Investigating & Responding Ransomware Incidents

Anurag Khanna

v1.0

What will we talk about today?

- Ransomware!
- Anatomy of a ransomware attack
- Key technical trends

Takeaway: Understand the ransomware attacks. prepare, prevent and respond.

Primary Motivations & Objectives

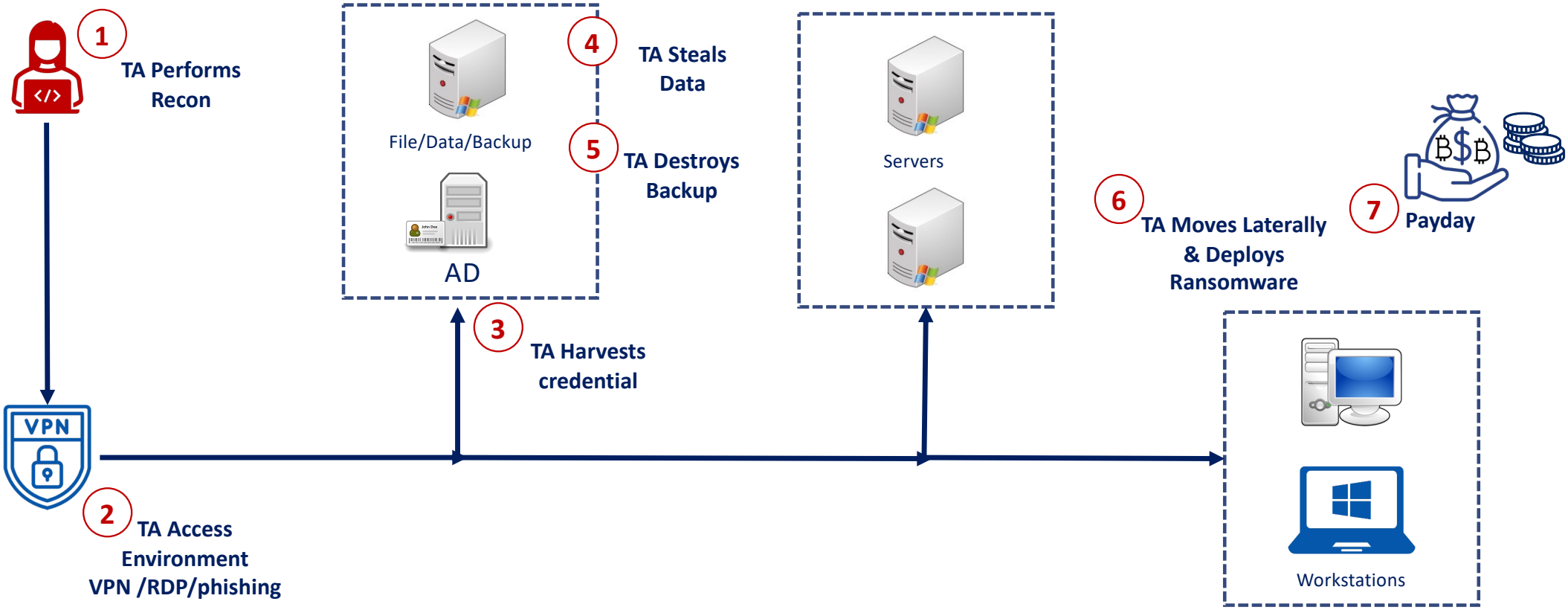
- Primary motivations
  - Get Paid! – Threat Actor with a business model
  - Sometimes deploy ransomware on servers and endpoints
  - Sometimes destroy backups making it difficult to recover
  - Exfiltrate critical data from systems for extortion

