



# **“AND AGAIN ADVERSARY KNOWS YOUR NEW PASSWORD”**

**A Threat Hunting Walkthrough**

**– Arvind Javali**

# AGENDA

- c:\windows\system32\WHOAMI.exe 1
- Who is this presentation for 2
- When to kick start threat hunt? 3
- What is “Persistence”? 4
- Threat Groups – “Persistence” 5
- Hunt for “Persistence” 6



C:\WINDOWS\SYSTEM32\WHOAMI.EXE

1



Arvind Javali

GCFA | Cyber Security Incident Responder

12+ years of experience in advisory and implementation of Information Security technologies.

Certified – Incident Response, Threat Hunting and Forensics

Connect me:



ARVIND JAVALI



@JAVALIREPORTS



@JAVALIREPORTS



arvind.jayanth5@gmail.com



# WHO IS THIS PRESENTATION FOR:

- Cyber Security Professionals:
  - SOC Analysts
  - Penetration Testers (Beginners)
  - Threat Hunters (Beginners)
  - Cyber Product Managers
  - Cyber Sales Team
- Data Science Engineers (Cyber Security)
- HR Recruitment Professionals (Cyber Security)
- Aspirants who want to learn and understand “what is cyber threat hunting?”
- DISCLAIMER: In this presentation I am showing threat hunting for one of the artefact only.



# WHEN TO KICK START THREAT HUNT 3.1

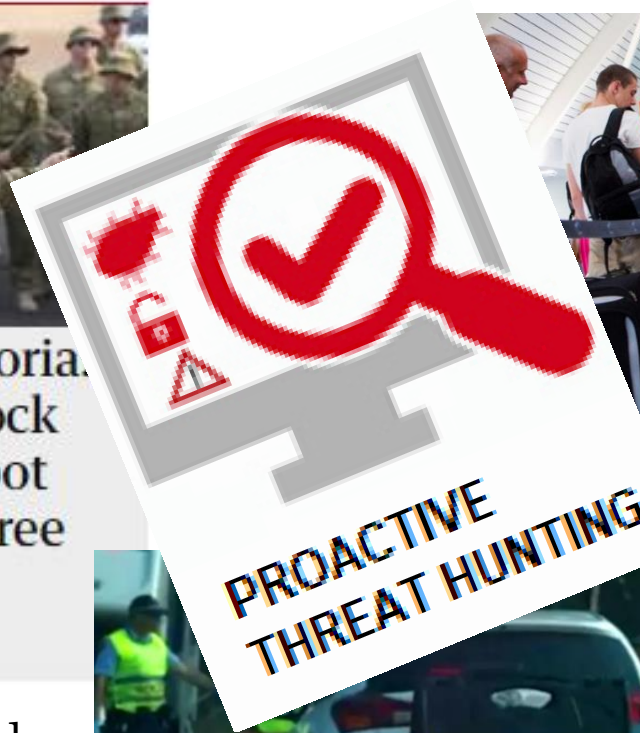


Coronavirus Victoria: army to door-knock Melbourne hotspot suburbs to offer free Covid-19 testing

25 Jun 2020

A

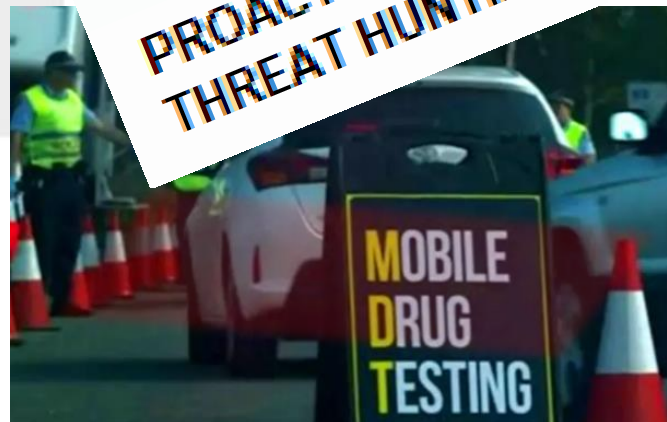
compromised



check the luggage of passengers waiting to check in to a flight. (Supplied)

B

suspect



C

periodic



## WHEN TO KICK START THREAT HUNT 3.2

- The system is identified as “compromised” **A**
- You “suspect” of malicious activity in the servers / network **B**
- Random checks on “periodic” basis **C**



# THREAT HUNTING IN WINDOWS

## 4.1

- “Example Case Description”

*“Multiple users of ‘EXAMPLE COMPANY’ reported that they are unable to login to servers due to incorrect password and several tickets created to reset passwords.*

*After a few rounds of troubleshooting, IT staffs from ‘EXAMPLE COMPANY’ noticed unusual behaviour on a that server. IT staffs confirmed confidently that they have successfully eradicated the threat.*

*But few users still reported their passwords getting reset.”*

- Lets hunt for “Persistence”



# “PERSISTENCE” IN ACTION

4.2



IT Staff

Maintaining “Persistence”  
using ladder`

Attacker





# WHAT MITRE SAY?

4.3

**MITRE** | **ATT&CK**<sup>®</sup>

Matrices

Tactics ▾


Techniques ▾

Mitigations ▾


Groups

Software

Resources ▾

Blog 

Contribute

Search 

The sub-techniques beta is [now live!](#) Read the [release blog post](#) for more info.

