unsupported
- Many of these capabilities leave visible fingerprints for attackers to look for

Future directions

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is

Future directions

- More primitives to be explored
- New features can bear fruit
 - Inject token data into Windows Recall?
 - More hybrid functionality can mean there is Azure-based visibility



Wrap-up

Takeaways

- Introduced Defending-off-the-Land
 - Repurposing built-in OS functionality
- Showed 11 techniques for defenders
 - Four are immediately available from <https://canarytokens.org>
 - Seven are available from <https://github.com/thinkst/defending-off-the-land>
- Celebrate your sysadmins, let them get clever

Thank you!

Links

- Tools demonstrated in this talk
 - <https://canarytokens.org>
 - <https://github.com/thinkst/defending-off-the-land>
- Additional Links
 - <https://github.com/thinkst/canarytokens>
 - <https://lolbas-project.github.io/>
 - <https://gtfobins.github.io/>
 - <https://www.loldrivers.io/>
 - <https://github.com/JFLarvoire/SysToolsLib/blob/master/PowerShell/PSService.ps1>