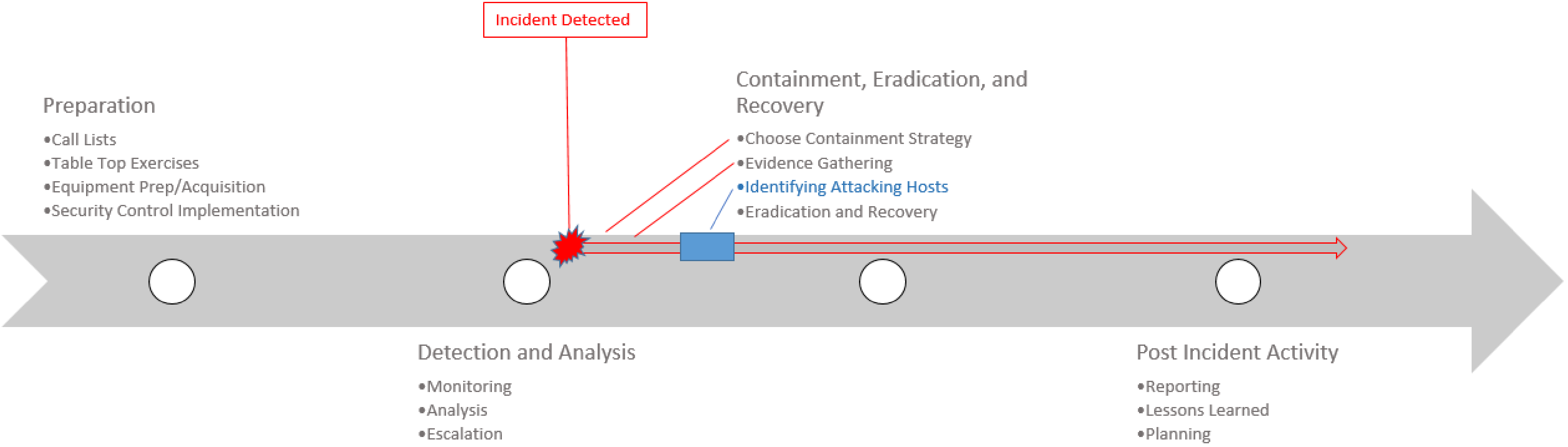
DEAN DORTON FORENSIC ARTIFACT PARSER (D2FAP)

Automating the creation of a unified timeline for triage response

PROBLEM SOLVING

- Initial Response (Triage Phase)
- Direct Containment Efforts
- Plan Remediations
- Provide Concrete Understanding to Leaders

PROCESS



Incident Detected

Preparation

- Call Lists
- Table Top Exercises
- Equipment Prep/Acquisition
- Security Control Implementation

Detection and Analysis

- Monitoring
- Analysis
- Escalation

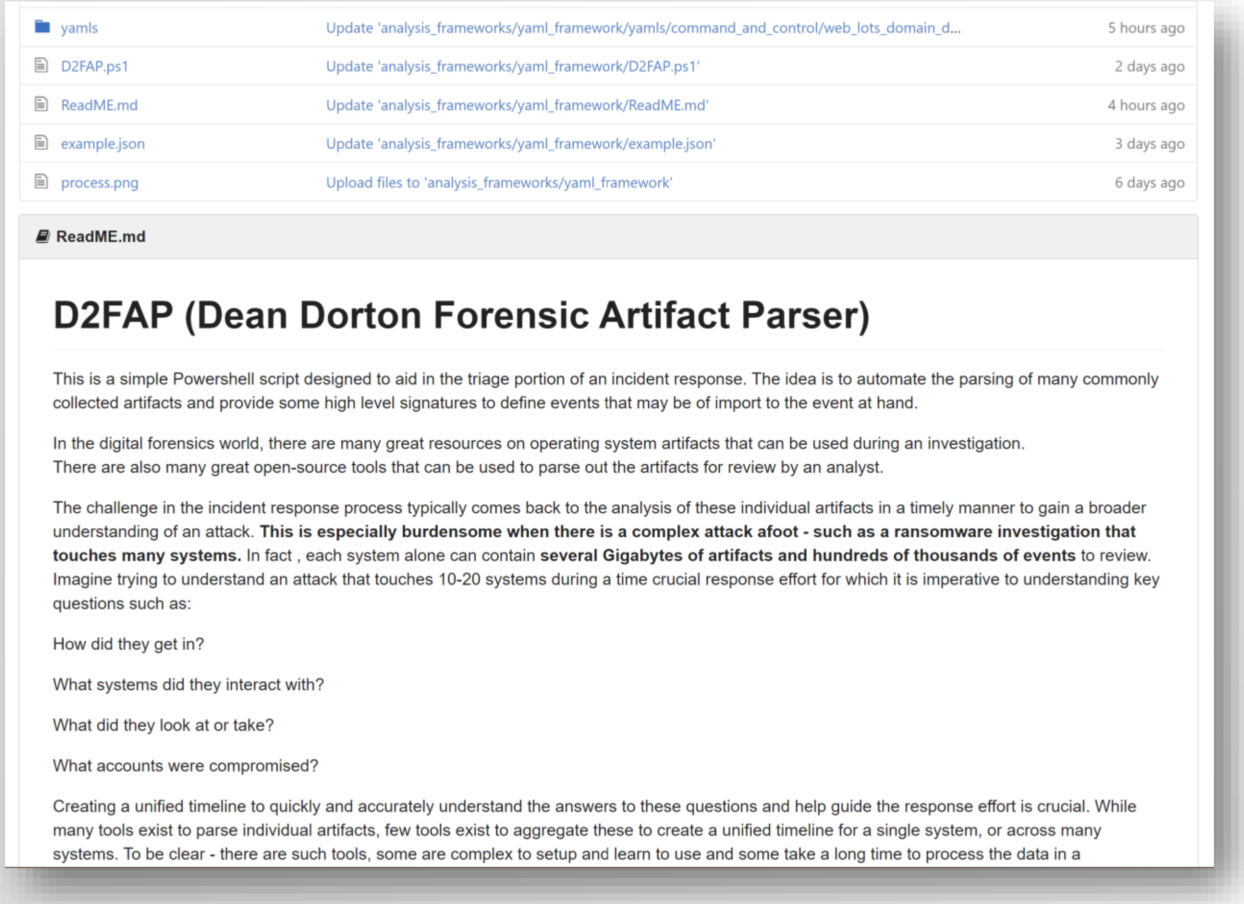
Containment, Eradication, and Recovery

- Choose Containment Strategy
- Evidence Gathering
- Identifying Attacking Hosts
- Eradication and Recovery

