Windows Experts [~] Shape-Shifting Malware

Introduction

In this document, I'm going to cover a forum post that I submitted to [bleepingcomputer.com], at this link:
https://www.bleepingcomputer.com/forums/t/768015/windows-experts-check-out-the-virus-that-no-one-wants-to-acknowledge

I'm about to reveal some of my [research capabilities], as well as my [writing] and [communication skills], so that [anybody and their mother], who [carefully reads] what I [write], and [carefully examines] the [exhibits] that I have to [share] can [easily determine] that I'm [an expert at what I do].

...and that I have the same technological capabilities as those who work for the [GTAG/Google Threat Analysis Group], or [Microsoft Research].

The [forum post] is me [specifically] talking about a [cyberattack] that I [caught on video] and in a [number of files] and [logs] after I posted [this particular video] to [Facebook]...

02/25/22	Censorship on Facebook	https://youtu.be/Jmq4yBqGhTs

Allow me to explain what's happening in that video.

I commented on somebody's post → my post didn't violate any rules or anything → it was immediately removed.
That is mainly because the owner of [Facebook] has been having a [surrogate] of his aggressively censoring my account and various aspects of my experience on [Facebook].

Though to be perfectly clear, the [surrogate] could very well be the [Central Intelligence Agency], as I often write about [Julien Assange] and [Edward Snowden], and the [Central Intelligence Agency] does not take kindly to [anybody] who talks about them, or other [famous dissidents].

I'm going to cover a number of other details as well, particularly this video right here...

02/17/22	A Matter of National Security	https://youtu.be/e4VnZObiez8

...as well as...

02/26/22	After Midnight/Assassin (BSOD)	https://youtu.be/40sQXpVh_8Y
02/26/22	After Midnight/Assassin (Desktop/OBS Angle)	https://youtu.be/LYVUMLpofWg
02/26/22	After Midnight/Assassin (Smartphone Angle)	https://youtu.be/oShPs6_uXIk

Please consider the dates listed above, as there are multiple indicators in the [research] below, that I did, as well as [development] of this particular log file:

02/26/22	https://github.com/mcc85s/FightingEntropy/blob/main/2022_0226-(Serious%20Cyberthreat).txt

These are things that I mentioned to (3) dudes from the [Saratoga County Sheriffs Office] in [New York State]...

03/01/22	SCSO being morons	https://drive.google.com/file/d/1BNfF9vWjG4vBIO-8oXmIw6aLeNvFRjRL

...but they are fuckin' stupid.

They decided to [thoroughly examine] the [evidence] without even [looking] at [any] of it, and they were able to arrive at an [adamantly firm conclusion], that there was [no way] that the [Russians] or [Chinese] were involved in [hacking my equipment], in [any of the videos I recorded], [listed above].

Because, even though they don't even have a [cybercrimes division]...?

[They're the experts], and I'm not. Experts who [didn't see] any of this [critical supporting evidence] before forcibly dragging me to [Saratoga Hospital] for an [involuntary admission].

03/01/22	https://github.com/mcc85s/FightingEntropy/blob/main/Records/SCSO-2022-013379.pdf

Sounds stupid, right...? Wrong.
It's not stupid at all.
You gotta keep in mind, they have the ability to [teleport] and [travel backward and forward in time].
And with those capabilities, they are never able to be [proven incorrect] or otherwise [wrong].

Introduction

Comment List

Index	Username	Posts	Posted
1	EyeMinUrHeadz	21	02/02/2022 03:53
2	EyeMinUrHeadz	21	02/02/2022 03:57
3	Budapest	27537	02/02/2022 04:02
4	EyeMinUrHeadz	21	02/02/2022 09:18
5	ET_Explorer	5495	02/02/2022 09:30
6	EyeMinUrHead	21	02/02/2022 11:34
7	Budapest	27537	02/02/2022 14:53
8	EyeMinUrHead	21	02/03/2022 22:02
9	EyeMinUrHead	21	02/03/2022 22:16
10	ET_Explorer	5495	02/03/2022 22:34
11	Budapest	27537	02/03/2022 23:06
12	EyeMinUrHead	21	02/04/2022 01:09
13	Budapest	27537	02/04/2022 01:38
14	ET_Explorer	5495	02/04/2022 02:40
15	Torchwood	231	02/04/2022 13:18
16	Budapest	27537	02/04/2022 15:12
17	aquaenigma	14	02/05/2022 04:39
18	Chris Cosgrove	23339	02/05/2022 04:46
19	EyeMinUrHead	21	02/18/2022 23:13
20	EyeMinUrHead	21	02/18/2022 23:14
21	EyeMinUrHead	21	02/18/2022 23:17
22	EyeMinUrHead	21	02/18/2022 23:26
23	Budapest	27537	02/19/2022 00:23
24	EyeMinUrHead	21	02/19/2022 17:43
25	EyeMinUrHead	21	02/19/2022 20:42
26	Budapest	27537	02/19/2022 21:10
27	greg18	1332	02/19/2022 22:04
28	mcc85s	2	03/22/2022 04:46
29	Budapest	27537	03/23/2022 18:08
30	mcc85s	2	03/25/2022 07:46
31	EyeMinUrHead	21	08/02/2022 00:27
32	EyeMinUrHead	21	08/21/2022 11:57
33	electricult	1	08/25/2022 01:37
34	TheUnluckyOne	2	03/02/2023 19:23

Comment [01: EyeMinUrHeadz]

Index : 1
Username : EyeMinUrHeadz
Posts : 21
Posted : 02/02/2022 03:53

Started out in the [malware arena].
A [stalwart warrior] stepped forward, to offer the [cleansing ritual] that had cleared most of the plague
[a thousand times and running].

But- he found out that this is [rubber] and you are [glue].
And it bounced off [him] and [slowly chips away at your data], as it systematically
(and seeming on a timed basis) [erodes your ability to control your own machine] before it comes out right
before you, with a:

[System]: Here's an update you don't have scheduled at all, but it's not really an update.
It's a script from hell that'll put you in a [script from hell] for the rest of your existence while
we pilot the real thing from the shadows...

...style [haymaker] that leaves [you] seriously [WTF'ked].

You're [amazed].
And, [impressed] the first few times...

But, after the 10,000th [Windows] re-install...?
You start to learn how [bleakly hopeless] this is looking.

You get angry, and you get all:
[You]: REALLY???!
REALLY?!

ALL I DID WAS DISABLE ONE SERVICE THAT WAS WRECKING MY INTERNET SPEED!

Then you have to have a conversation with yourself, about how much of your computer you will allow someone else to have... just so that you can have SOME of the computer. Because, he's calling the shots by now.

He's make [little tiny drives] on [every drive] you have.
You can't let a [media device] touch your computer, without it putting itself on it.
It's on your [phone], you [tablet], you [laptop], your [desktop], maybe worse...
Like your [work computer].

[No one is taking this very seriously].
There's a very nasty thing out there that is capable of stopping things.
Cold.

What kind of things...?
Major things.
So, can someone take a BLEEPING LOOK at what I'm trying to showcase here?!

Because, all it takes is for someone to get [sandboxed]... think it's all fine and dandy, and introduce it to the [wrong place]. Like I (almost did/hopefully didn't).

What would some big super [Windows Expert] need, to see to get their [socks blown off]...?

Please let me know, so that I can [show you what happens] when there's [nothing you can do] on your own computer anymore that [isn't controlled by something else].

There is no more [clean install].
That option is [gone].

Allow me to show you how.
Just let some brave soul step forward and say:
[Somebody]: Ok, crazy boy.
            Just do this, and post what it says, or what you see.
[You]   : I will do what you say.

Eat your [Wheaties].
Eat your [Flintstone vitamins].
Put on your [big boy pants].

Then, try to figure out how to [fight yourself] out of a [Windows 95] instance that looks like [Windows 11] while you listen to your [fans] crank up to [high heaven], just because you opened [Notepad].

There's a bunch of stuff I [run in] and [do] right after I [reinstall Windows]. (Up to 10 times a day on days off)
But, [here's a few pics of the registry] and [other directories] that you get to start out with when this nasty thing is on your machine.

And I'll throw in some (*.inf) files that make me scratch my head.
Please let me know if this is the [standard stuff].

This is [machine.inf].
It seems to be the [core file] to help your [system] get [even more cool stuff].

The thing I love most about these files, is that [Microsoft] was nice enough to add [color-coded flavor text] and [instructions] for us to [open/modify] [Windows]' files.

That's what this is, right...?

Log:

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Logs/01-01.log |

Here's some registry entries you always start with:

Attached Thumbnails:

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/01-01.png |
| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/01-02.png |

_____/ Comment [01: EyeMinUrHeadz]

Comment [02: EyeMinUrHeadz]

Index : 2
Username : EyeMinUrHeadz
Posts : 21
Posted : 02/02/2022 03:57

Here's a [DISM] command I just ran after I told [Windows] not to update a damn thing for two weeks:

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Logs/02-01.log |

Comment [03: Budapest]

Index : 3
Username : Budapest
Posts : 27537
Posted : 02/02/2022 04:02

So what is the actual problem? What makes you suspect a virus?

| Quote | What kind of things? Major things. |

Describe them. [(← He did describe them, but the message needed to be dissected)]

Can you give us a few particulars.
Version of Windows...? [(← Guy did not look at the logs that the OP posted, cops do this too)]

I assume [Win10] because you posted in the [Win10] forum, but you mention [Win95].