TACTICS

PRE-ATT&CK

Enterprise

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

▼

▲

Home > Tactics > Enterprise > Persistence

## Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

ID: TA0003

Created: 17 October 2018

Last Modified: 19 July 2019

[version](#) [permalink](#)



# PERSISTENCE FOR WINDOWS

## 4.4

Initial Access 11 items	Execution 28 items	Persistence 44 items	Privilege Escalation 25 items	Defense Evasion 60 items	Credential Access 16 items	Discovery 23 items	Lateral Movement 16 items	Collection 13 items	Command And Control 10 items	Exfiltration 9 items	Impact 16 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Graphical User Interface	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	InstallUtil	Component Firmware	Hooking	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	LSASS Driver	Component Object Model Hijacking	Image File Execution Options Injection	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Msihta	Create Account	New Service	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Query Registry	Taint Shared Content	Video Capture	Multiband Communication		Service Stop
	PowerShell	DLL Search Order Hijacking	Parent PID Spoofing	Deobfuscate/Decode Files or Information	Network Sniffing	Remote System Discovery	Third-party Software		Multilayer Encryption		Stored Data Manipulation
	Regsvcs/Regasm	External Remote Services	Path Interception	Disabling Security Tools	Password Filter DLL	Security Software Discovery	Windows Admin Shares		Remote Access Tools		System Shutdown/Reboot
	Regsvr32	File System Permissions Weakness	Port Monitors	DLL Search Order Hijacking	Private Keys	Software Discovery	Windows Remote Management		Remote File Copy		Transmitted Data Manipulation
	Rundll32	Hidden Files and Directories	PowerShell Profile	DLL Side-Loading	Steal Web Session Cookie	System Information Discovery			Standard Application Layer Protocol		
	Scheduled Task	Hooking	Process Injection	Execution Guardrails	Two-Factor Authentication Interception	System Network Configuration Discovery			Standard Cryptographic Protocol		
	Scripting	Hypervisor	Scheduled Task	Exploitation for Defense Evasion		System Network Connections Discovery			Standard Non-Application Layer Protocol		
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Extra Window Memory Injection		System Owner/User Discovery			Uncommonly Used Port		
	Signed Binary Proxy Execution	Logon Scripts	SID-History Injection	File and Directory Permissions Modification		System Service Discovery					
	Signed Script Proxy Execution	LSASS Driver	Valid Accounts	File Deletion		System Time Discovery					
	Third-party Software	Modify Existing Service	Web Shell	File System Logical Offsets		Virtualization/Sandbox Evasion					
	Trusted Developer Utilities	Netsh Helper DLL		Group Policy Modification							
	User Execution	New Service		Hidden Files and Directories							
	Windows Management Instrumentation	Office Application Startup		Hidden Window							
	Windows Remote Management	Path Interception		Image File Execution Options Injection							
	XSL Script Processing	Port Monitors		Indicator Blocking							
		PowerShell Profile		Indicator Removal from Tools							
		Redundant Access		Indicator Removal on Host							
		Registry Run Keys / Startup Folder		Indirect Command Execution							
		Scheduled Task		Install Root Certificate							
		Screensaver		InstallUtil							

# PERSISTENCE FOR WINDOWS (44 ITEMS) 4.5

Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Logon Scripts
LSASS Driver

Modify Existing Service
Netsh Helper DLL
New Service
Office Application Startup
Path Interception
Port Monitors
PowerShell Profile
Redundant Access
Registry Run Keys / Startup Folder
Scheduled Task
Screensaver
Security Support Provider
Server Software Component
Service Registry Permissions Weakness
Shortcut Modification
SIP and Trust Provider Hijacking
System Firmware
Time Providers
Valid Accounts
Web Shell
Windows Management Instrumentation Event Subscription
Winlogon Helper DLL



# THREAT GROUPS – PERSISTENCE

5

## ○ Scheduled Task – Technique ID: T1053

APT18
APT29
APT3
APT32
APT33
APT39
APT41
at
BADNEWS
BONDUPDATER
BRONZE BUTLER
Carbon
Cobalt Group
CosmicDuke
CozyCar
Dragonfly 2.0
Duqu
Emotet
Empire
EvilBunny
FIN10