Post Incident Activity

- Reporting
- Lessons Learned
- Planning

PURPOSE



yamls	Update 'analysis_frameworks/yaml_framework/yamls/command_and_control/web_lots_domain_d...	5 hours ago
D2FAP.ps1	Update 'analysis_frameworks/yaml_framework/D2FAP.ps1'	2 days ago
ReadME.md	Update 'analysis_frameworks/yaml_framework/ReadME.md'	4 hours ago
example.json	Update 'analysis_frameworks/yaml_framework/example.json'	3 days ago
process.png	Upload files to 'analysis_frameworks/yaml_framework'	6 days ago

ReadME.md

D2FAP (Dean Dorton Forensic Artifact Parser)

This is a simple Powershell script designed to aid in the triage portion of an incident response. The idea is to automate the parsing of many commonly collected artifacts and provide some high level signatures to define events that may be of import to the event at hand.

In the digital forensics world, there are many great resources on operating system artifacts that can be used during an investigation.
There are also many great open-source tools that can be used to parse out the artifacts for review by an analyst.

The challenge in the incident response process typically comes back to the analysis of these individual artifacts in a timely manner to gain a broader understanding of an attack. **This is especially burdensome when there is a complex attack afoot - such as a ransomware investigation that touches many systems.** In fact , each system alone can contain **several Gigabytes of artifacts and hundreds of thousands of events** to review. Imagine trying to understand an attack that touches 10-20 systems during a time crucial response effort for which it is imperative to understanding key questions such as:

How did they get in?

What systems did they interact with?

What did they look at or take?

What accounts were compromised?

Creating a unified timeline to quickly and accurately understand the answers to these questions and help guide the response effort is crucial. While many tools exist to parse individual artifacts, few tools exist to aggregate these to create a unified timeline for a single system, or across many systems. To be clear - there are such tools, some are complex to setup and learn to use and some take a long time to process the data in a

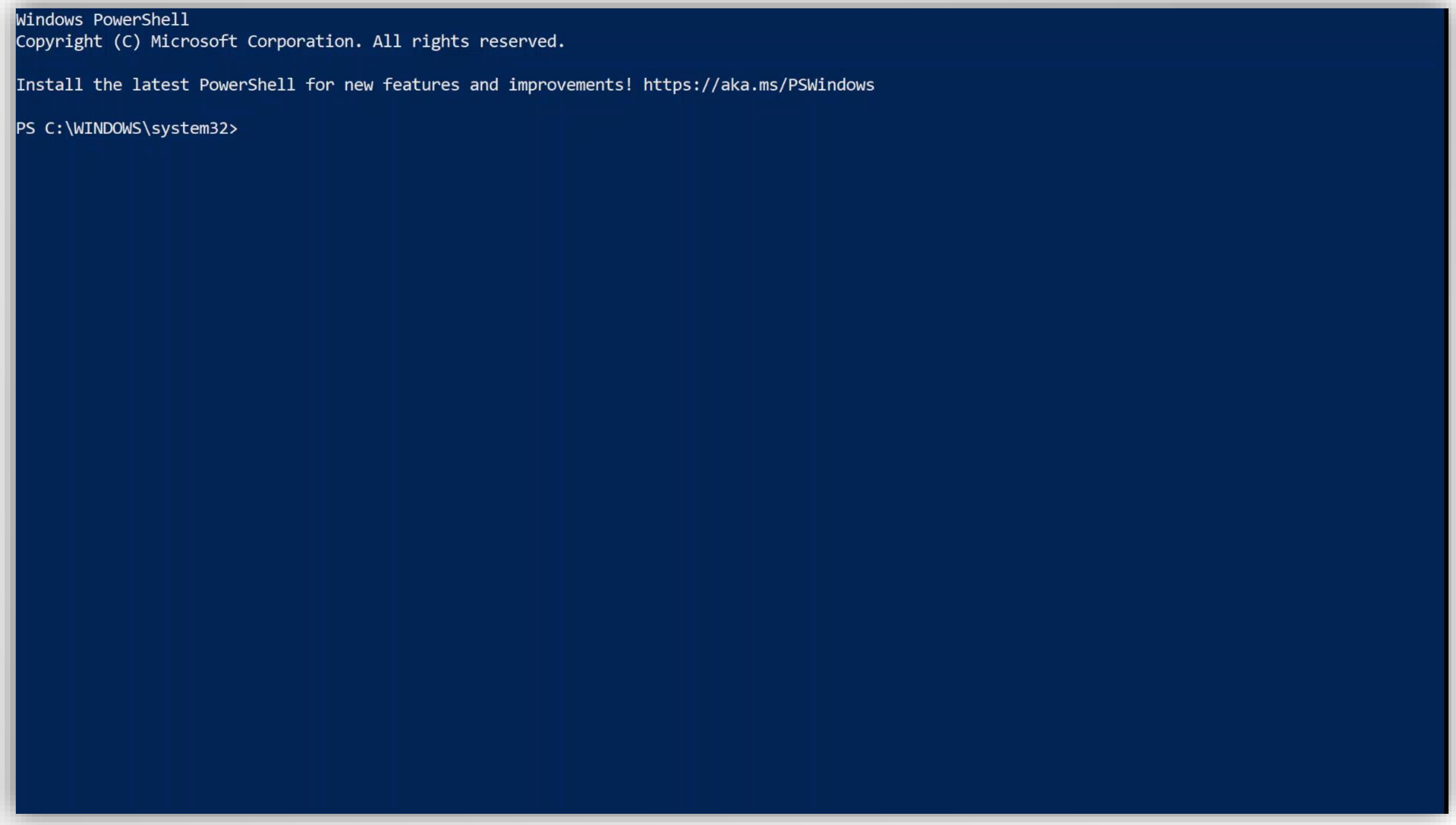
- Automate Parsing of Common Artifacts
- Combine Parsed Artifacts into a Unified Timeline
- Combine Timelines of Disparate Systems
- Apply Simple Intel/Signatures to Artifacts