Battling Ransomware

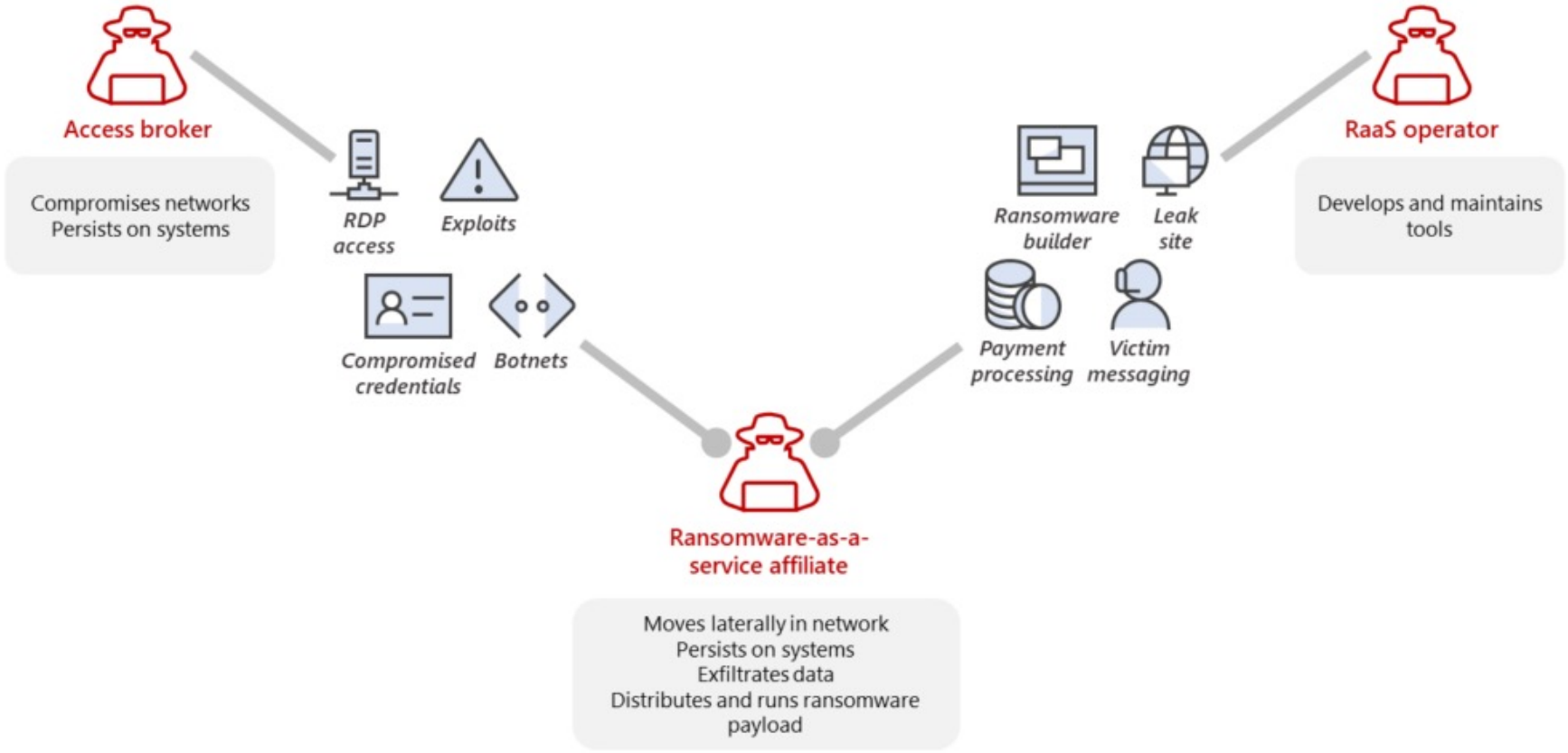
Ransomware is a business problem!

- Today we will talk about technical response to the problem
- Responding to Ransomware needs a business response

Anatomy of Ransomware attack



Ransomware as a Service



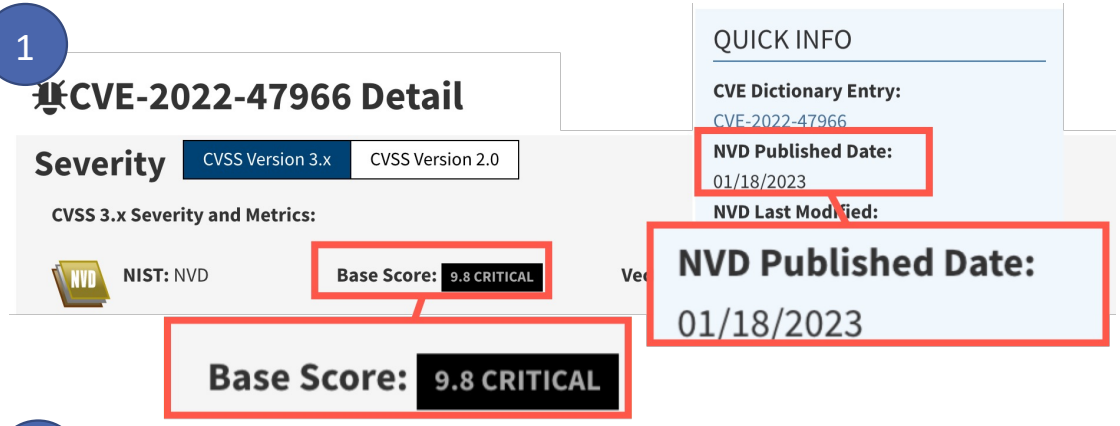
https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Initial Access