FIN6
FIN7
FIN8
Gazer
GravityRAT
GRIFFON
Helminth
ISMinjector
JHUHUGIT
Machete
Machete
Matroyshka
menuPass
MURKYTOP
NotPetya
OilRig
OopsIE
Patchwork
PowerSploit
POWERSTATS
POWRUNER

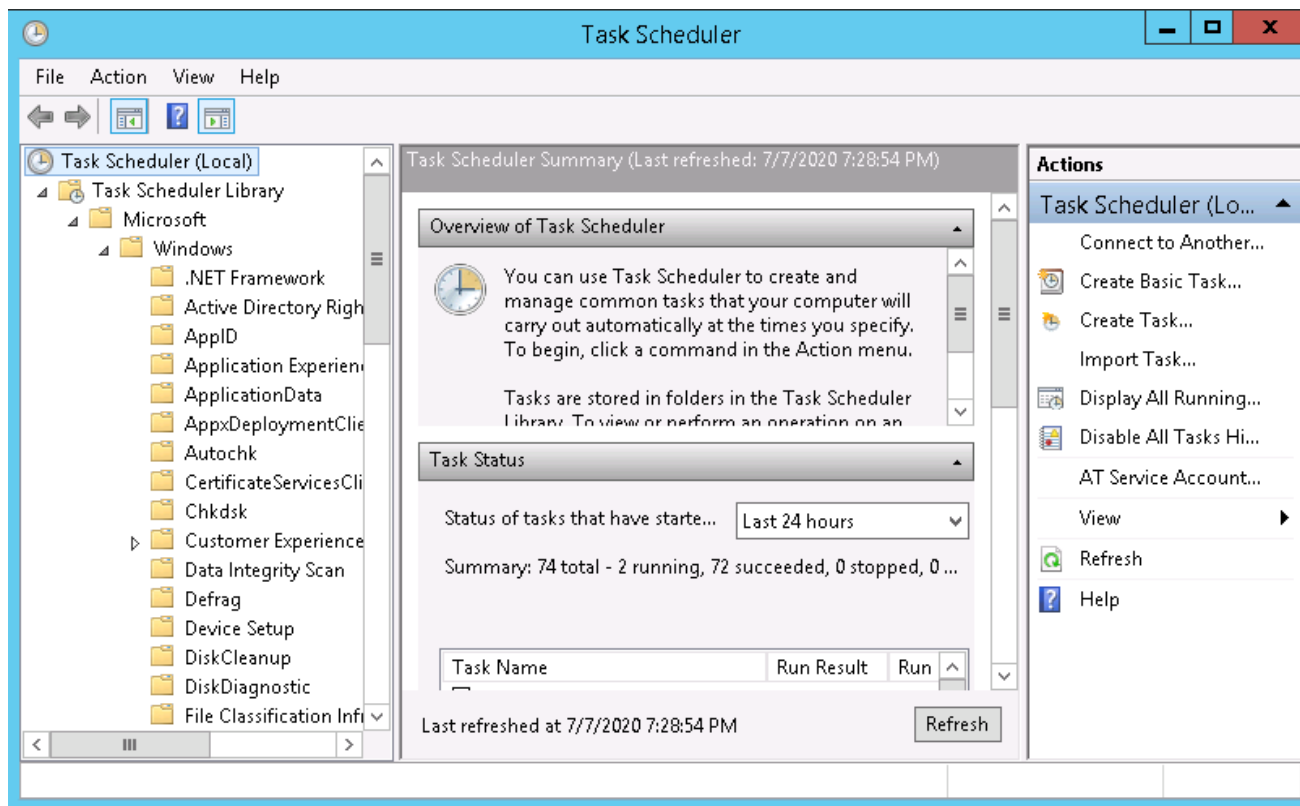
Pteranodon
QUADAGENT
QuasarRAT
Rancor
Remexi
RemoteCMD
Remsec
Revenge RAT
RTM
schtasks
ServHelper
Shamoon
Silence
Smoke Loader
Soft Cell
SQLRat
Stealth Falcon
TEMP.Veles
Threat Group-3390
TrickBot
yty
zwShell