D2FAP USAGE

- CLI Arguments:

  -Config PATH_TO_CONFIG

- Requirements
  - Powershell v5
  - Local Administrator
  - PowerForensics
  - Powershell-YAML
  - Eric Zimmerman Tools
  - Nirsoft Browsing History Viewer

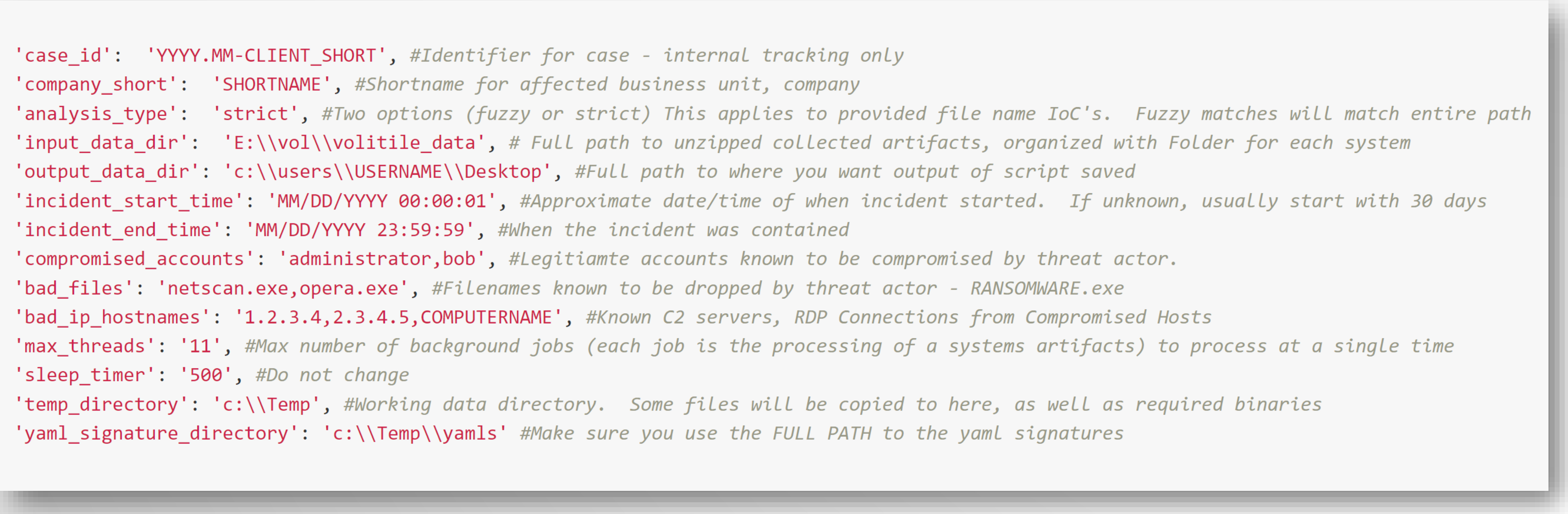


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\WINDOWS\system32>
```

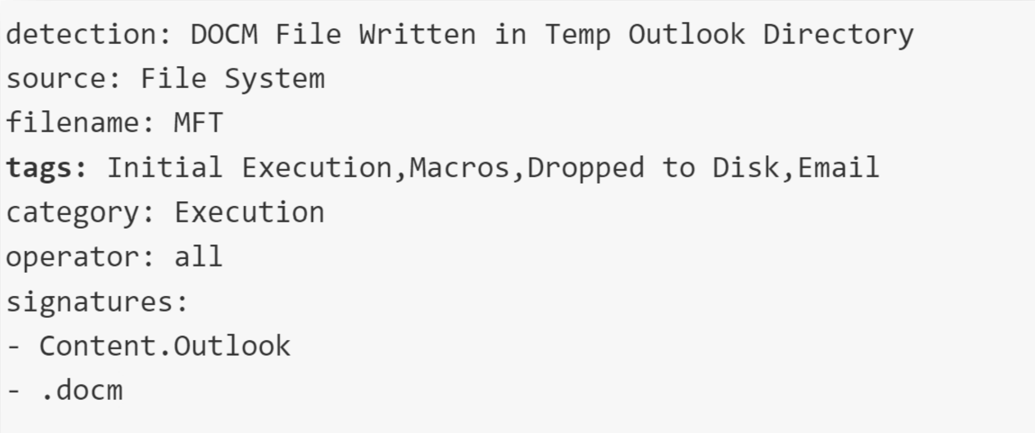
CONFIG FILE