[Make] and [model number] of your [computer].

I do not want to appear [rude] or [condescending], but maybe it's a [touch of paranoia] and
[nothing] is actually wrong. [(← Cops and psychiatrists do this too, before looking at
evidence that was already provided, typically because [they do not understand the evidence])]

| The power of [accurate observation] is commonly called [cynicism] by those who haven't got it. |
| -George Bernard Shaw |

Comment [04: EyeMinUrHeadz]

Index : 4
Username : EyeMinUrHeadz
Posts : 21
Posted : 02/02/2022 09:18

Greetings.
So... It all started with [late night turn-ons], er... the computer [turning on at night by itself].

And [lack of performance].
And when nothing was running, the system was.
Hard.
[Permissions disappeared], programs either showed up [spontaneously] or would not go away.

I installed [Windows 11 Pro] (this was just the forum that the kind [Nasdaq] linked me to from the other forum),
and had some [programs] telling me that it didn't work with [Windows NT] when attempting to install them.

There was a lot of [network activity] for me cutting everything down, except for the [IPv4] and then a lot of
[strange devices] started showing up in [Device Manager] (see attachment). [(← Attachment not there)]

When I got rid of something I knew I didn't want (running/having around), I noticed that I could no longer boot
into [Windows]. I'd have to reinstall the [whole program again], because something would end up happening to my
[restore points] and [backups].

Then [Chrome] goes off into a different folder, and all these [weird processes] start popping up from the
[Program Data] folder or from deep within my [user folder]. Then devices start to act strange, so you go take

a look in [Device Manager] and discover that they were [reconfigured] by some strange (*.inf) files that have [instructions] for [editing] and [customizing them].

And then you notice that you can't even get it to accept that:
[This is a home computer; it's not part of a business network]

And then you notice that there's a whole lot of [DCOM] goings on for a [non-networked home PC].
Which leads to: [evil shims], the virtue of [persistence], and things being [compatible].

I want this to be [paranoia].
But- [it puts me in the closet and takes away all my toys].

Earlier, right after I made the posts in this thread, [Chrome] shut down, and memory usage went up and stayed at [99%] until everything started getting really skittish and my fan blades were about to fly off.

[Process Hacker] listed the unknown process "C:\" as one of many vaguely named similar process that were just... [using all the memory all of a sudden]. I don't think that's [paranoia], but I admit I could have somehow create that issue myself with all my paranoia-proofing after this [Windows] install.

I will not have my feelings hurt, if someone takes [a real look at this], and tells me:

[Dude]: Hey stupid.
        You got what we folks here at [Bleeping Computer] like to call 'F-ing Windows.'
        Stop screwing with it, because there's nothing wrong with it.

I don't think that's the case. [(← I don't either, I think you're just really intelligent, and people have a hard time understanding someone THAT intelligent)]

[This computer] was [assembled] by [me] like [two years ago].

AMD Ryzen 7 3800X
XFX AMD x590 Fatboy
ASUS TUF Gaming 570x Plus Wi-Fi
32 GB Corsair memory
32 GB XPG memory
2x 1GB NVMe
2GB Samsung Evo SSD

So, what can I show you that would make you scratch your head and say [Well, that's odd...?]

_____/ Comment [04: EyeMinUrHeadz]

Comment [05: ET_Explorer] /-----\

Index   : 5
Username : ET_Explorer
Posts   : 5495
Posted   : 02/02/2022 09:30

| Quote | The computer turning on at night by itself |

Why does my computer randomly turn on at night?

The problem computer turns on by itself at night may be caused by the scheduled updates which are designed to wake up your system so as to perform the scheduled [Windows Updates]. Therefore, in order to solve this issue computer turns on itself on Windows 10, you can try to disable those scheduled Windows updates.

| Useless link | https://www.minitool.com/backup-tips/computer-turns-on-by-itself.html |

_____/ Comment [05: ET_Explorer]

Comment [06: EyeMinUrHead] /-----\

Index   : 6
Username : EyeMinUrHead
Posts   : 21
Posted   : 02/02/2022 11:34

I feel like you didn't truly get the essence of what I was trying to say... [(← Agreed)]

Also: I deleted [all scheduled tasks] (except for the [Update Orchestrator] which I can't delete) and [paused updates].

I was just saying that was [one of the strange things] that [led me to believe] that there is actually
[something wrong] [(← Yeah, someone from (the Central/a foreign) Intelligence Agency is spying on you)] and that
I'm not in the group of people pointing at legit [Windows] files, and thinking they're [malware].

Which I still might be doing.

_____/ Comment [06: EyeMinUrHead]

Comment [07: Budapest] /-----\

Index : 7
Username : Budapest
Posts : 27537
Posted : 02/02/2022 14:53

[There is a lot to process here]. Let's try to get to a [bit more specific] on a few items.

[(^ Good idea, but- I'll explain why this doesn't actually matter, shortly)]

| Quote | Programs either showed up spontaneously, or would not go away |

What are the names of these programs...?

| Quote | A lot of strange devices started showing up in Device Manager (see attachment) |

Nothing was attached. [(← Correct)]
What are the names of these strange devices...?

| Quote | All these weird processes start popping up from the Program Data folder, |
| or from deep within my user folder |

What are the names of these processes?

| The power of [accurate observation] is commonly called [cynicism] by those who haven't got it. |
| -George Bernard Shaw |

_____/ Comment [07: Budapest]

Comment [08: EyeMinUrHead] /-----\

Index : 8
Username : EyeMinUrHead
Posts : 21
Posted : 02/03/2022 22:02

Ok. We're moving now.

All valid questions [Mr. Budapest].

[Firstly] I'd like to make a [blanket statement] by saying that it is by far, easier for me to [answer questions]
like THAT, by SHOWING [files/keys/settings] on my computer, (rather) than to do so by listing them.

I didn't keep [perfect logs], but I have [a lot of files] renamed and moved, even though I've lost a lot.

Secondly, I'm going to have to take pictures of my screen.
Because my [snipping tool gets cut off].

Now, this is MOST PROBABLY from me screwing with something.
I'll take the big on that.

What I can do really easily right now is post the DevManager info I tried to attach last post.

_____/ Comment [08: EyeMinUrHead]

Comment [09: EyeMinUrHead] /-----\

Index : 9
Username : EyeMinUrHead
Posts : 21
Posted : 02/03/2022 22:16

Now, that's just the [System Devices] folder.

And I think that is almost all fake devices created by dirty (*.inf) files that are actually ways for my [processor throttle to be controlled remotely].

WHAT WOULD YOU HAVE TO SEE TO BE CONVINCED??? [(← Start recording videos of this)]

Comment [10: ET_Explorer]

Index : 10
Username : ET_Explorer
Posts : 5495
Posted : 02/03/2022 22:34

How do you know that someone is remotely controlling your computer.

Do you see strange activity going on with your computer, mouse cursor moving on its own etc.

[Edited by ET_Explorer, 03 February 2022 - 10:49 PM]

Comment [11: Budapest]

Index : 11
Username : Budapest
Posts : 27537
Posted : 02/03/2022 23:06

Now, that's just the [System Devices] folder.

> Quote | And I think that is almost all fake devices created by dirty (*.inf) files that are actually ways for my [processor throttle to be controlled remotely].

None of those entries look unusual.
Looks very similar to what I see on my own computer.

> The power of [accurate observation] is commonly called [cynicism] by those who haven't got it.
> -George Bernard Shaw

Comment [12: EyeMinUrHead]

Index : 12
Username : EyeMinUrHead
Posts : 21
Posted : 02/04/2022 01:09

Well...
There's less [mouse moving] and more [DCOMMS-related script execution] which leads to [fake windows update package installation] and [file execution through RPC].

Keep in mind this is a home computer that doesn't want to be networked.
And, I turned off the stuff in [group policy] about [ramdisks] and [nvram], yet still have a [registry entry] which makes a [ramdisk] as the [boot device] (*attach 1*) and had all sorts of weird stuff like (*attach 2*).

And find little breadcrumbs laying around, like (*attach 3*) when you're "*running*" [Win 11 Pro]?

Gentlemen I beg you: Tell me what to show you so that you may judge. Tell me what will could sway your doubt.

I could show you a bunch of things I think are jacked up.
But I need to show you what you have to see.
So tell me what the F those things are.

Please. With sugar on top.

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/12-01.jpg |

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/12-02.jpg |
| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/12-03.jpg |

Comment [12: EyeMinUrHead]
Comment [13: Budapest]

Index   : 13
Username : Budapest
Posts   : 27537
Posted   : 02/04/2022 01:38

I cannot read the first two attachments.