# HUNT FOR “PERSISTENCE”

6.1

## ○ Scheduled Task – Technique ID: T1053



# HUNT FOR “PERSISTENCE”

## 6.2

Host Name	Task Name	Next Ru...	Status	Logon Mode	Last Run Time	Author	Task To Run	Run As User
HomeLab	Microsoft\Windows\WindowsUp...	2/5/2020 ...	Ready	Interactive/Background	2/4/2020 5:31:27 PM	Microsoft Corporat...	C:\Windows\system32\sc.exe start wuau...	SYSTEM
HomeLab	Microsoft\Windows\WindowsUp...	2/5/2020 ...	Ready	Interactive/Background	2/4/2020 5:31:27 PM	Microsoft Corporat...	C:\Windows\system32\sc.exe start wuau...	SYSTEM
HomeLab	Microsoft\Windows\WindowsUp...	2/5/2020 ...	Ready	Interactive/Background	2/4/2020 5:31:40 PM	Microsoft Corporat...	C:\Windows\system32\sc.exe start wuau...	SYSTEM
HomeLab	Microsoft\Windows\WindowsUp...	2/5/2020 ...	Ready	Interactive/Background	2/4/2020 5:31:40 PM	Microsoft Corporat...	C:\Windows\system32\sc.exe start wuau...	SYSTEM
HomeLab	Microsoft\Windows\WindowsUp...	2/5/2020 ...	Ready	Interactive/Background	2/4/2020 5:31:40 PM	Microsoft Corporat...	C:\Windows\system32\sc.exe start wuau...	SYSTEM
HomeLab	Microsoft\Windows\WindowsUp...	2/5/2020 ...	Ready	Interactive/Background	2/4/2020 5:31:40 PM	Microsoft Corporat...	C:\Windows\system32\sc.exe start wuau...	SYSTEM
HomeLab	Microsoft\Windows\Wininet\Ca...	N/A	Running	Interactive/Background	2/4/2020 1:07:00 PM	Microsoft	COM handler	Users
HomeLab	Microsoft\Windows\Workplace J...	N/A	Disabled	Interactive/Background	N/A	N/A	%SystemRoot%\System32\AutoWorkplac...	Authenticated Users
HomeLab	Microsoft\Windows\WS\Badge ...	N/A	Ready	Interactive/Background	2/4/2020 1:44:56 PM	Microsoft Corporat...	COM handler	INTERACTIVE
HomeLab	Microsoft\Windows\WS\License ...	2/7/2020 ...	Ready	Interactive/Background	2/4/2020 3:11:42 AM	Microsoft Corporat...	rundll32.exe WSClient.dll,WSpTLR licens...	LOCAL SERVICE
HomeLab	Microsoft\Windows\WS\Sync Li...	N/A	Ready	Interactive/Background	N/A	Microsoft Corporat...	COM handler	Users
HomeLab	Microsoft\Windows\WS\WSRefr...	2/6/2020 ...	Ready	Interactive/Background	2/4/2020 8:34:34 AM	Microsoft Corporat...	rundll32.exe WSClient.dll,RefreshBanned...	Users
HomeLab	Microsoft\Windows\WS\WSTask	N/A	Ready	Interactive/Background	N/A	Microsoft Corporat...	COM handler	SYSTEM
HomeLab	MicrosoftOfficialUpdates	N/A	Running	Interactive only	5/26/2019 3:21:00 PM	administrator	C:\TMP\mim.exe sekurlsa::LogonPasswo...	DefaultDomain\adminis
HomeLab	\Optimize Start Menu Cache Files...	N/A	Ready	Background only	N/A	Microsoft Corporat...	COM handler	NT AUTHORITY\SYST
HomeLab	\Optimize Start Menu Cache Files...	N/A	Ready	Background only	N/A	Microsoft Corporat...	COM handler	NT AUTHORITY\SYST
HomeLab	\Optimize Start Menu Cache Files...	N/A	Ready	Background only	N/A	Microsoft Corporat...	COM handler	NT AUTHORITY\SYST
HomeLab	\Optimize Start Menu Cache Files...	N/A	Ready	Background only	2/15/2019 10:58:31 PM	Microsoft Corporat...	COM handler	NT AUTHORITY\SYST
HomeLab	\Optimize Start Menu Cache Files...	N/A	Ready	Background only	10/21/2019 7:39:32 PM	Microsoft Corporat...	COM handler	Arvind
HomeLab	\Optimize Start Menu Cache Files...	N/A	Ready	Background only	5/26/2019 12:42:36 PM	Microsoft Corporat...	COM handler	Arvind
HomeLab	\Optimize Start Menu Cache Files...	N/A	Ready	Background only	5/26/2019 12:42:36 PM	Microsoft Corporat...	COM handler	NT AUTHORITY\SYST
HomeLab	\Optimize Start Menu Cache Files...	N/A	Ready	Background only	5/26/2019 12:42:36 PM	Microsoft Corporat...	COM handler	Arvind

Malicious Scheduled Task:

**mimikatz > sekurlsa::logonpasswords**

Steals authentication information stored in the OS. This tool is used to acquire a user's password and use it for unauthorized login.



# THANKS FOR YOUR TIME 😊

Please hit , Share and Subscribe

Connect me:



ARVIND JAVALI



@JAVALIREPORTS



@JAVALIREPORTS

You can watch the video presentation from this link:

<https://youtu.be/ymiA0xKzPrM>



arvind.jayanth5@gmail.com