```
'case_id':  'YYYY.MM-CLIENT_SHORT', #Identifier for case - internal tracking only
'company_short':  'SHORTNAME', #Shortname for affected business unit, company
'analysis_type':  'strict', #Two options (fuzzy or strict) This applies to provided file name IoC's.  Fuzzy matches will match entire path
'input_data_dir':  'E:\\vol\\volitile_data', # Full path to unzipped collected artifacts, organized with Folder for each system
'output_data_dir': 'c:\\users\\USERNAME\\Desktop', #Full path to where you want output of script saved
'incident_start_time': 'MM/DD/YYYY 00:00:01', #Approximate date/time of when incident started.  If unknown, usually start with 30 days
'incident_end_time': 'MM/DD/YYYY 23:59:59', #When the incident was contained
'compromised_accounts': 'administrator,bob', #Legitiamte accounts known to be compromised by threat actor.
'bad_files': 'netscan.exe,opera.exe', #Filenames known to be dropped by threat actor - RANSOMWARE.exe
'bad_ip_hostnames': '1.2.3.4,2.3.4.5,COMPUTERNAME', #Known C2 servers, RDP Connections from Compromised Hosts
'max_threads': '11', #Max number of background jobs (each job is the processing of a systems artifacts) to process at a single time
'sleep_timer': '500', #Do not change
'temp_directory': 'c:\\Temp', #Working data directory.  Some files will be copied to here, as well as required binaries
'yaml_signature_directory': 'c:\\Temp\\yamls' #Make sure you use the FULL PATH to the yaml signatures
```

SIGNATURES

- **DETECTION** - Name that appears in the Detection field of the Timeline if matched
- **SOURCE** - Which artifact supported by signatured to parse (BrowserHistory, Event Logs, File System)
- **FILENAME** - Comma separated strings to match filename to be parsed. Security.evtx, MFT (for Master File Table). For event logs, will match on partial file name.
- **TAGS** - Comma separated list of TAG’s to be applied to detected event
- **CATEGORY** - Comma separated list of Kill Chain stage to be applied to the detected event
- **OPERATOR** - ANY or ALL - Simple if any signatures need to match or all
- **SIGNATURES** - Any number of strings that need to be matched when parsing artifacts