The third attachment - what is that?
What did you do to bring up that dialog box?

==========
| The power of [accurate observation] is commonly called [cynicism] by those who haven't got it. |
| -George Bernard Shaw |
==========

Comment [13: Budapest]
Comment [14: ET_Explorer]

Index   : 14
Username : ET_Explorer
Posts   : 5495
Posted   : 02/04/2022 02:40

If you wish, you could [reinstall windows] and make sure you >>
[disable windows remote desktop], preventing intruders from accessing your computer remotely.

Comment [14: ET_Explorer]
Comment [15: Torchwood]

Index   : 15
Username : Torchwood
Posts   : 231
Posted   : 02/04/2022 13:18

I'm intrigued why is google running from appdata, should be running straight from C

I also see IObit, they were hacked awhile back, and sent phishing emails.... did you open one
[Edited by Torchwood, 04 February 2022 - 01:51 PM].

Comment [15: Torchwood]
Comment [16: Budapest]

Index   : 16
Username : Budapest
Posts   : 27537
Posted   : 02/04/2022 15:12

Apparently debug showing the wrong operating system is a common bug with notepad++.

https://github.com/notepad-plus-plus/notepad-plus-plus/issues/11011

==========
| The power of [accurate observation] is commonly called [cynicism] by those who haven't got it. |
| -George Bernard Shaw |
==========

Comment [16: Budapest]
Comment [17: aquaenigma]

Index   : 17
Username : aquaenigma

Posts   : 14
Posted   : 02/05/2022 04:39

Hi I've [messaged you], but I notice all the PCI's in your files.

There's a [vulnerability] in [ACPI], they are in the [firmware].

If it is being [executed] from [remote VM], you will find it in [registry].

I'll need to [look at my logs] to tell you [where to look], but [I do believe you].

Your [hard drive] is probably not even yours, as [they wipe it] and [run everything] from
[their end]. Is there a mention of [RAID] anywhere in those files?

I'm short of time just now but I will pop back with a note of where you need to look.

Comment [18: Chris Cosgrove]

Index   : 18
Username : Chris Cosgrove
Posts   : 23339
Posted   : 02/05/2022 04:46

@ aquaenigma #17

From the Forum rules:

| Quote | All help must be provided in the forums or on our [Discord Server] |

We [do not allow support] to be [provided] or [requested] via [personal message],
[email], or [remote desktop control programs (Logmein, TeamViewer, etc)].

The reason for this is quite simple.
If [mistaken] or [incorrect advice] is given in [open forum], then [any such errors] will be
[quickly picked up] and [corrected].

This is not the case if other channels are used.

Chris Cosgrove

Comment [19: EyeMinUrHead]

Index   : 19
Username : EyeMinUrHead
Posts   : 21
Posted   : 02/18/2022 23:13

Finally able to get on here. Don't know if I opened one of those emails.

Has anyone heard of MAML? Check out these things I've found since last post. It's been hard.
Just see if anything looks like it could help.

Comment [20: EyeMinUrHead]

Index   : 20
Username : EyeMinUrHead
Posts   : 21
Posted   : 02/18/2022 23:14

[One]
Attached Thumbnails:

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/20-01.jpg |
| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/20-02.jpg |

Comment [21: EyeMinUrHead]

Index : 21
Username : EyeMinUrHead
Posts : 21
Posted : 02/18/2022 23:17

[Two]
Attached Thumbnails:

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/21-01.jpg |

Comment [22: EyeMinUrHead]

Index : 22
Username : EyeMinUrHead
Posts : 21
Posted : 02/18/2022 23:26

It won't let me [upload] any of the [damn pictures].

But- it goes something like this I think: the use of MAML
(https://en.wikipedia.org/wiki/Microsoft_Assistance_Markup_Language?wprov=sfla1)
to execute [PowerShell scriptlets] combined with [XML compilers] to change malicious
files into [compatibility shims] and [code] which is [injectable] to (*.dll)'s.

When [Windows] is installed, it [downloads] the real bad bleep.
The next step is a [well-executed systematic takeover] with [full ownership].

If that ain't EXACTLY it, is [pretty damn close].
Someone alert the [authorities]. [(← Probably IS the authorities doing that)]

Comment [23: Budapest]

Index : 23
Username : Budapest
Posts : 27537
Posted : 02/19/2022 00:23

[amdkmpfd.inf] is related to the driver for your graphics chip.
It is not malicious. [(← it was shimmed into becoming malicious.)]

| The power of [accurate observation] is commonly called [cynicism] by those who haven't got it. |
| -George Bernard Shaw |

Comment [24: EyeMinUrHead]

Index : 24
Username : EyeMinUrHead
Posts : 21
Posted : 02/19/2022 17:43

The strange thing about [RAID] in the [BIOS] boot:

Attached Thumbnails:

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/24-01.jpg |

Comment [25: EyeMinUrHead]

/----------

Index : 25
Username : EyeMinUrHead
Posts : 21
Posted : 02/19/2022 20:42

[Boot partition] sector image:

Attached Thumbnails:

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/25-01.jpg |

_____/ Comment [25: EyeMinUrHead]
Comment [26: Budapest] /----------\
/----------

Index : 26
Username : Budapest
Posts : 27537
Posted : 02/19/2022 21:10

| Quote | The strange thing about [RAID] in the [BIOS] boot |

What is strange about it?
==========
| The power of [accurate observation] is commonly called [cynicism] by those who haven't got it. |
| -George Bernard Shaw |
==========

_____/ Comment [26: Budapest]
Comment [27: greg18] /----------\
/----------

Index : 27
Username : greg18
Posts : 1332
Posted : 02/19/2022 22:04

Quote	Budapest, on 19 Feb 2022 - 9:10 PM, said:
	Quote	The strange thing about [RAID] in the [BIOS] boot	

What is strange about it?
It has to be strange because the OP is just trolling everyone.

_____/ Comment [27: greg18]
Comment [28: mcc85s] /----------\
/----------

Index : 28
Username : mcc85s
Posts : 2
Posted : 03/22/2022 04:46

I don't think the OP is trolling anybody. I had an incident almost a month ago where my system went into
a BSOD [https://youtu.be/40sQXpVh_8Y], and then it created a [kernel dump file] among many other things.

I spent like (12) hours doing some [forensics] on the system, here's a 100K log file that shows [SFC],
[DISM], and [CBS] with [strange peculiar errors] that feel like the [system files were being shimmed].

[Serious Cyberthreat]
https://raw.githubusercontent.com/mcc85s/FightingEntropy/main/2022_0226-(Serious%20Cyberthreat).txt

(The above link is a 14.3MB text file, so I chunked it out.)

| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-01.log |
| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-02.log |

| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-03.log |
| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-04.log |
| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-05.log |
| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-06.log |
| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-07.log |
| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-08.log |
| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-09.log |
| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-10.log |

What is not in those links, are many, many files that I found which seemed questionable to me, on the system.

Basically when analyzing the system after the BSOD, I found a number of folders in the [Windows] folder that weren't named a typical name at all... I used [WinDbg] to scope out the dump file AFTER I made the log up above, and it suggests that the file...

[C:\WINDOWS\System32\DriverStore\FileRepository\asussci.inf_amd64_436e2c8baeab176f\asussci.inf]

As well as [ASUSSAIO.sys], was causing the BSOD which led to the [kernel dump file].

There are a couple of [Asus files] listed in that log, [one] of them one pertains to a certificate that uses a [compromised Microsoft Certificate Authority/DCA 2011]. I believe that it's [Russia] AND [China]'s handiwork.

Some [nation state actors] appear to have found a way to [replace ALL of the system files] on the system by using [this certificate authority] I just mentioned, and [every time] I ran [SFC] or [DISM], it would tell me that [all of the files were validated successfully], as well as the system [passing every virus scan] with flying colors... but- I knew something was up, in the same manner that the OP was concerned about his [system slowing down].

When I was throwing that huge ass log file together, I found a lot of indicators that either [DCOM] or [CBS] was [replacing every system file] with a [slightly altered file] which was [never permanently written to the disk], those files all contain something [linking them to a compromised Asus Software Updater program], and it was [updating the files] with something that looks [exactly] like the [actual files] that [Microsoft] wrote...

IDK how accurate I am about all of this, but [the ransomware was there for sure].

I recorded a video of myself browsing around on the computer while it was in the process of losing a lot of functionality... it appeared to me, that the permissions on a ton of files had been in the process of being changed, but it couldn't actually use the [Ncrypt API] to [encrypt the files], because for some strange reason, the [primary encryption key] and the [backup encryption key] stopped matching each other.

[Microsoft-Windows-Crypto-DPAPI]
Event logs from: 02/07/2022 4:09:43 PM
to: 02/28/2022 5:26:34 PM
(583 events)

| https://github.com/mcc85s/FightingEntropy/blob/main/Logs/20230304/Pics/28-11.log |

The bottom line, is that I believe [Asus] had this [false certificate authority validating malicious packages] and then [packing them into the system] with [DISM] or whatever.

