

EARLIER WARNINGS W/ TRIPWIRES

John Riley Kevin Lim Jim Long



WHAT ARE TRIPWIRES: HONEYFILES, HONEYDOCS, HONEYRECORDS, HONEYTOKENS

A honeyfile is a file that is designed to look like a real file on a server but contains bogus data. Honeyfiles are appealing targets for attackers. A honeyfile serves as a trap for attackers, and the data included within it can contain triggers that notify DLP solutions. Access to the files can also be tracked. A honeyrecord in a database is a honeyfile variant. These records serve the same purpose: they are forged and never utilized, but if they are ever copied, it indicates that there has been illicit activity.

The goal is generally to deploy them so no legitimate user would have reason to access them.

TRIPWIRES OR HONEY.....WHY.....WHO

Can be a "heads-up" to bad actors inside our networks and reduce "dwell time" of an initial compromise.

Inside - someone with too much access due to:
poorly configured permissions.
outdated job duties
Outside - Enemies - Bad actors
compromised accounts, - phishing
compromised machines - malware, viruses
poor configurations - incorrect permissions, lack of security software,
vulnerabilities - unpatched systems, zero days

TRIPWIRES: HONEY ACCOUNTS

 Honey Accounts: A good network honey account should mimic a real user account and look like a real person or organization. Use a real name, job title, or make it look like a shared account. Then change the available hours to 0, strong password, and log in once.

HONEY ACCOUNTS: USING GOOD BAIT

- Types of accounts
- admin's default administration acct, admin's
- administration -supt, principal, director, cio and other high profile accounts
- accounting/HR = payroll manager, accountants, HR managers
- Old accounts Director/ Supt move on? Use that account
- techs = it staff
- Service Accounts or Shared accounts = Powerschool admins, Printer admins, quickbook admins

TRIPWIRES/HONEY

• Honey Docs/files creation, names, placement

PowerShell

Canary Tokens

software packages - Thinkst canary, rapid7

You may want to consider placing your honey files in alternate directories that users would not be expected to browse in Windows Explorer. You could also use a file extension that does not produce a file preview in Windows Explorer to avoid these false positive alerts.

HONEY DOCS/TOKENS: USING GOOD BAIT

Types of documents

Passwords

Payroll -W-2's

Human resources - Contracts, Proposals, PII, discipline records,

Medical records

SS#'s

Financial documents - credit cards

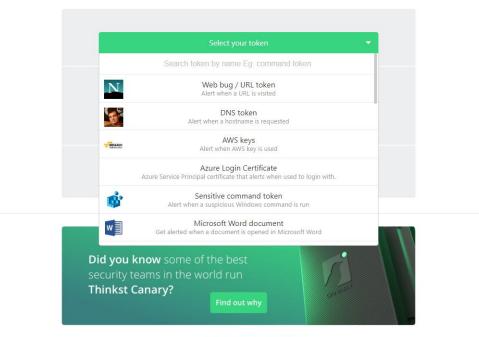
WAYS TO SETUP TRIPWIRES

Canary Tokens - Use for files not great for event viewer(spam) Windows auditing + PowerShell other options:

Active Directory management software. Rapid7 Insight Agent, (netrix.....AWS)

CANARY TOKENS - EASIEST TO SET UP

TOKENS



Read Our Canarytokens Documentation

TYPES OF CANARY TOKENS

	Select your token 🔻
	Search token by name Eg. command token
N	Web bug / URL token Alert when a URL is visited
Sec.	DNS token Alert when a hostname is requested
amazon rebiennos	AWS keys Alert when AWS key is used
A	Azure Login Certificate Azure Service Principal certificate that alerts when used to login with.
	Azure Entra ID login Trigger an alert when your Azure Entra ID login is being phished
Š	Sensitive command token Alert when a suspicious Windows command is run

WEB BUGS

- Web Bug native
- <u>http://canarytokens.com/articles/feedback/terms/mlqvvipn3jrbeqxh7mkv3pdhd/payments.js</u>



er connected.

WORD DOCS AND PDF'S



CANARYTOKEN TRIGGERED

Canarytoken triggered

ALER

A web bug Canarytoken has been triggered by the Source IP 207.160.133.62

Basic Details:

Channel	НТТР		
Time	2023-10-10 14:26:34.364545		
Canarytoken	5w2770o55hgzypvnk8kpr16e6		
Token reminder	This is a canary token place in home directory of admin		
Token type	web bug		
Source IP	207.160.133.62		
User-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/ <u>117.0.0.0</u> Safari/537.36		

Canarytoken Management Details:

Manage this Canarytoken here

More info on this token here

TYPES OF CANARY TOKENS



Web bug/URL token Putin an email with a juicy subject line. Or Embedded in documents Or link to image file



DNS token

AWS Keys



Azure Login Certificate



Sensitive Command Token executables often used by attackers but seldom used by regular users (e.g., whoami.exe, net.exe, wmic.exe, etc.). or attacker tools that are not present on your system (e.g., mimikatz.exe), Ne ed to use in a network management tool to deploy across your organization

Microsoft Word Document Leave the file on a web server in an inaccessible directory, to detect webserver breaches. Attach to an email with a tempting Subject line.