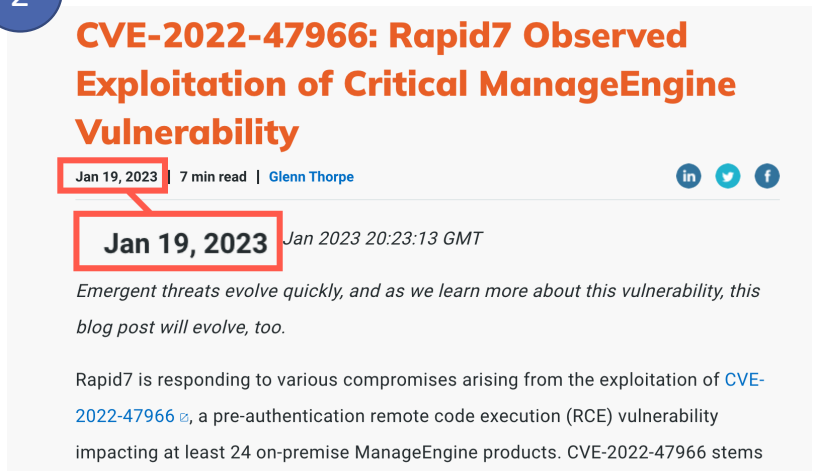
- Single Factor VPN
  - Yes, it is still a thing. Probably still the most common Initial Access vector
  - Password guessing/ password spraying
  - Credential stuffing is effective
- Even if you have MFA
  - Do you have it on ALL accounts?
  - Sim Swapping is more real than ever – SCATTEREDSPIDER
  - MFA Spam attacks work
  - Legacy authentication enabled?
  - MFA configuration/registration?

Example of Initial vector – Manage engine Vulnerability

1



2



3

Security advisory for remote code execution vulnerability in multiple ManageEngine products