```
detection: DOCM File Written in Temp Outlook Directory
source: File System
filename: MFT
tags: Initial Execution,Macros,Dropped to Disk,Email
category: Execution
operator: all
signatures:
- Content.Outlook
- .docm
```

SIGNATURES

Malware Detection - Cisco Amp Behavioral Protection

Malware Detection - Cisco Amp Malicious Activity Protection

Malware Detection - Cisco Amp System Process Protection

Malware Detection - Cisco Amp Script Protection

Malware Detection - Crowdstrike

Malware Detection - Sentinel One

Malware Detection - Symantec Endpoint Protection

Malware Detection - Windows Defender

Defense Evasion - Windows Defender Disabled

Bloodhound CLI Arguments Detected

Collection Tool Detected

Exfiltration Tool Detected

Share Access Detected

Remote Access Tool Detected

ScreenConnect Incoming Connection

Web History - LOTS URL Detected

Credential Theft Technique - CompSpec VSSAdmin Service 1

Credential Theft Technique - CompSpec VSSAdmin Service 2

Credential Theft Technique - CompSpec VSSAdmin Service 3

Credential Theft Technique - CompSpec VSSAdmin Service 4

Cred Dump Tools Dropped Files

DLL File Written in ProgramData Directory

DLL File Written in Public Directory

DUMP File Written in ProgramData Directory

DUMP File Written in Public Directory

DUMP File Written in System32 Directory

EXE File Written in ProgramData Directory

EXE File Written in Public Directory

MIMIKATZ Cli Arguments Detected

Minidump Usage - Possible Credential Theft Technique

PowerShell Veeam Backup Credential Access

ZIP File Written in ProgramData Directory

ZIP File Written in public Directory

ZIP File Written in System32 Directory

PowerShell Antiforensics Commands Detected

PowerShell Windows Defender Disabled Attempt

Event Logs Cleared

Data Discovery Tool Detected

Filesystem Activity - File Opened LNK Created

Port Scanning Tool Detected

PowerShell Discovery Command Detected

Interesting Technique - Certutil Decode

DOCM File Written in Temp Outlook Directory

EXE File Written in ProgramData Directory

Execution Technique - ODBCCONF REGSRV

PowerShell Possible Hacking Tool Execution

XLSM File Written in Temp Outlook Directory

Exfiltration Domains Detected in Browser History

Scheduled Task Created

New Service Installed

Remote Desktop - Inbound Connection

Remote Desktop - Outbound Connection

Application Installation

Application Popup Detected

Suspicious Download File Extension with Bits

Bits Suspicious Task Added by PowerShell

BAT File Written in Startup Directory

EXE File Written in Startup Directory

HTA File Written in Startup Directory

Local Admin Group Updated

Local Group Modified

Local User Account Added

Local Account Password Reset

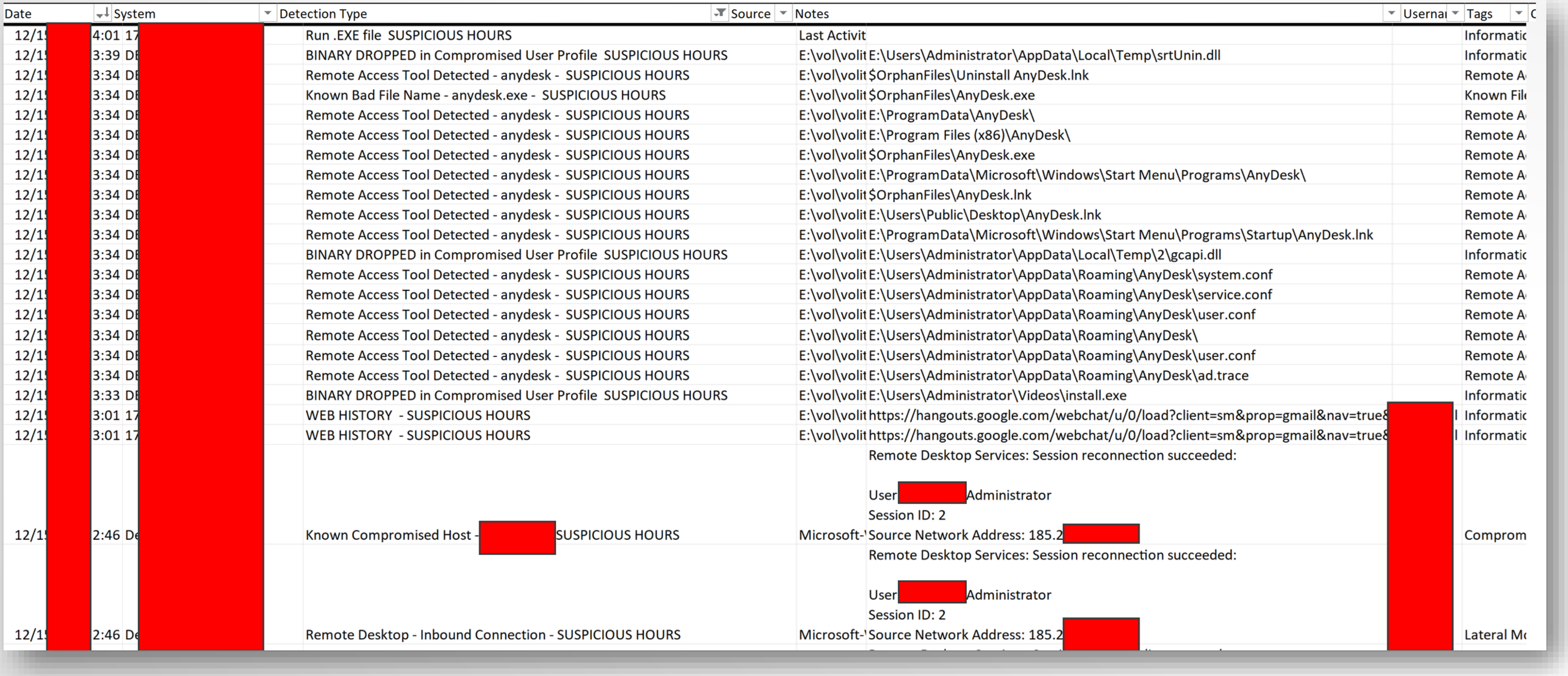
Powerview Add-DomainObjectAcl DCSync AD Extend

VBS File Written in Startup Directory

PowerShell - Possible Mimikatz Execution Attempt

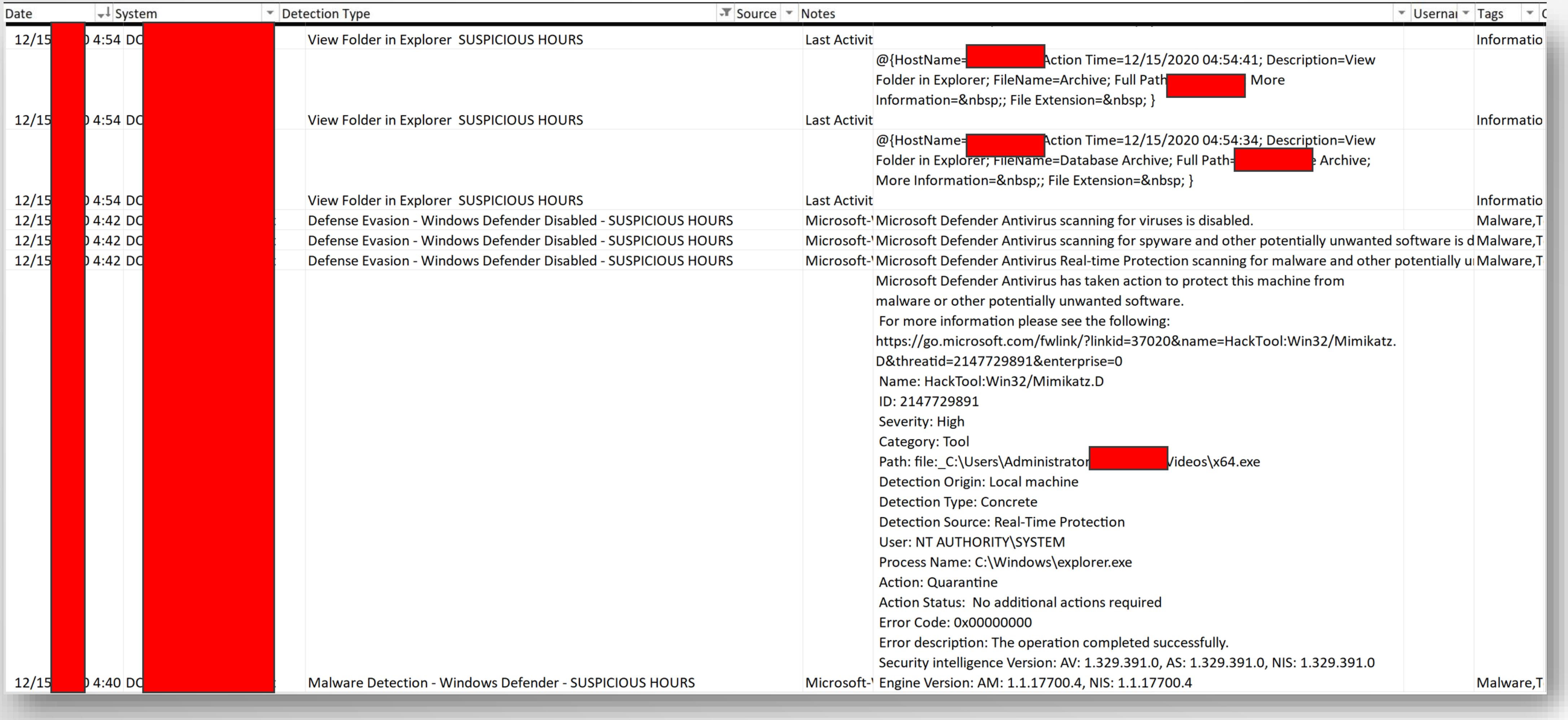
PowerShell Encoded Command Execution

RESULTS



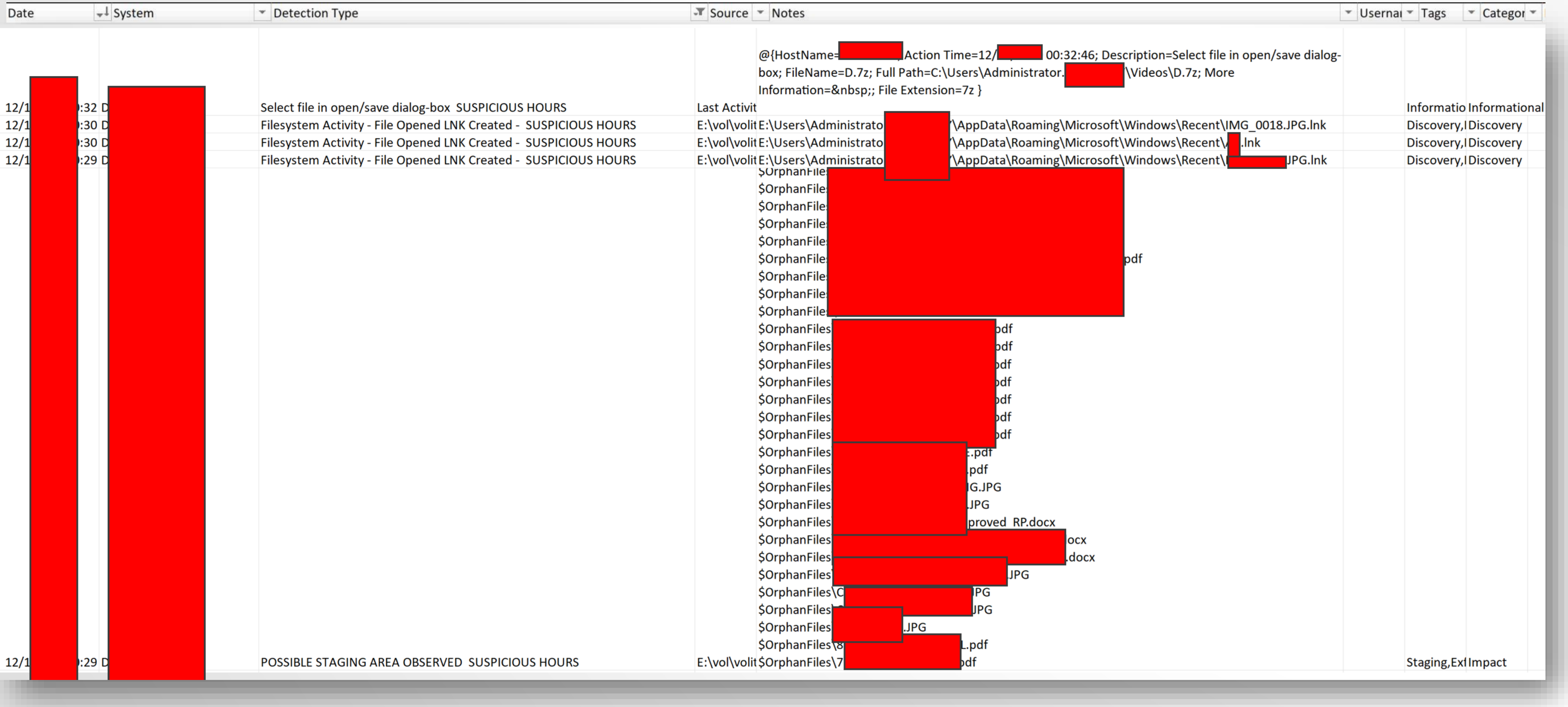
Date	System	Detection Type	Source	Notes	Usernai	Tags	C