This isn't the [first UEFI firmware exploit] that made it's way to my [Asus] equipment.
[Asus Q504UA - https://youtu.be/in7IrkoLOHo]

This [UEFI firmware exploit] happened to a [Q504UA laptop] I had in (2019), the server manager was literally saying [Processor in group 0 is being limited by system firmware], among many other glitches and conveniently timed service interruptions and unplugging my USB lan turtle even when it wasn't physically unplugged.

As for this recent event, it occurred on a much newer laptop than the [Q504UA]. It's an [Asus TUF FX7505DY].

I upgraded from [Windows 10] to [Windows 11] in early [February], and I remember seeing the [Asus software] just [pop up] and [ask me if I wanted it to install to my system]... [I closed that Window each time it showed up], but [every time I rebooted the machine] it [showed up again].

The [Asus Software Updater] deploys a number of [Asus] programs to the system, basically [services].
Even if you [cancel out of the software it tries to install after Windows is installed]...?
That's too bad.

It gives you a [middle finger] and [still propogates itself to the device as a bunch of services].

I found some [triggers] in [event viewer] that show when the [ransomware attack] was first [enabled/scheduled], though the [actual commitment] to [ransomware attack my system] wouldn't happen until [much later in the month], the truth is, [there were plenty of signs that my system was compromised beforehand].

Here are the [pertinent log entries] for [Microsoft-Windows-Crypto-DPAPI] that apparently had a [primary encryption key matches the backup encryption key] messages until one day, they no longer matched. Then it just started [throwing errors], until [one night] it [scheduled the attack on my laptop after a reboot], and then my system was [remotely handed a BSOD]. (Not unlike in this video https://youtu.be/12x8TrO9B5Q)

I was able to [replicate the hard drive of that system].
I am able to throw it back into the system to collect anything else needed, but the bottom line is that the [event viewer] stuff sorta lined up observations I made where a folder in the [%SystemRoot%] folder had many altered subfolder names.

I don't typically go through Windows folder to figure out whether a file or folder is legitimate... but this [MoSetup] folder had a [log file] that talks about the [OP's observation] about [Windows.Kernel.LA57] among MANY other various optional packages that didn't need to be installed to my system...
...such as a lot of [RSAT] stuff that would normally be deployed to a [server].
Ultimately, I believe this attack bears a [pretty good resemblance] to an associated [Asus UEFI BIOS firmware] grade attack I detected in 2019... (https://youtu.be/in7IrkoLOHo)

[Asus Support] caused me to [lose my cool], they kept saying [send it in for an RMA] when I asked them for an [updated BIOS]... I told them to [bleep off bro, not spending my own money for your screwup].

They somehow uploaded the [UX560 firmware] to the support website in place of the [Q504UA firmware], then [Windows Update] saw that updated file, and then [Windows Update] asked me one day:

[Windows Update]: Hey.
There's a newer version of the ACPI driver for this laptop.
Wanna upgrade this ACPI driver...?

And I said:
[Me]: Fine.
Go ahead.

Ever since then, that device wouldn't let me modify the firmware, not even with the same version of the file.

When I first contacted [Asus Support] regarding this incident in [July 2019], they heard me say the specific problem... and then they eventually [uploaded the correct firmware] to the [support website], and had BOTH versions named the SAME thing, and then [I called them again], and told them that [they never got back to me] about the [updated firmware]...

Well, they figured that even though I asked for the updated file...?
It would be cool for them to just take the [wrong file off of the website], and [not tell me].
Then when I found out, a [chain of emails between myself and many people who work at Asus] began, where I just started [calling them all sorts of names].

[UEFI firmware] attacks deploy [malware] that is able to be [persistently installed] across [any number of operating system installations], or [new hard drives]... because [guess where they are deployed from]...?

The [UEFI BIOS rom chip].
Yeah.

[So, what “persistently installed” means, is this]...

If someone says	Tell them
just reinstall the operating system	Won't work, it redeploys itself from the bios chip on the motherboard
a guy blowing another guy isn't gay	Yeah, it is, because there are (0) females involved, that means = gay
that's really offensive	Read a dictionary sometime

The people who work for the [Asus RnD] department have about the same level of sense where they will argue that it is all in my head, or that if a guy is blowing another guy, that doesn't make them gay... whatever you say.

I'm rather confident that some [nation state actors] either HELPED [Asus] write this firmware... or that the guys that work in their [RnD] department are [nation state actors] that [sit around] and [create new cool ways] to [piss off Asus' customers], or [indiscriminately insert phallic shaped objects in their rectal cavities], or [both].

I'm leaning toward [both], since I've been purchasing [Asus products] since the [P3V4X] motherboard, and they thought that I would be [too stupid] to know that [they were playing games with me], or that they weren't doing it because I made a video in [March 2019] where I blasted [Linus Sebastian] from [Linus Tech Tips] for being their [bottom bitch], and [helping them sell their products].

The [Windows\Logs\MoSetup] folder that the [firmware attack] deployed to the system had an [UpdateAgent.Log] file which contains an entry [Windows.Kernel.LA57], among [many other questionable things].

While I think there's more to my situation than the OP, I do believe that this entry shouldn't be in any of these logs. A guy a couple messages up says that the [amdkmpfd.inf] file is not malicious, well... that might be the case when this exploit that feels [extremely bleep sophisticated] isn't [offsetting the content of the file that AMD actually wrote].

Otherwise, this exploit seems [high level] and alters basically [anything it wants to], into being a [malicious file]. Take a look at the log I posted.

Comment [28: mcc85s]

Comment [29: Budapest]

Index : 29
Username : Budapest
Posts : 27537
Posted : 03/23/2022 18:08

How do you know that you have a [compromised digital certificate]?

| The power of [accurate observation] is commonly called [cynicism] by those who haven't got it. |
| -George Bernard Shaw |

Comment [29: Budapest]

Comment [30: mcc85s]

Index : 30
Username : mcc85s
Posts : 2
Posted : 03/25/2022 07:46

Well, I saw [this particular certificate chain] with a [very special certificate on the end], where it allows [Windows System Component Verification].

I saved the [certificate file] because it seemed suspicious to me, that the [Asus Software Updater] program was linking a bunch of files to it. With this [particular certificate], an exploit that replaces components of [Windows] could allow [SFC] to report [100% system files verified], as well [DISM] flying right through to 100%...

However, those [verifications] may just happen [a lot faster than they normally would], because [it isn't verifying anything]- it's literally [skipping right over those files].

I found this to be the [exact case] when I checked the [CBS.log] file, which is included in log I've already posted. Many of the [errors] in that log file look like they're [normal errors]- but then again, hackers just dumped [39GB] of [Microsoft]'s source code...

Maybe portions of [Microsoft]'s own [security measures] have been [compromised].

Could be as [dead simple] as a [certificate chain] that's able to [validate modifications] to [system components], whereby causing an [alternate version of Windows], where [all of its components] have been [altered], to [manifest itself].