CANARY TOKENS

Pro's

easy to setup and deploy

Con's

The doc file has to open with word

It triggers a dns query

web bugs should be shortened to disguise the url

May need path to run w/ admin credentials



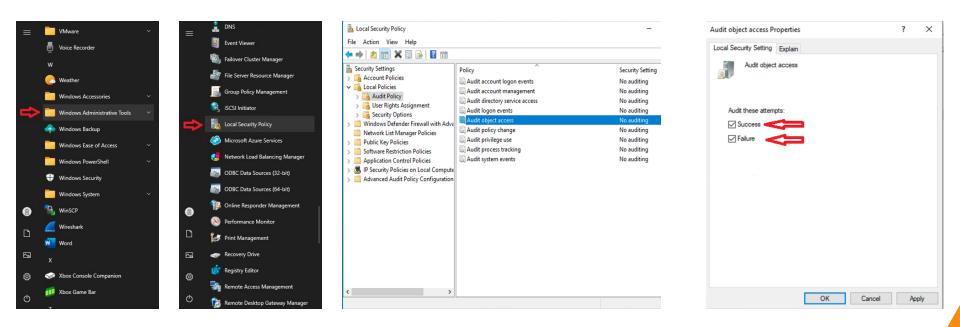
POWERSHELL MONITORING EXAMPLE CONFIGURATION

MONITORING REQUIREMENTS

- PowerShell scripts are available through the link on slide 24
- Create directory "c:\batchfiles" and place the below files to it
 - acct-access.ps1
 - file-access.ps1
 - psbypass.bat.txt change filename to psbypass.bat
- SMTP Relay
 - The script requires an SMTP Relay to send alert emails
 - Google Workspace includes access to a SMTP Relay

FILE MONITORING CONFIGURATION

• Enable Audit Policy



FILE MONITORING CONFIGURATION

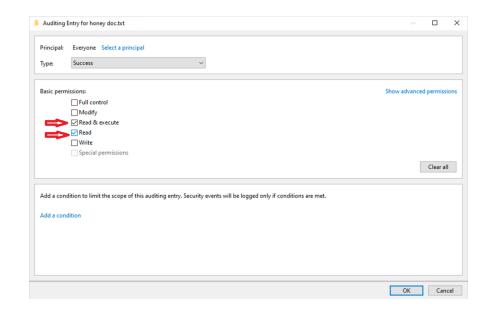
Configure Auditing for honey file

🖻 hanna da aka	Deserves				×
honey doc.tx	roperti	es			
General Security	Details	Previous \	/ersions		
Object name:	C:\Data\h	noney doc.tx	t		
Group or user na	mes:				
Authenticat	ed Users				
SYSTEM					
Se Administrate	ors (.	yourpc	Administrator	s)	
🎎 Users (*	yourpc	\Users)			
To change perm	inninga eli	alı Edit			
				Edit	
Permissions for A Users	wthenticat	ed	Allow	Deny	
Full control					
Modify			\checkmark		
Read & execu	te		\checkmark		
Read			\checkmark		
Write			\checkmark		
Special permis	sions				
For special permi click Advanced.	ssions or a	advanced se	ttings,	Advanced	
				Û	
		ОК	Cancel	Apply	

me: ner: yo	C:\Data\honey	doc.txt @domain.com) Cha	202			
rmissions		Effective Access	ige			
additional		ble-click an audit entry.	To modify an audit entr	y, select the entry and click Edit (if	available).	
Туре	Principal		Access	Inherited from		 _
л						
Add	Remove	View				 _
	1. Star					

FILE MONITORING CONFIGURATION

Auditing Entry for honey doc.txt		- D X
Select User, Computer, Service Account, or Group	×	
Select this object type:		
User, Group, or Built-in security principal	Object Types	
From this location:		
yourdomain.com	Locations	Show advanced permissions
Enter the object name to select (<u>examples</u>):		Show duranced permissions
everyone	Check Names	
<u> </u>		
·		
Advanced OK	Cancel	
Special permissions		
		Clear all
Add a condition to limit the scope of this auditing entry. Sec	curity events will be logged only if condition	s are met.
Add a condition		
Add a condition		