12/1[redacted]4:01	17[redacted]	Run .EXE file SUSPICIOUS HOURS	Last Activit			Informatic	
12/1[redacted]3:39	DE[redacted]	BINARY DROPPED in Compromised User Profile SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrator\AppData\Local\Temp\srtUnin.dll		Informatic	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	$OrphanFiles\Uninstall AnyDesk.lnk		Remote A	
12/1[redacted]3:34	DE[redacted]	Known Bad File Name - anydesk.exe - SUSPICIOUS HOURS	E:\vol\volit	$OrphanFiles\AnyDesk.exe		Known File	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\ProgramData\AnyDesk\		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\Program Files (x86)\AnyDesk\		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	$OrphanFiles\AnyDesk.exe		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\ProgramData\Microsoft\Windows\Start Menu\Programs\AnyDesk\		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	$OrphanFiles\AnyDesk.lnk		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Public\Desktop\AnyDesk.lnk		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\AnyDesk.lnk		Remote A	
12/1[redacted]3:34	DE[redacted]	BINARY DROPPED in Compromised User Profile SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrator\AppData\Local\Temp\2\gcapi.dll		Informatic	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrator\AppData\Roaming\AnyDesk\system.conf		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrator\AppData\Roaming\AnyDesk\service.conf		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrator\AppData\Roaming\AnyDesk\user.conf		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrator\AppData\Roaming\AnyDesk\		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrator\AppData\Roaming\AnyDesk\user.conf		Remote A	
12/1[redacted]3:34	DE[redacted]	Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrator\AppData\Roaming\AnyDesk\ad.trace		Remote A	
12/1[redacted]3:33	DE[redacted]	BINARY DROPPED in Compromised User Profile SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrator\Videos\install.exe		Informatic	
12/1[redacted]3:01	17[redacted]	WEB HISTORY - SUSPICIOUS HOURS	E:\vol\volit	https://hangouts.google.com/webchat/u/0/load?client=sm&prop=gmail&nav=true&	[redacted] l	Informatic	
12/1[redacted]3:01	17[redacted]	WEB HISTORY - SUSPICIOUS HOURS	E:\vol\volit	https://hangouts.google.com/webchat/u/0/load?client=sm&prop=gmail&nav=true&	[redacted] l	Informatic	
12/1[redacted]2:46	De[redacted]	Known Compromised Host - [redacted] SUSPICIOUS HOURS	Microsoft-\	Remote Desktop Services: Session reconnection succeeded: User[redacted]Administrator Session ID: 2 Source Network Address: 185.2[redacted]	[redacted]	Comprom	
12/1[redacted]2:46	De[redacted]	Remote Desktop - Inbound Connection - SUSPICIOUS HOURS	Microsoft-\	Remote Desktop Services: Session reconnection succeeded: User[redacted]Administrator Session ID: 2 Source Network Address: 185.2[redacted]	[redacted]	Lateral Mc	

RESULTS



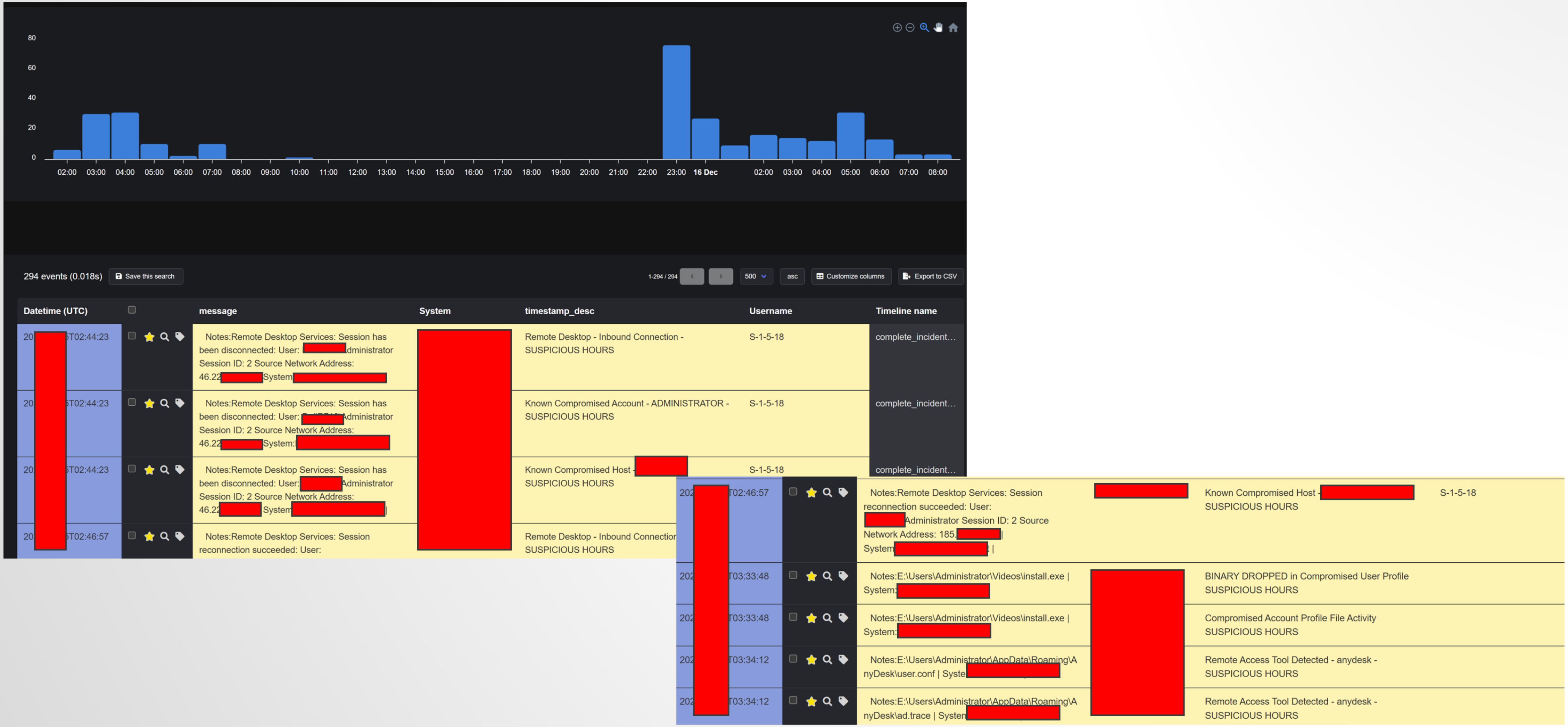
Date	System	Detection Type	Source	Notes	Usernai	Tags	C