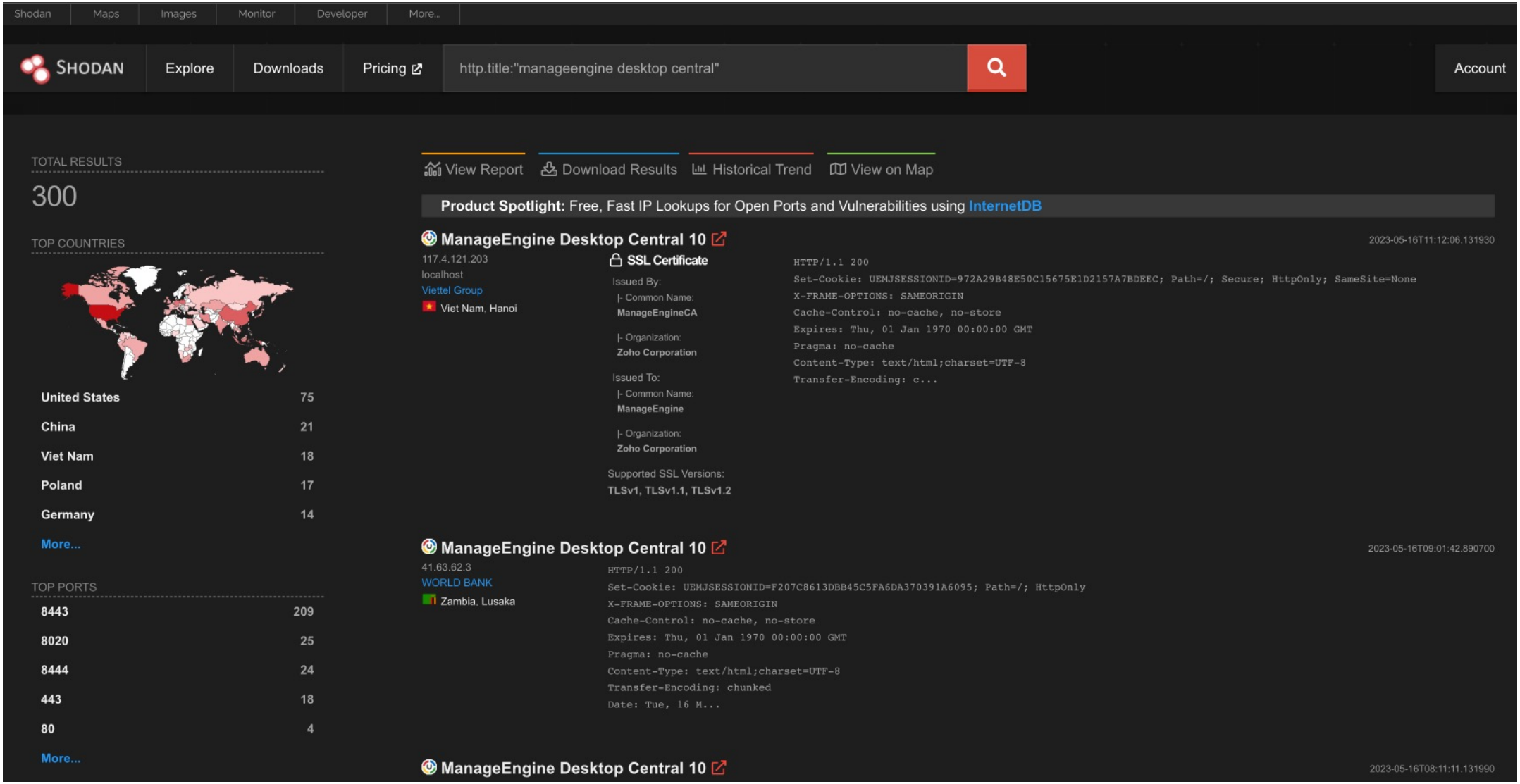
Severity : Critical

CVE ID : CVE-2022-47966

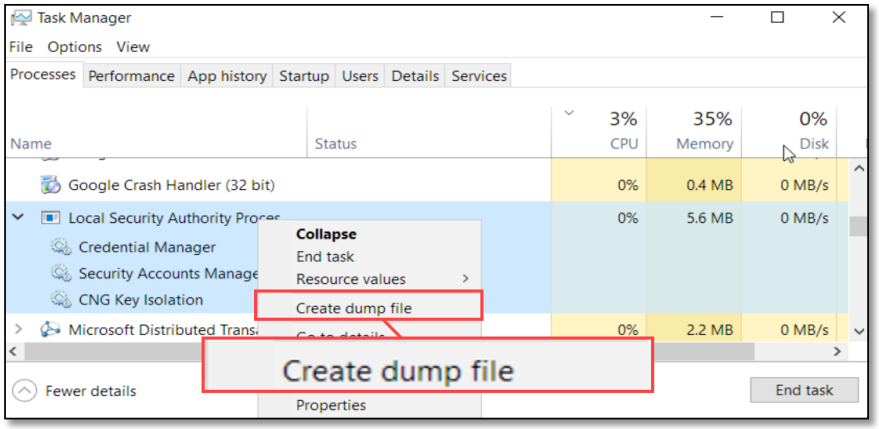
Details :
This advisory addresses an unauthenticated remote code execution vulnerability reported and patched in the following ManageEngine OnPremise products due to the usage of an outdated third party dependency, Apache Santuario.
ManageEngine On-Demand/cloud products are not affected by this vulnerability.

Applicability :
This advisory is applicable only when **SAML SSO is/was enabled** in the ManageEngine setup.