Might be [jumping the shark] with a claim like that though...

```
FriendlyName               : Microsoft Root Certificate Authority 2010
Thumbprint                 : 3B1EFD3A66EA28B16697394703A72CA340A05BD5
Issuer                     : CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington,
C=US
SerialNumber               : 28CC3A25BFBA44AC449A9B586B4339AA
Version                    : 3
SignatureAlgorithm         : sha256RSA
ValidFrom                  : 6/23/2010 5:57:24 PM
ValidTo                    : 6/23/2035 6:04:01 PM
Subject                    : CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington,
C=US
PublicKey                  : 30 82 05 ED 30 82 03 D5 A0 03 02 01 02 02
                             10 28 CC 3A 25 BF BA 44 AC 44 9A 9B 58 6B
                             43 39 AA 30 0D 06 09 2A 86 48 86 F7 0D 01
                             01 0B 05 00 30 81 88 31 0B 30 09 06 03 55
```

```
04 06 13 02 55 53 31 13 30 11 06 03 55 04
08 13 0A 57 61 73 68 69 6E 67 74 6F 6E 31
10 30 0E 06 03 55 04 07 13 07 52 65 64 6D
6F 6E 64 31 1E 30 1C 06 03 55 04 0A 13 15
4D 69 63 72 6F 73 6F 66 74 20 43 6F 72 70
6F 72 61 74 69 6F 6E 31 32 30 30 06 03 55
04 03 13 29 4D 69 63 72 6F 73 6F 66 74 20
52 6F 6F 74 20 43 65 72 74 69 66 69 63 61
74 65 20 41 75 74 68 6F 72 69 74 79 20 32
30 31 30 30 1E 17 0D 31 30 30 36 32 33 32
31 35 37 32 34 5A 17 0D 33 35 30 36 32 33
32 32 30 34 30 31 5A 30 81 88 31 0B 30 09
06 03 55 04 06 13 02 55 53 31 13 30 11 06
03 55 04 08 13 0A 57 61 73 68 69 6E 67 74
6F 6E 31 10 30 0E 06 03 55 04 07 13 07 52
65 64 6D 6F 6E 64 31 1E 30 1C 06 03 55 04
0A 13 15 4D 69 63 72 6F 73 6F 66 74 20 43
6F 72 70 6F 72 61 74 69 6F 6E 31 32 30 30
06 03 55 04 03 13 29 4D 69 63 72 6F 73 6F
66 74 20 52 6F 6F 74 20 43 65 72 74 69 66
69 63 61 74 65 20 41 75 74 68 6F 72 69 74
79 20 32 30 31 30 30 82 02 22 30 0D 06 09
2A 86 48 86 F7 0D 01 01 01 05 00 03 82 02
0F 00 30 82 02 0A 02 82 02 01 00 B9 08 9E
28 E4 E4 EC 06 4E 50 68 B3 41 C5 7B EB AE
B6 8E AF 81 BA 22 44 1F 65 34 69 4C BE 70
40 17 F2 16 7B E2 79 FD 86 ED 0D 39 F4 1B
A8 AD 92 90 1E CB 3D 76 8F 5A D9 B5 91 10
2E 3C 05 8D 8A 6D 24 54 E7 1F ED 56 AD 83
B4 50 9C 15 A5 17 74 88 59 20 FC 08 C5 84
76 D3 68 D4 6F 28 78 CE 5C B8 F3 50 90 44
FF E3 63 5F BE A1 9A 2C 96 15 04 D6 07 FE
1E 84 21 E0 42 31 11 C4 28 36 94 CF 50 A4
62 9E C9 D6 AB 71 00 B2 5B 0C E6 96 D4 0A
24 96 F5 FF C6 D5 B7 1B D7 CB B7 21 62 AF
12 DC A1 5D 37 E3 1A FB 1A 46 98 C0 9B C0
E7 63 1F 2A 08 93 02 7E 1E 6A 8E F2 9F 18
89 E4 22 85 A2 B1 84 57 40 FF F5 0E D8 6F
9C ED E2 45 31 01 CD 17 E9 7F B0 81 45 E3
AA 21 40 26 A1 72 AA A7 4F 3C 01 05 7E EE
83 58 B1 5E 06 63 99 62 91 78 82 B7 0D 93
0C 24 6A B4 1B DB 27 EC 5F 95 04 3F 93 4A
30 F5 97 18 B3 A7 F9 19 A7 93 33 1D 01 C8
DB 22 52 5C D7 25 C9 46 F9 A2 FB 87 59 43
BE 9B 62 B1 8D 2D 86 44 1A 46 AC 78 61 7E
30 09 FA AE 89 C4 41 2A 22 66 03 91 39 45
9C C7 8B 0C A8 CA 0D 2F FB 52 EA 0C F7 63
33 23 9D FE B0 1F AD 67 D6 A7 50 03 C6 04
70 63 B5 2C B1 86 5A 43 B7 FB AE F9 6E 29
6E 21 21 41 26 06 8C C9 C3 EE B0 C2 85 93
A1 B9 85 D9 E6 32 6C 4B 4C 3F D6 5D A3 E5
B5 9D 77 C3 9C C0 55 B7 74 00 E3 B8 38 AB
83 97 50 E1 9A 42 24 1D C6 C0 A3 30 D1 1A
5A C8 52 34 F7 73 F1 C7 18 1F 33 AD 7A EC
CB 41 60 F3 23 94 20 C2 48 45 AC 5C 51 C6
2E 80 C2 E2 77 15 BD 85 87 ED 36 9D 96 91
EE 00 B5 A3 70 EC 9F E3 8D 80 68 83 76 BA
AF 5D 70 52 22 16 E2 66 FB BA B3 C5 C2 F7
3E 2F 77 A6 CA DE C1 A6 C6 48 4C C3 37 51
23 D3 27 D7 B8 4E 70 96 F0 A1 44 76 AF 78
CF 9A E1 66 13 02 03 01 00 01 A3 51 30 4F
30 0B 06 03 55 1D 0F 04 04 03 02 01 86 30
0F 06 03 55 1D 13 01 01 FF 04 05 30 03 01
01 FF 30 1D 06 03 55 1D 0E 04 16 04 14 D5
F6 56 CB 8F E8 A2 5C 62 68 D1 3D 94 90 5B
D7 CE 9A 18 C4 30 10 06 09 2B 06 01 04 01
82 37 15 01 04 03 02 01 00 30 0D 06 09 2A
86 48 86 F7 0D 01 01 0B 05 00 03 82 02 01
00 AC A5 96 8C BF BB AE A6 F6 D7 71 87 43
31 56 88 FD 1C 32 71 5B 35 B7 D4 F0 91 F2
AF 37 E2 14 F1 F3 02 26 05 3E 16 14 7F 14
BA B8 4F FB 89 B2 B2 E7 D4 09 CC 6D B9 5B
3B 64 65 70 66 B7 F2 B1 5A DF 1A 02 F3 F5
51 B8 67 6D 79 F3 BF 56 7B E4 84 B9 2B 1E
9B 40 9C 26 34 F9 47 18 98 69 D8 1C D7 B6
D1 BF 8F 61 C2 67 C4 B5 EF 60 43 8E 10 1B
36 49 E4 20 CA AD A7 C1 B1 27 65 09 F8 CD
F5 5B 2A D0 84 33 F3 EF 1F F2 F5 9C 0B 58
93 37 A0 75 A0 DE 72 DE 6C 75 2A 66 22 F5
8C 06 30 56 9F 40 B9 30 AA 40 77 15 82 D7
8B EC C0 D3 B2 BD 83 C5 77 0C 1E AE AF 19
53 A0 4D 79 71 9F 0F AF 30 CE 67 F9 D6 2C
CC 22 41 7A 07 F2 97 42 18 CE 59 79 10 55
DE 6F 10 E4 B8 DA 83 66 40 16 09 68 23 5B
```

```
                            97 2E 26 9A 02 BB 57 8C C5 B8 BA 69 62 32
                            80 89 9E A1 FD C0 92 7C 7B 2B 33 19 84 2A
                            63 C5 00 68 62 FA 9F 47 8D 99 7A 45 3A A7
                            E9 ED EE 69 42 B5 F3 81 9B 47 56 10 7B FC
                            70 36 84 18 73 EA EF F9 97 4D 9E 33 23 DD
                            26 0B BA 2A B7 3F 44 DC 83 27 FF BD 61 59
                            2B 11 B7 CA 4F DB C5 8B 0C 1C 31 AE 32 F8
                            F8 B9 42 F7 7F DC 61 9A 76 B1 5A 04 E1 11
                            3D 66 45 B7 18 71 BE C9 24 85 D6 F3 D4 BA
                            41 34 5D 12 2D 25 B9 8D A6 13 48 6D 4B B0
                            07 7D 99 93 09 61 81 74 57 26 8A AB 69 E3
                            E4 D9 C7 88 CC 24 D8 EC 52 24 5C 1E BC 91
                            14 E2 96 DE EB 0A DA 9E DD 5F B3 5B DB D4
                            82 EC C6 20 50 87 25 40 3A FB C7 EE CD FE
                            33 E5 6E C3 84 09 55 03 25 39 C0 E9 35 5D
                            65 31 A8 F6 BF A0 09 CD 29 C7 B3 36 32 2E
                            DC 95 F3 83 C1 5A CF 8B 8D F6 EA B3 21 F8
                            A4 ED 1E 31 0E B6 4C 11 AB 60 0B A4 12 23
                            22 17 A3 36 64 82 91 04 12 E0 AB 6F 1E CB
                            50 05 61 B4 40 FF 59 86 71 D1 D5 33 69 7C
SubjectKeyIdentifier       : d5f656cb8fe8a25c6268d13d94905bd7ce9a18c4
AuthorityKeyIdentifier     :
KeyUsage                   : Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
EnhancedKeyUsage           :
CRLDistributionPoints      :
AuthorityInformationAccess :
SubjectAlternateName       :
BasicContraints            : Subject Type=CA
                             Path Length Constraint=None
```

```
FriendlyName               : Microsoft Windows Production PCA 2011
Thumbprint                 : 580A6F4CC4E4B669B9EBDC1B2B3E087B80D0678D
Issuer                     : CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington,
C=US
SerialNumber               : 61077656000000000008
Version                    : 3
SignatureAlgorithm         : sha256RSA
ValidFrom                  : 10/19/2011 2:41:42 PM
ValidTo                    : 10/19/2026 2:51:42 PM
Subject                    : CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
PublicKey                  : 30 82 05 D7 30 82 03 BF A0 03 02 01 02 02
                             0A 61 07 76 56 00 00 00 00 00 08 30 0D 06
                             09 2A 86 48 86 F7 0D 01 01 0B 05 00 30 81
                             88 31 0B 30 09 06 03 55 04 06 13 02 55 53
                             31 13 30 11 06 03 55 04 08 13 0A 57 61 73
                             68 69 6E 67 74 6F 6E 31 10 30 0E 06 03 55
                             04 07 13 07 52 65 64 6D 6F 6E 64 31 1E 30
                             1C 06 03 55 04 0A 13 15 4D 69 63 72 6F 73
                             6F 66 74 20 43 6F 72 70 6F 72 61 74 69 6F
                             6E 31 32 30 30 06 03 55 04 03 13 29 4D 69
                             63 72 6F 73 6F 66 74 20 52 6F 6F 74 20 43
                             65 72 74 69 66 69 63 61 74 65 20 41 75 74
                             68 6F 72 69 74 79 20 32 30 31 30 30 1E 17
                             0D 31 31 31 30 31 39 31 38 34 31 34 32 5A
                             17 0D 32 36 31 30 31 39 31 38 35 31 34 32