12/15[redacted] 4:54	DC[redacted]	View Folder in Explorer SUSPICIOUS HOURS	Last Activit			Informatio	
12/15[redacted] 4:54	DC[redacted]	View Folder in Explorer SUSPICIOUS HOURS	Last Activit	@{HostName=[redacted]Action Time=12/15/2020 04:54:41; Description=View Folder in Explorer; FileName=Archive; Full Path[redacted] More Information= ; File Extension= }		Informatio	
12/15[redacted] 4:54	DC[redacted]	View Folder in Explorer SUSPICIOUS HOURS	Last Activit	@{HostName=[redacted]Action Time=12/15/2020 04:54:34; Description=View Folder in Explorer; FileName=Database Archive; Full Path=[redacted] Archive; More Information= ; File Extension= }		Informatio	
12/15[redacted] 4:42	DC[redacted]	Defense Evasion - Windows Defender Disabled - SUSPICIOUS HOURS	Microsoft-\	Microsoft Defender Antivirus scanning for viruses is disabled.		Malware,T	
12/15[redacted] 4:42	DC[redacted]	Defense Evasion - Windows Defender Disabled - SUSPICIOUS HOURS	Microsoft-\	Microsoft Defender Antivirus scanning for spyware and other potentially unwanted software is d		Malware,T	
12/15[redacted] 4:42	DC[redacted]	Defense Evasion - Windows Defender Disabled - SUSPICIOUS HOURS	Microsoft-\	Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially u		Malware,T	
12/15[redacted] 4:40	DC[redacted]	Malware Detection - Windows Defender - SUSPICIOUS HOURS	Microsoft-\	Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software. For more information please see the following: https://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:Win32/Mimikatz.D&threatid=2147729891&enterprise=0 Name: HackTool:Win32/Mimikatz.D ID: 2147729891 Severity: High Category: Tool Path: file:_C:\Users\Administrator[redacted]Videos\x64.exe Detection Origin: Local machine Detection Type: Concrete Detection Source: Real-Time Protection User: NT AUTHORITY\SYSTEM Process Name: C:\Windows\explorer.exe Action: Quarantine Action Status: No additional actions required Error Code: 0x00000000 Error description: The operation completed successfully. Security intelligence Version: AV: 1.329.391.0, AS: 1.329.391.0, NIS: 1.329.391.0 Engine Version: AM: 1.1.17700.4, NIS: 1.1.17700.4		Malware,T	

RESULTS



Date	System	Detection Type	Source	Notes	Usernai	Tags	Categor
12/1[redacted]:32	D[redacted]	Select file in open/save dialog-box SUSPICIOUS HOURS	Last Activit	@{HostName=[redacted]Action Time=12/[redacted] 00:32:46; Description=Select file in open/save dialog-box; FileName=D.7z; Full Path=C:\Users\Administrator.[redacted]\Videos\D.7z; More Information= ; File Extension=7z }		Informatio	Informational
12/1[redacted]:30	D[redacted]	Filesystem Activity - File Opened LNK Created - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrato[redacted]\AppData\Roaming\Microsoft\Windows\Recent\IMG_0018.JPG.lnk		Discovery,I	Discovery
12/1[redacted]:30	D[redacted]	Filesystem Activity - File Opened LNK Created - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrato[redacted]\AppData\Roaming\Microsoft\Windows\Recent\[redacted].lnk		Discovery,I	Discovery