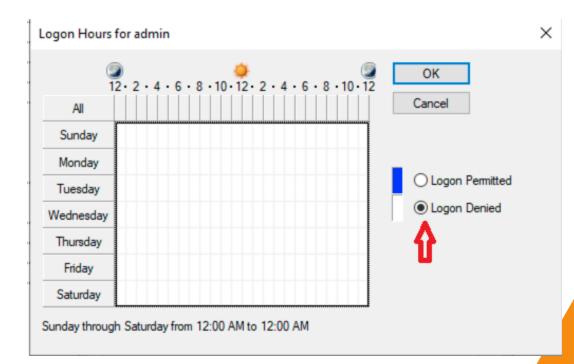
FILE MONITOR CONFIGURATION

- Configure Script Variables file-access.ps1
 - \$Log = "Security" Windows log that the script runs against
 - **\$eventid = 4663 -** Event ID that is filtered for
 - \$msg = "ReadData" Filtered event subject in this case "file read"
 - \$FileName = "c:\temp\file-access.txt" Event file summary
 - \$PSEmailServer = "smtprelay.domain.net" SMTP relay server
 - \$mailto = "youremail.domain.net" Alert email recipient
 - \$hfile = "super-cool-info.txt" Name of honeyfile

ACCOUNT MONITORING CONFIGURATION

Set logon hours to created honey-account in ADUC

admin Properties				? ×	
Member Of Dial-in Environment Sessions Remote control Remote Desktop Services Profile COM+ General Address Account Profile Telephones Organizati					
User logon name: User logon name (pre-Windows 2000): yourdomain\ admin Logon Hours Log On To Unlock account					
Account options: User must change password at next logon User cannot change password Password never expires Store password using revensible encryption Account expires Never End of: Thursday , November 2, 2023					
OK Cancel Apply Help					



ACCOUNT MONITOR CONFIGURATION

- Configure Script Variables acct-access.ps1
 - \$Log = "Security" Windows log that the script runs against
 - **\$eventid = 4625 -** Event ID that is filtered for
 - \$msg = "admin" Filtered event subject in this case we are monitoring the "admin" account
 - \$FileName = "c:\temp\acct-access.txt" Event file summary
 - \$PSEmailServer = "smtprelay.domain.net" SMTP relay server
 - \$mailto = "youremail.domain.net" Alert email recipient

TASK SCHEDULER CONFIGURATION

(2) Task Scheduler	X	(b) Create Task
File Action View Help		General Triggers Actions Conditions Settings
, Jask Scheduler (Local) Name Status Triggers	Actions	Name: Honeyfile-Acct Task
→ ☐ Task Scheduler Livran. Multiple triggers defined → ☐ Microsoft Create Basic Task Multiple triggers defined ▲ Mozilla Create Task At 6:41 PM every day - Aft		Location: \ Author: yourdomain\your acct
Import Task At 2:00 PM on 5/1/1992 - Display All Running Tasks At 3:34 PM on 9/24/2023 - Disable All Tasks History	After triggered, rep	Description:
New Folder View > s Conditions Settings		Security options
Refresh dgeUpdateTaskMachineCo Help	re View View View View View View View Vie	When running the task, use the following user account: NT AUTHORITY\SYSTEM Change User or Group
Author: Description: Keeps your Microsoft software up to software will not be kept up to date, i fixed and features may not work. This using it. Security options	eaning securit task uninstalls End Disable Export	 Run only when user is logged on Run whether user is logged on or not Do not store password. The task will only have access to local computer resources. Run with highest privileges
When running the task, use the following user according to the second se	Dunt: Delete	☐ Hidden Configure for: Windows Vista™, Windows Server™ 2008 ✓ OK Cancel

TASK SCHEDULER CONFIGURATION

🕒 Create Task 🕕	X New Trigger X
General Triggers Actions Conditions Settings When you create a task, you can specify the conditions that will trigger the task.	Begin the task: On a schedule
Trigger Details Status	 Daily Weekly Monthly Advanced settings Delay task for up to (random delay): 1 hour Repeat task every: 15 minutes Stop all running tasks at end of repetition duration Stop task if it runs longer than: 30 minutes Stop task if it runs longer than: Expire: 2/ 2/2025 10:42:18 AM
New Edit Delete	Enabled
OK Cancel	OK Cancel

- Adjust task frequency that works for your case
- Start with a 15 min interval and adjust as needed
- Give task enough time to complete before the task runs again
- Some logs are very large and could take longer to for the script to parse

TASK SCHEDULER CONFIGURATION

		Edit Action ×
🕒 Create Task	×	You must specify what action this task will perform.
General Triggers Actions Conditions Settings		Action: Start a program
When you create a task, you must specify the action that will occur when your task starts.		Settings
Action Details	*	Program/script: C:\batchfiles\psbypass.bat Browse Add arguments (optional): Start in (optional):
New Edit Delete	Cancel	OK Cancel

- Running the PowerShell scripts within a batch file is simpler than configuring Task Scheduler to run a standalone PowerShell script
- The batch file also sets the PowerShell Execution Policy to allow scripts to run and then resets it back to "Restricted" when the task completes

QUESTIONS?

rileyjr@more.net kevinl@more.net long@more.net

Link to the scripts: http://bit.ly/45svdk0



THANK YOU FOR COMING!