                             5A 30 81 84 31 0B 30 09 06 03 55 04 06 13
                             02 55 53 31 13 30 11 06 03 55 04 08 13 0A
                             57 61 73 68 69 6E 67 74 6F 6E 31 10 30 0E
                             06 03 55 04 07 13 07 52 65 64 6D 6F 6E 64
                             31 1E 30 1C 06 03 55 04 0A 13 15 4D 69 63
                             72 6F 73 6F 66 74 20 43 6F 72 70 6F 72 61
                             74 69 6F 6E 31 2E 30 2C 06 03 55 04 03 13
                             25 4D 69 63 72 6F 73 6F 66 74 20 57 69 6E
                             64 6F 77 73 20 50 72 6F 64 75 63 74 69 6F
                             6E 20 50 43 41 20 32 30 31 31 30 82 01 22
                             30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05
                             00 03 82 01 0F 00 30 82 01 0A 02 82 01 01
                             00 DD 0C BB A2 E4 2E 09 E3 E7 C5 F7 96 69
                             BC 00 21 BD 69 33 33 EF AD 04 CB 54 80 EE
                             06 83 BB C5 20 84 D9 F7 D2 8B F3 38 B0 AB
                             A4 AD 2D 7C 62 79 05 FF E3 4A 3F 04 35 20
                             70 E3 C4 E7 6B E0 9C C0 36 75 E9 8A 31 DD
                             8D 70 E5 DC 37 B5 74 46 96 28 5B 87 60 23
                             2C BF DC 47 A5 67 F7 51 27 9E 72 EB 07 A6
                             C9 B9 1E 3B 53 35 7C E5 D3 EC 27 B9 87 1C
                             FE B9 C9 23 09 6F A8 46 91 C1 6E 96 3C 41
                             D3 CB A3 3F 5D 02 6A 4D EC 69 1F 25 28 5C
                             36 FF FD 43 15 0A 94 E0 19 B4 CF DF C2 12
                             E2 C2 5B 27 EE 27 78 30 8B 5B 2A 09 6B 22
                             89 53 60 16 2C C0 68 1D 53 BA EC 49 F3 9D
                             61 8C 85 68 09 73 44 5D 7D A2 54 2B DD 79
                             F7 15 CF 35 5D 6C 1C 2B 5C CE BC 9C 23 8B
                             6F 6E B5 26 D9 36 13 C3 4F D6 27 AE B9 32
```

```
                           3B 41 92 2C E1 C7 CD 77 E8 AA 54 4E F7 5C
                           0B 04 87 65 B4 43 18 A8 B2 E0 6D 19 77 EC
                           5A 24 FA 48 03 02 03 01 00 01 A3 82 01 43
                           30 82 01 3F 30 10 06 09 2B 06 01 04 01 82
                           37 15 01 04 03 02 01 00 30 1D 06 03 55 1D
                           0E 04 16 04 14 A9 29 02 39 8E 16 C4 97 78
                           CD 90 F9 9E 4F 9A E1 7C 55 AF 53 30 19 06
                           09 2B 06 01 04 01 82 37 14 02 04 0C 1E 0A
                           00 53 00 75 00 62 00 43 00 41 30 0B 06 03
                           55 1D 0F 04 04 03 02 01 86 30 0F 06 03 55
                           1D 13 01 01 FF 04 05 30 03 01 01 FF 30 1F
                           06 03 55 1D 23 04 18 30 16 80 14 D5 F6 56
                           CB 8F E8 A2 5C 62 68 D1 3D 94 90 5B D7 CE
                           9A 18 C4 30 56 06 03 55 1D 1F 04 4F 30 4D
                           30 4B A0 49 A0 47 86 45 68 74 74 70 3A 2F
                           2F 63 72 6C 2E 6D 69 63 72 6F 73 6F 66 74
                           2E 63 6F 6D 2F 70 6B 69 2F 63 72 6C 2F 70
                           72 6F 64 75 63 74 73 2F 4D 69 63 52 6F 6F
                           43 65 72 41 75 74 5F 32 30 31 30 2D 30 36
                           2D 32 33 2E 63 72 6C 30 5A 06 08 2B 06 01
                           05 05 07 01 01 04 4E 30 4C 30 4A 06 08 2B
                           06 01 05 05 07 30 02 86 3E 68 74 74 70 3A
                           2F 2F 77 77 77 2E 6D 69 63 72 6F 73 6F 66
                           74 2E 63 6F 6D 2F 70 6B 69 2F 63 65 72 74
                           73 2F 4D 69 63 52 6F 6F 43 65 72 41 75 74
                           5F 32 30 31 30 2D 30 36 2D 32 33 2E 63 72
                           74 30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B
                           05 00 03 82 02 01 00 14 FC 7C 71 51 A5 79
                           C2 6E B2 EF 39 3E BC 3C 52 0F 6E 2B 3F 10
                           13 73 FE A8 68 D0 48 A6 34 4D 8A 96 05 26
                           EE 31 46 90 61 79 D6 FF 38 2E 45 6B F4 C0
                           E5 28 B8 DA 1D 8F 8A DB 09 D7 1A C7 4C 0A
                           36 66 6A 8C EC 1B D7 04 90 A8 18 17 A4 9B
                           B9 E2 40 32 36 76 C4 C1 5A C6 BF E4 04 C0
                           EA 16 D3 AC C3 68 EF 62 AC DD 54 6C 50 30
                           58 A6 EB 7C FE 94 A7 4E 8E F4 EC 7C 86 73
                           57 C2 52 21 73 34 5A F3 A3 8A 56 C8 04 DA
                           07 09 ED F8 8B E3 CE F4 7E 8E AE F0 F6 0B
                           8A 08 FB 3F C9 1D 72 7F 53 B8 EB BE 63 E0
                           E3 3D 31 65 B0 81 E5 F2 AC CD 16 A4 9F 3D
                           A8 B1 9B C2 42 D0 90 84 5F 54 1D FF 89 EA
                           BA 1D 47 90 6F B0 73 4E 41 9F 40 9F 5F E5
                           A1 2A B2 11 91 73 8A 21 28 F0 CE DE 73 39
                           5F 3E AB 5C 60 EC DF 03 10 A8 D3 09 E9 F4
                           F6 96 85 B6 7F 51 88 66 47 19 8D A2 B0 12
                           3D 81 2A 68 05 77 BB 91 4C 62 7B B6 C1 07
                           C7 BA 7A 87 34 03 0E 4B 62 7A 99 E9 CA FC
                           CE 4A 37 C9 2D A4 57 7C 1C FE 3D DC B8 0F
                           5A FA D6 C4 B3 02 85 02 3A EA B3 D9 6E E4
                           69 21 37 DE 81 D1 F6 75 19 05 67 D3 93 57
                           5E 29 1B 39 C8 EE 2D E1 CD E4 45 73 5B D0
                           D2 CE 7A AB 16 19 82 46 58 D0 5E 9D 81 B3
                           67 AF 6C 35 F2 BC E5 3F 24 E2 35 A2 0A 75
                           06 F6 18 56 99 D4 78 2C D1 05 1B EB D0 88
                           01 9D AA 10 F1 05 DF BA 7E 2C 63 B7 06 9B
                           23 21 C4 F9 78 6C E2 58 17 06 36 2B 91 12
                           03 CC A4 D9 F2 2D BA F9 94 9D 40 ED 18 45
                           F1 CE 8A 5C 6B 3E AB 03 D3 70 18 2A 0A 6A
                           E0 5F 47 D1 D5 63 0A 32 F2 AF D7 36 1F 2A
                           70 5A E5 42 59 08 71 4B 57 BA 7E 83 81 F0
                           21 3C F4 1C C1 C5 B9 90 93 0E 88 45 93 86
                           E9 B1 20 99 BE 98 CB C5 95 A4 5D 62 D6 A0
                           63 08 20 BD 75 10 77 7D 3D F3 45 B9 9F 97
                           9F CB 57 80 6F 33 A9 04 CF 77 A4 62 1C 59
SubjectKeyIdentifier       : a92902398e16c49778cd90f99e4f9ae17c55af53
AuthorityKeyIdentifier     : KeyID=d5f656cb8fe8a25c6268d13d94905bd7ce9a18c4
KeyUsage                   : Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
EnhancedKeyUsage           :
CRLDistributionPoints      : [1]CRL Distribution Point
                                  Distribution Point Name:
                                       Full Name:
                                            URL=http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl

AuthorityInformationAccess : [1]Authority Info Access
                                  Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
                                  Alternative Name:
                                       URL=http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt

SubjectAlternateName       :
BasicContraints            : Subject Type=CA
                             Path Length Constraint=None
```

```
FriendlyName               : Microsoft Windows Publisher
```

```
Thumbprint                : 7B2177E03D07812A5A5842565A647DB565F77BB8
Issuer                    : CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
SerialNumber              : 33000002F49E469C54137B85E00000000002F4
Version                   : 3
SignatureAlgorithm        : sha256RSA
ValidFrom                 : 4/29/2021 3:15:49 PM
ValidTo                   : 4/28/2022 3:15:49 PM