Product Name	Impacted Version(s)	Fixed Version(s)	Released On
Access Manager Plus*	4307 and below	4308	7/11/2022
Active Directory 360**	4309 and below	4310	28/10/2022
ADAudit Plus**	7080 and below	7081	28/10/2022
ADManager Plus**	7161 and below	7162	28/10/2022
ADSelfService Plus**	6210 and below	6211	28/10/2022
Analytics Plus*	5140 and below	5150	7/11/2022
Application Control Plus*	10.1.2220.17 and below	10.1.2220.18	28/10/2022
Asset Explorer**	6982 and below	6983	27/10/2022
Browser Security Plus*	11.1.2238.5 and below	11.1.2238.6	28/10/2022
Device Control Plus*	10.1.2220.17 and below	10.1.2220.18	28/10/2022


Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Downloads
Pricing
http.title:"manageengine desktop central"
Account
TOTAL RESULTS
300
TOP COUNTRIES
United States 75
China 21
Viet Nam 18
Poland 17
Germany 14
More...
TOP PORTS
8443 209
8020 25
8444 24
443 18
80 4
More...
View Report
Download Results
Historical Trend
View on Map
Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB
ManageEngine Desktop Central 10
2023-05-16T11:12:06.131930
117.4.121.203
localhost
Viettel Group
Viet Nam, Hanoi
SSL Certificate
Issued By:
|- Common Name:
ManageEngineCA
|- Organization:
Zoho Corporation
Issued To:
|- Common Name:
ManageEngine
|- Organization:
Zoho Corporation
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
HTTP/1.1 200
Set-Cookie: UEMJSESSIONID=972A29B48E50C15675E1D2157A7BDEEC; Path=/; Secure; HttpOnly; SameSite=None
X-FRAME-OPTIONS: SAMEORIGIN
Cache-Control: no-cache, no-store
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: c...
ManageEngine Desktop Central 10
2023-05-16T09:01:42.890700
41.63.62.3
WORLD BANK
Zambia, Lusaka
HTTP/1.1 200
Set-Cookie: UEMJSESSIONID=F207C8613DBB45C5FA6DA370391A6095; Path=/; HttpOnly
X-FRAME-OPTIONS: SAMEORIGIN
Cache-Control: no-cache, no-store
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 16 M...
ManageEngine Desktop Central 10
2023-05-16T08:11:11.131990

Credential Theft – Local System



Task Manager

```
C:\Tools>procdump -ma lsass.exe C:\tools\lsass.dmp
….
[04:02:26] Dump 1 initiated: C:\tools\lsass1.dmp
[04:02:26] Dump 1 writing: Estimated dump file size is 43 MB.
[04:02:26] Dump 1 complete: 43 MB written in 0.1 seconds
[04:02:26] Dump count reached.
```

SysInternals Procdump

```
C:\Tools>createdump -u -f lsass.dmp -d 640
Writing full dump to file lsass.dmp
Dump successfully written
```

Dotnet Createdump

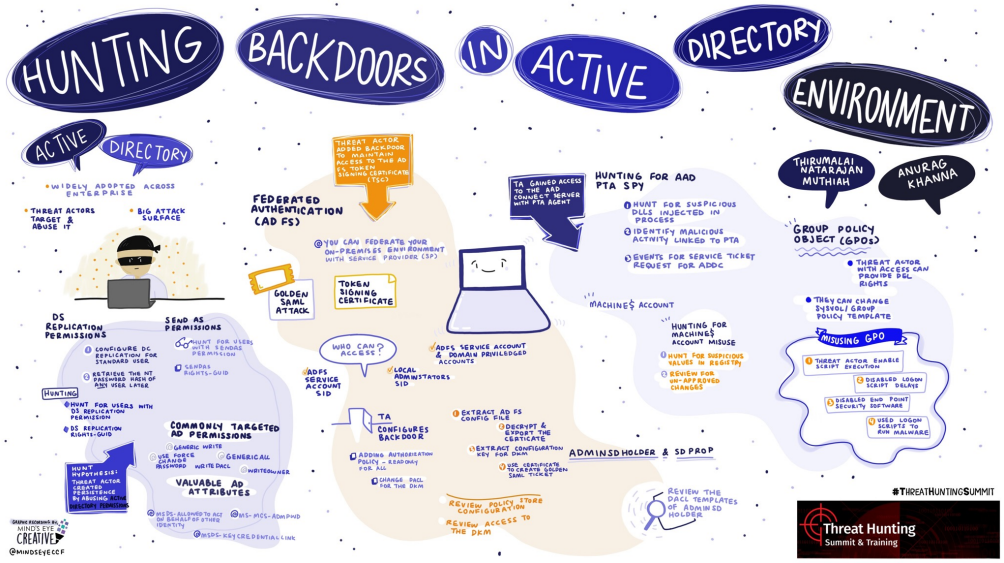
Credential Theft - Keys to the Kingdom – Dumping NTDS.DIT

```
C:\temp>powershell ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp\ntd' q q
Copying registry files...
Copying c:\temp\ntd\registry\SYSTEM
Copying c:\temp\ntd\registry\SECURITY
Snapshot {ddb1f6fa-a650-4f5b-b49e-074db672985e} unmounted.
IFM media created successfully in c:\temp\ntd
```