12/1[redacted]:29	D[redacted]	Filesystem Activity - File Opened LNK Created - SUSPICIOUS HOURS	E:\vol\volit	E:\Users\Administrato[redacted]\AppData\Roaming\Microsoft\Windows\Recent\[redacted]JPG.lnk		Discovery,I	Discovery
12/1[redacted]:29	D[redacted]	POSSIBLE STAGING AREA OBSERVED SUSPICIOUS HOURS	E:\vol\volit	$OrphanFile[redacted] $OrphanFile $OrphanFile $OrphanFile $OrphanFile $OrphanFile pdf $OrphanFile $OrphanFile $OrphanFile $OrphanFiles[redacted]pdf $OrphanFiles pdf $OrphanFiles pdf $OrphanFiles pdf $OrphanFiles pdf $OrphanFiles pdf $OrphanFiles pdf $OrphanFiles[redacted].pdf $OrphanFiles .pdf $OrphanFiles G.JPG $OrphanFiles .JPG $OrphanFiles proved RP.docx $OrphanFiles[redacted]ocx $OrphanFiles .docx $OrphanFiles[redacted].JPG $OrphanFiles\C[redacted]PG $OrphanFiles JPG $OrphanFiles[redacted].JPG $OrphanFiles\8[redacted]L.pdf $OrphanFiles\7 pdf		Staging,Ex	Impact

GOOGLE TIMESKETCH



Datetime (UTC)	☐	message	System	timestamp_desc	Username	Timeline name
20[redacted]5T02:44:23	☐ ★	Notes:Remote Desktop Services: Session has been disconnected: User: [redacted]dministrator Session ID: 2 Source Network Address: 46.22[redacted]System[redacted]	[redacted]	Remote Desktop - Inbound Connection - SUSPICIOUS HOURS	S-1-5-18	complete_incident…
20[redacted]5T02:44:23	☐ ★	Notes:Remote Desktop Services: Session has been disconnected: User: [redacted]dministrator Session ID: 2 Source Network Address: 46.22[redacted]System:[redacted]	[redacted]	Known Compromised Account - ADMINISTRATOR - SUSPICIOUS HOURS	S-1-5-18	complete_incident…
20[redacted]5T02:44:23	☐ ★	Notes:Remote Desktop Services: Session has been disconnected: User:[redacted]Administrator Session ID: 2 Source Network Address: 46.22[redacted]System[redacted]|	[redacted]	Known Compromised Host [redacted] SUSPICIOUS HOURS	S-1-5-18	complete_incident…
20[redacted]5T02:46:57	☐ ★	Notes:Remote Desktop Services: Session reconnection succeeded: User:	[redacted]	Remote Desktop - Inbound Connection SUSPICIOUS HOURS		

202[redacted]T02:46:57	☐ ★	Notes:Remote Desktop Services: Session reconnection succeeded: User: [redacted]Administrator Session ID: 2 Source Network Address: 185.[redacted]| System[redacted] |	[redacted]	Known Compromised Host - [redacted] SUSPICIOUS HOURS	S-1-5-18
202[redacted]T03:33:48	☐ ★	Notes:E:\Users\Administrator\Videos\install.exe | System:[redacted]	[redacted]	BINARY DROPPED in Compromised User Profile SUSPICIOUS HOURS	
202[redacted]T03:33:48	☐ ★	Notes:E:\Users\Administrator\Videos\install.exe | System:[redacted]		Compromised Account Profile File Activity SUSPICIOUS HOURS	
202[redacted]T03:34:12	☐ ★	Notes:E:\Users\Administrator\AppData\Roaming\AnyDesk\user.conf | Syste[redacted]		Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	
202[redacted]T03:34:12	☐ ★	Notes:E:\Users\Administrator\AppData\Roaming\AnyDesk\ad.trace | Systen[redacted]		Remote Access Tool Detected - anydesk - SUSPICIOUS HOURS	

STORIES…..

- Learn a Scripting Language
- Learn How to Parse Various Data Structures
- Learn Methods for Turning Unstructured Data into Structured Data
- Identify Key Opportunities to Automate Tasks
  - Especially when fast turnaround is required!

KEY TAKEAWAYS

THANKS