Subject                   : CN=Microsoft Windows Publisher, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
PublicKey                 : 30 82 05 1C 30 82 04 04 A0 03 02 01 02 02
                            13 33 00 00 02 F4 9E 46 9C 54 13 7B 85 E0
                            00 00 00 00 02 F4 30 0D 06 09 2A 86 48 86
                            F7 0D 01 01 0B 05 00 30 81 84 31 0B 30 09
                            06 03 55 04 06 13 02 55 53 31 13 30 11 06
                            03 55 04 08 13 0A 57 61 73 68 69 6E 67 74
                            6F 6E 31 10 30 0E 06 03 55 04 07 13 07 52
                            65 64 6D 6F 6E 64 31 1E 30 1C 06 03 55 04
                            0A 13 15 4D 69 63 72 6F 73 6F 66 74 20 43
                            6F 72 70 6F 72 61 74 69 6F 6E 31 2E 30 2C
                            06 03 55 04 03 13 25 4D 69 63 72 6F 73 6F
                            66 74 20 57 69 6E 64 6F 77 73 20 50 72 6F
                            64 75 63 74 69 6F 6E 20 50 43 41 20 32 30
                            31 31 30 1E 17 0D 32 31 30 34 32 39 31 39
                            31 35 34 39 5A 17 0D 32 32 30 34 32 38 31
                            39 31 35 34 39 5A 30 7A 31 0B 30 09 06 03
                            55 04 06 13 02 55 53 31 13 30 11 06 03 55
                            04 08 13 0A 57 61 73 68 69 6E 67 74 6F 6E
                            31 10 30 0E 06 03 55 04 07 13 07 52 65 64
                            6D 6F 6E 64 31 1E 30 1C 06 03 55 04 0A 13
                            15 4D 69 63 72 6F 73 6F 66 74 20 43 6F 72
                            70 6F 72 61 74 69 6F 6E 31 24 30 22 06 03
                            55 04 03 13 1B 4D 69 63 72 6F 73 6F 66 74
                            20 57 69 6E 64 6F 77 73 20 50 75 62 6C 69
                            73 68 65 72 30 82 01 22 30 0D 06 09 2A 86
                            48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00
                            30 82 01 0A 02 82 01 01 00 92 ED 20 54 B6
                            84 72 29 F1 F8 2C F1 57 66 1C CB 94 3B 08
                            99 12 F4 37 4C 95 0C 38 CE 90 6D 02 55 0E
                            B7 FF 89 51 2D 3B CC 11 09 98 16 BA FD 01
                            4E 53 AA 71 B7 E0 3F 8B 01 8D 00 D5 6F 96
                            63 93 77 D9 7E 33 1C 68 DA FE 96 3C 23 96
                            C2 72 13 9A 55 F1 F1 C5 03 E4 63 A4 39 68
                            64 BD 25 B9 63 9F 49 2A 2D B0 E8 1B B2 3D
                            61 8C 48 25 5F 66 1B 03 06 E9 AA 9D 78 ED
                            EB 0D E6 36 D8 D6 C5 53 90 EA 70 30 7C DA
                            0D 23 67 54 E5 D3 A0 24 4E 5C 3D 36 43 7C
                            95 D2 5D 64 25 0E A5 69 CA 60 B2 F7 0A 0F
                            8F E9 D3 16 C0 B0 1F 2F B8 28 A2 32 42 D6
                            9A 23 2E DF BF E5 BF B8 B0 27 6D 58 21 49
                            89 2B 80 6B 97 C0 7D D2 13 70 4C 6C D9 1A
                            85 C7 4D 7D 86 53 D4 8B 65 40 84 6E CF B9
                            C0 92 01 33 FD FC A2 44 C5 AF D2 F4 74 F0
                            AE 26 08 5F 04 D9 A3 38 CC 53 2B BC 44 69
                            CB AC 97 FB B0 E8 F6 2F 12 13 15 E3 C5 02
                            03 01 00 01 A3 82 01 8E 30 82 01 8A 30 2B
                            06 03 55 1D 25 04 24 30 22 06 0A 2B 06 01
                            04 01 82 37 0A 03 16 06 0A 2B 06 01 04 01
                            82 37 0A 03 06 06 08 2B 06 01 05 05 07 03
                            03 30 1D 06 03 55 1D 0E 04 16 04 14 04 F6
                            B0 9E 2D B9 52 37 3C 9A F6 6F CD 1B 6E 3D
                            66 A2 7B 1F 30 54 06 03 55 1D 11 04 4D 30
                            4B A4 49 30 47 31 2D 30 2B 06 03 55 04 0B
                            13 24 4D 69 63 72 6F 73 6F 66 74 20 49 72
                            65 6C 61 6E 64 20 4F 70 65 72 61 74 69 6F
                            6E 73 20 4C 69 6D 69 74 65 64 31 16 30 14
                            06 03 55 04 05 13 0D 32 33 30 32 38 30 2B
                            34 36 34 35 36 39 30 1F 06 03 55 1D 23 04
                            18 30 16 80 14 A9 29 02 39 8E 16 C4 97 78
                            CD 90 F9 9E 4F 9A E1 7C 55 AF 53 30 54 06
                            03 55 1D 1F 04 4D 30 4B 30 49 A0 47 A0 45
                            86 43 68 74 74 70 3A 2F 2F 77 77 77 2E 6D
                            69 63 72 6F 73 6F 66 74 2E 63 6F 6D 2F 70
                            6B 69 6F 70 73 2F 63 72 6C 2F 4D 69 63 57
                            69 6E 50 72 6F 50 43 41 32 30 31 31 5F 32
                            30 31 31 2D 31 30 2D 31 39 2E 63 72 6C 30
                            61 06 08 2B 06 01 05 05 07 01 01 04 55 30
                            53 30 51 06 08 2B 06 01 05 05 07 30 02 86
                            45 68 74 74 70 3A 2F 2F 77 77 77 2E 6D 69
                            63 72 6F 73 6F 66 74 2E 63 6F 6D 2F 70 6B
                            69 6F 70 73 2F 63 65 72 74 73 2F 4D 69 63
                            57 69 6E 50 72 6F 50 43 41 32 30 31 31 5F
                            32 30 31 31 2D 31 30 2D 31 39 2E 63 72 74
                            30 0C 06 03 55 1D 13 01 01 FF 04 02 30 00
                            30 0D 06 09 2A 86 48 86 F7 0D 01 01 0B 05
                            00 03 82 01 01 00 0A 88 1C C5 B5 38 60 68
```

```
                           73 D3 8B 88 71 7B D9 F3 EA 7F 4A F1 06 BF
                           66 C4 2B 6D DA D0 CD 32 34 C2 DB A1 AD 9C
                           21 C9 7A 8E 29 D9 F5 AE CA B5 00 42 BA 69
                           5F 3B 8F 0D E8 31 84 A1 73 E7 63 6D CA 9E
                           C8 CE 8F F9 4F 97 06 91 01 A3 A1 EC CC 49
                           25 BB BE AA 1A F0 55 C1 8A E3 32 31 92 B8
                           A9 0E 6D 03 38 80 CA 5D 2D 09 4B CE 5E 38
                           AC 15 ED 05 24 7C 7B 8E D7 81 D6 1F 5D 52
                           46 7A C5 2C F4 0A 5F C9 6A 09 B6 5D FC 79
                           81 A5 50 6E 80 74 23 77 41 23 34 5B AA F7
                           80 F6 01 77 E3 F1 20 E9 A3 43 98 30 A2 AC
                           A8 7A 7D 2E 3A B9 FC D0 98 1C D2 39 55 CB
                           75 25 AC BD 47 30 3E 2A 37 5A 4E E4 67 6C
                           F4 F0 BD B0 F8 D5 5E CC 6C DE CB 75 24 8B
                           5E A7 0C 38 18 D6 66 D4 E8 63 5E 0B 3C EC
                           ED 73 4E 49 9C C6 B6 2A 44 84 6F 54 3A BB
                           6A CE 9C F8 2B CE FF DF 12 37 ED B5 FE 63
SubjectKeyIdentifier       : 04f6b09e2db952373c9af66fcd1b6e3d66a27b1f
AuthorityKeyIdentifier     : KeyID=a92902398e16c49778cd90f99e4f9ae17c55af53
KeyUsage                   :
EnhancedKeyUsage           : Protected Process Light Verification (1.3.6.1.4.1.311.10.3.22)
                             Windows System Component Verification (1.3.6.1.4.1.311.10.3.6)
                             Code Signing (1.3.6.1.5.5.7.3.3)

CRLDistributionPoints      : [1]CRL Distribution Point
                                  Distribution Point Name:
                                       Full Name:
                                            URL=http://www.microsoft.com/pkiops/crl/MicWinProPCA2011_2011-10-19.crl

AuthorityInformationAccess : [1]Authority Info Access
                                  Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
                                  Alternative Name:
                                       URL=http://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt

SubjectAlternateName       : Directory Address:
                                  SERIALNUMBER="230280+464569"
                                  OU=Microsoft Ireland Operations Limited

BasicContraints            : Subject Type=End Entity
                             Path Length Constraint=None
```