Stealing NTDS.DIT

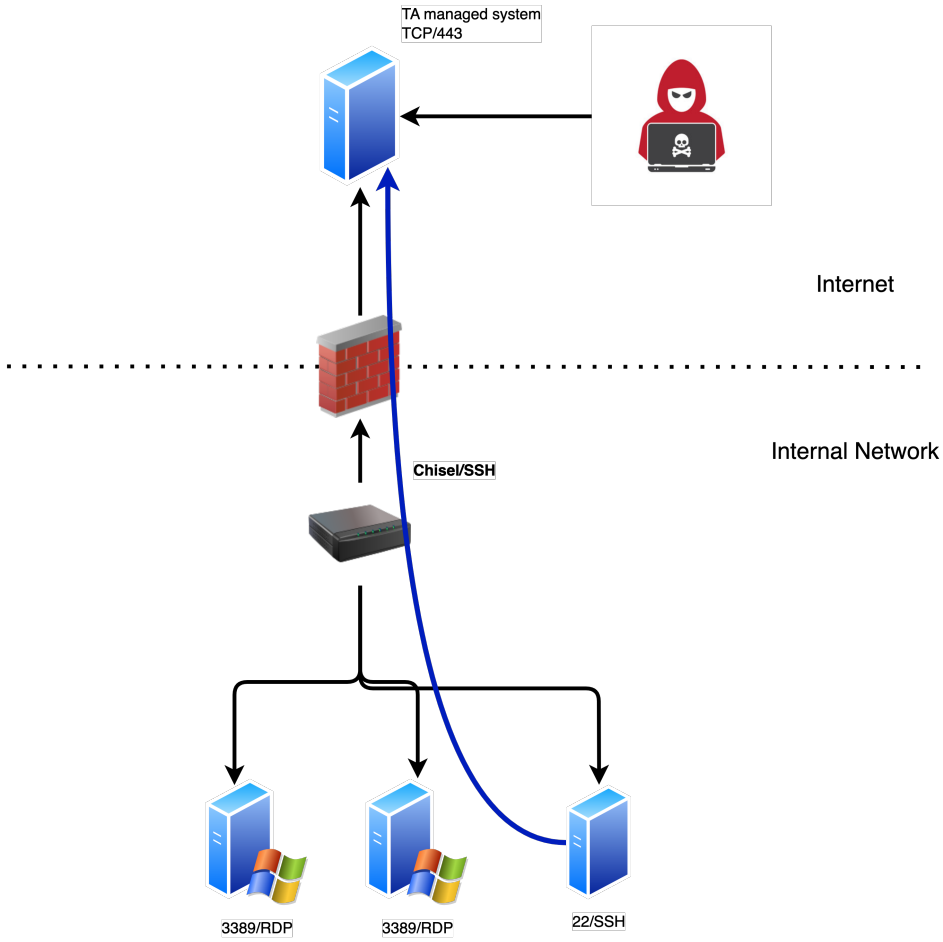
Persistence – I am there!

- Persistent methods to maintain long term access
  - Backdoors and Implants
  - Valid Credentials connecting over VPN
  - Out of Band management software
    - AnyDesk, TeamViewer, ConnectWise
  - Stealthier approaches



Remote Tunnels – You do not see me

- Pivoting and Lateral Movement
- Chisel/SSH/Ngrok etc
- Can you detect this?



Data Exfiltration - Actions on Objectives

- Techniques that adversaries use to steal data from the network
- Traditional/common way is to perform data staging
  - Create Archives (zip, 7zip, rar, etc.) and delete once exfiltrated
  - Often chunked in small files, to ensure successful file transfer

Data Exfil Options

- Open a web-browser, signin/up, upload (more common than what is sounds)
  - OneDrive, SharePoint, GoogleDrive, MEGA, Box, DropBox, Cloud Storage,
- Rclone
  - Very common, Supports lot of cloud services
- File Transfer
  - WinSCP, FileZilla …
- HTTP connections

How about these?

How about:

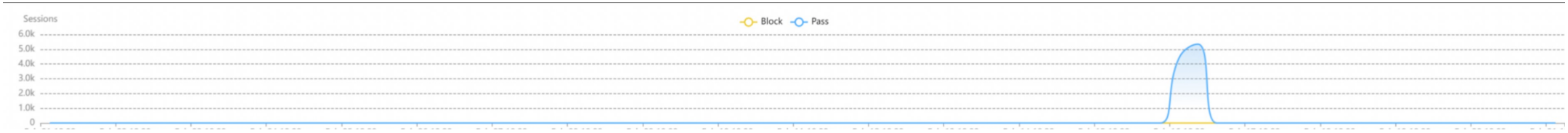
- Shares/Drives accessed over VPN
- Remote Desktop Protocol (RDP)/Mapped drives (No logging)
- TeamViewer/AnyDesk
- Remote Management Tools

- Often more difficult to investigate/detect

Detect/Investigate data exfil

Network traffic is probably your best bet

- Firewall/Traffic logs/Netflow
  - Traffic spikes and traffic to unknown IP address
- Just know traffic went out, nothing more



Host based artifacts

Falcon OverWatch Threat Hunting Contributes to Seamless Protection Against Novel BlackCat Attack

March 23, 2022 Falcon OverWatch Team From The Front Lines

CROWDSTRIKE | BLOG Featured Re

Upon investigation, OverWatch quickly uncovered the adversary's use of "sender2" — identified as a file exfiltration tool (also known as Exmatter) — that was executed remotely with PsExec from an unmanaged host.

The sample sender2 executable crawls the computer for files with a list of file extensions and is configured to send them to a remote server via the SFTP or WebDAV protocols. In the activity observed by OverWatch, the tool was set to evade detection in the following ways:

- It executes using the parameter `-nownd`, causing the tool's window to be hidden during execution.
- At the completion of its execution, it launches a PowerShell command to forcibly stop the sender2 process and delete the executable.

Self-deletion powershell.exe command:

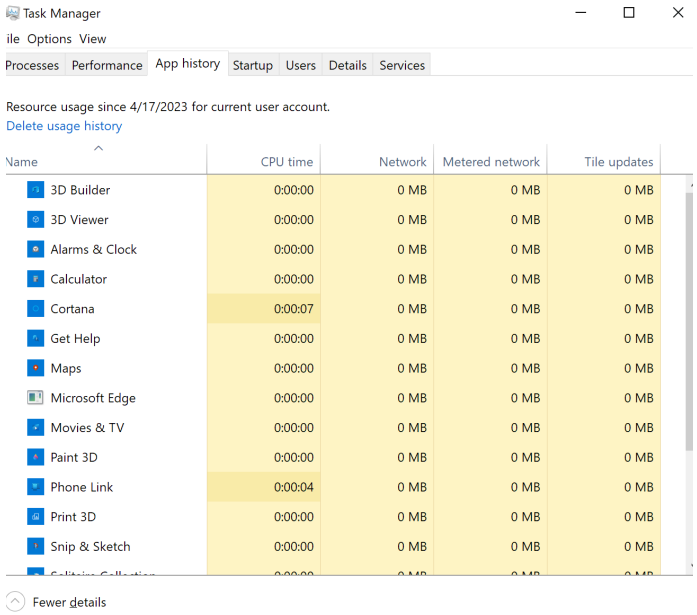
```
powershell.exe -WindowStyle Hidden -C $path = '\\[REDACTED]\123\sender.exe'
```

https://www.crowdstrike.com/blog/falcon-overwatch-contributes-to-blackcat-protection

SRUM

SRUM is the System Resource Usage Monitor

- Built-in to Windows, part of the diagnostic policy service
- Maintains a 30-day history of system activity including programs executed, Wi-Fi networks, network use statistics, energy usage, and more