_____/ Comment [30: mcc85s] /---------- Comment [31: EyeMinUrHead] /----------\

Index : 31
Username : EyeMinUrHead
Posts : 21
Posted : 08/02/2022 00:27

It somehow uses an aspect of [Windows Defender] during [OOBE/Out-Of-Box Experience] to [disable user privileges] and [set the stage for takeover]. If it isn't [WinDefender], then [it's an executable] that is very similar to it.

I had to put together a [new computer], and while I think this one may be [already gone] due to what I think may be [registry entries] that shouldn't be there, the last thing I want to do is hook up one of the hard drives from the other computer.

[This wasn't a troll]. It may have something to do with the [exceptionally large hack attacks] going on lately. But I do know that [when I started this thread], [I was infected with something really nasty]. I've dumped TWO computers since because I thought a drive was clean.

It doesn't take much to just look, folks.

The proof is in the virus pudding.

_____/ Comment [31: EyeMinUrHead] /---------- Comment [32: EyeMinUrHead] /----------\

Index : 32
Username : EyeMinUrHead
Posts : 21
Posted : 08/21/2022 11:57

Does [Windows 11] usually come with a lot of [BizTalk Server 2004] stuff in the registry?

_____/ Comment [32: EyeMinUrHead]

Comment [33: electricult]

Index : 33
Username : electricult
Posts : 1
Posted : 08/25/2022 01:37

I'm [currently experiencing] the [same issue] you guys are, but I've got a [Lenovo laptop].

It initially had [Windows 10 Home] on it then updated to [Windows 11].

About 2 months ago, I noticed my computer [running a lot slower than it used to], and everything just felt off.

Tried clean installs of windows to no avail.
Now I don't have any [clean devices] to work with, so I ended up [biting the bullet] and bought a [physical key] of [Windows 11 Pro], after [wiping my SSD] on what used to be a [clean device]

[Think it might be compromised now], using the [System Rescue CD] booted to the [ram], I figured there's no way in hell it'd be compromised. I installed it and I thought I was in the clear... WRONG!!!

[Upon install it used the Windows key thats in the BIOS/UEFI], so then I tried to [activate my key].
[It wouldn't let me].

Then when I rebooted my computer, suddenly it said it had [Windows 11 Enterprise] edition activated WTF?!?

I figured that had been the case, as I when the issue was first happening, I noted that [remote assistance] was on when I didn't want it to be, along with it being part of a [workgroup]. I'm not too knowledgeable about all this stuff, but I've been doing [more] and [more research], and I [really hope] this issue gets [resolved] for y'all, because [it sounds like the same thing that's happening to me].

Hopefully I can get some tidbits on how to resolve my issue from this post.
I really hope my [Windows 11] key isn't somehow [compromised] either, but it did end up letting me activate it in the end.

Attached Thumbnails:

| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/33-01.jpg |
| https://github.com/mcc85s/FightingEntropy/blob/main/Docs/20230304/Pics/33-02.jpg |

Comment [33: electricult]

Comment [34: TheUnluckyOne]

Index : 34
Username : TheUnluckyOne
Posts : 2
Posted : 03/02/2023 19:23

Mate!!!!
Do you know how happy I am to have discovered your post!!!

I have been plagued by this exact scenario for years!
[You are not crazy], these are [threats actors] at the [top of their game].

I really appreciate how you have [documented the process] far better than me.

I have [reinstalled Windows], [obliterated the registry] to a [barely functioning computer] many times.
Tried every [antivirus software], and [all failed].

It is a [bleepty feeling] of knowing [everything you do is being watched] on the internet, and anything you do is [useless to stop them].

I will never buy [Asus] again, and I had [experienced the same bios download website stupidity] or plain evil from them. (It is because the people who work at [Asus] are fuckin' stupid.)

Trying to fight this has taught me how truly flawed [Windows] (it is not Windows' fault) is as a system and piling code onto of bad code for years has left it as vulnerable as a wet paper bag for everyone's detriment.

Please reach out to me to chat and I will do the same to get to a solution.
Keep your chin up bro!

Edited by Budapest, 02 March 2023 08:38 PM → Please don't bump topics

Comment [34: TheUnluckyOne]

Breakdown

The first comment, by the OP [EyeMinUrHeadz] is attempting to be rather dramatic with the storytelling upon initiation. The stuff that's in this document has been heavily modified with [my punctuation + styling].

Often times, text is compacted to the point where nobody wants to fuckin' read it.
Even though the story this dude is telling happens to be be [clever] and [creative], I can see where most people may say to themselves “This is fuckin' difficult to read, wtf.”

He has a long way to go to use the [correct punctuation], but [that takes a really long time to master].

The way that it is written causes his [dramatic, creative, and interesting storytelling] and his [verbatim research methodologies] to be [blended together], whereby causing [confusion], [chaos], [cacaphony], and [mayhem] for all involved... particularly for the [reader].

At which point, you're basically [extra fucked], and not in the way anybody wants to be [extra fucked]...

Here's a breakdown of relevant comments...

==[Comment #1]=======

Cleansing ritual	Performing a clean install
Seeming on a timed basis	Timed trigger event
Script from hell	Malware attack
Virtual machine	Containment
10,000th [Windows] re-install	Persistent malware attack
little tiny drives	Payload
No one is taking this very seriously	Some people are
There is no more [clean install].	Yes there is.
[Somebody]: Ok, crazy boy.	Indicates that people ALSO write off his observation skills
Eat your [Wheaties].	Does what he's told
Eat your [Flintstone vitamins].	Does what he's told
Put on your [big boy pants].	Does what he's told
[Windows 95] instance	It's not Win95
[high fan speed],opened [Notepad]	Firmware
reinstall Windows. (10 times a day)	What I do when testing PXE portion of [FightingEntropy/MDT/PSD]
helps [system] get [more cool stuff]	Payloads (After Midnight, etc.)

==[Comment #2]=======

Here's DISM output	Good, this is more helpful than the first comment.

==[Comment #3]=======

Version of Windows?	Read DISM logs [Version: 10.0.22000.1, Image Version: 10.0.22000.318]
You mention Win95	As a [joke]...
Make and model number of your computer	Standard-issue help desk question

==[Comment #4]=======

Turning on at night by itself	It's called Sleep Study or something stupid
Lack of performance	Not unlike when a guy has erectile dysfunction
Permissions disappeared	(After Midnight/Assassin)
Windows NT	Has something to do with Power Management
Network activity, strange devices	Standard-issue espionage
Chrome, weird processes, Program Data	Remotely infected -> Possible espionage
Home computer; not a business network	Forced to run on domain mode, possible espionage
DCOM, non-networked home PC	Intelligent dude
Evil shims, persistence	Dude knows he's being spied on, and even how.
I want this to be paranoia	Reverse psychology to shut down claims of psychosis
Puts me in the closet, takes away toys	Being poetic, this dude is extremely intelligent

==[Comment #5]=======

Scheduled Windows Updates	Sometimes that is the reason why, other times it's not.
	Many times, MY computer would turn itself on, or the screen
	would suddenly wake up, not unlike when the mouse would move.
	This can be a (HARDWARE/FIRMWARE) LEVEL EXPLOIT.

                                    | Not to mention, the dude says he's reinstalled Windows 10,000 times,
                                    | and has DISABLED KEY FEATURES RELATED TO WINDOWS UPDATES.
                                    | So...
    ==[Comment #8]=======

    Snipping tool gets cut off | [Snipping tool → CIA ARCHIMEDES https://youtu.be/QP25FbNhakQ]
    Probably from screwing w/ something | Or, it's someone trying to cover your mouth and suffocate you

                                                                                                                    __________/
____/ Breakdown
  Conclusion /---\
/------------

    I may or may not add more to this particular document.

                                                                                                                 __________/
____/ Conclusion

 ____
 |---|
 | Michael C. Cook Sr. |
 | Security Engineer |
 | Secure Digits Plus LLC |
 |____|