A	B	C	F	G	H	I
RUM ENTRY NUMBER	SRUM ENTRY CREATION	Application	Profile	Profile Flags	Bytes Sent	Bytes Received
6053	2023-03-27 3:00:00	SSDPSRV	0	Zero	0	11676
6054	2023-03-27 3:00:00		0	Zero	1222751	100492029
6055	2023-03-27 3:00:00	Spooler	0	Zero	0	0
6056	2023-03-27 3:00:00	Dhcp	0	Zero	1582	0
6057	2023-03-27 3:00:00	Dnscache	0	Zero	4110	8381
6058	2023-03-27 3:00:00	wlidsvc	0	Zero	27227	39669
6059	2023-03-27 3:00:00	1\program files\cuassistant\culauncher.exe	0	Zero	2269	3273
6060	2023-03-27 3:00:00	NlaSvc	0	Zero	327	773
6061	2023-03-27 3:00:00	System	0	Zero	5704	548
6062	2023-03-27 3:00:00					
6063	2023-03-27 3:00:00	les (x86)\google\update\googleupdate.exe	0	Zero	915908	50139601
6064	2023-03-27 3:00:00	volume1\windows\system32\sihclient.exe		Zero	4888	14219
		les (x86)\google\update\googleupdate.exe	0	Zero	915908	50139601
6068	2023-03-27 3:00:00	LicenseManager	0	Zero	3411	15135
6069	2023-03-27 3:00:00	DoSvc	0	Zero	34798	1596116
6070	2023-03-27 3:00:00	wlidsvc	0	Zero	12525	34841
6071	2023-03-27 3:00:00	soft\edgeupdate\microsoftedgeupdate.exe	0	Zero	2987	4779
6072	2023-03-27 3:00:00	kvolume1\windows\system32\wermgr.exe	0	Zero	6056	3521
6073	2023-03-27 3:00:00	wuauserv	0	Zero	1699	18457
6074	2023-03-27 3:00:00	DiagTrack	0	Zero	18673	347739
6075	2023-03-27 3:00:00	DsmSvc	0	Zero	5341	2976
6076	2023-03-27 3:00:00	volume1\program files\git\usr\bin\ssh.exe	0	Zero	14182	297162
		volume1\program files\git\usr\bin\ssh.exe	0	Zero	14182	297162

Ransomware Impact

- Once data exfil is complete/initiated, **sometimes** Threat Actors perform ransomware execution
- Backups
  - TAs destroy backups
  - Disable recovery mechanisms like Volume Shadows
  - Clear logs/tracks

Ransomware Deployment

Multiple ways to perform encryption:

- Group Policy Objects (GPOs)
- SCCM
- Manage Engine
- PsExec

Often targets are selected after scanning the environment using scanners

- Angry IP Scanner, Masscan

Hypervisor Jackpotting - Targeting VMware ESXi with ransomware

- Bare-Metal/ Type-1 Hypervisor
- Runs directly on the host
- Based on Linux

Hypervisor Jackpotting - Targeting VMware ESXi with ransomware

Three step process to encrypt ESXi:

- Gain interactive access via SSH (valid credentials)

- List and terminate running VM processes prior to encryption,

- Target the vmfs/volumes datastore path to encrypt disk volumes and snapshots

If SSH is disabled, Threat Actors often enable this by accessing the ESXi console for HTTPS

Hypervisor Jackpotting, Part 1: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ransomware to Maximize Impact

February 26, 2021 Eric Loui - Sergei Frankoff Research & Threat Intel

CROWDSTRIKE | BLOG

Hypervisor Jackpotting, Part 2: eCrime Actors Increase Targeting of ESXi Servers with Ransomware

August 30, 2021 Michael Dawson From The Front Lines

Hypervisor Jackpotting, Part 3: Lack of Antivirus Support Opens the Door to Adversary Attacks

May 15, 2023 CrowdStrike Services - CrowdStrike Intelligence Research & Threat Intel

https://www.crowdstrike.com/blog/carbon-spider-sprite-spider-target-esxi-servers-with-ransomware/

VMware Recommendations

- Ensure ESXi is not exposed to the Internet
- Ensure ESXi management interface is isolated
- SSH is disabled
- Regularly back up ESXi datastore volumes

Must do to protect against Ransomware

- Implement Multi Factor Authentication - **MFA** for **ALL** users on **ALL** external facing services
  - Remove non approved remote management tools
- Limit Privileged Access in your environment
  - Minimize accounts with domain privileges
    - Domain Admin is not the only privileged group
- Use Unique Local Admin Passwords
  - **Local Administrator Password Solution** is your BFF
- Patch Management is critical
  - **PATCH PATCH PATCH** devices, servers and clients
- Backups, offline or WORM

Thanks for listening!

@khannaanurag

https://threathunting.dev/talks/