MICROSOFT SECURITY RESPONSE CENTER

BH 23

BLUEHAT 2023 • REDMOND, WA USA

Microsoft

Microsoft

0-Day firmWarez

Nate Warfield
Director of Threat Intelligence & Research
Eclypsium

MICROSOFT SECURITY RESPONSE CENTER
BH 23
BLUEHAT 2023 • REDMOND, WA USA

/whois

Nate Warfield

- Network hacker
- Security researcher
- WIRED25 2020
- Former Microsoft (MSRC & Defender)
- 8th BlueHat; 3rd speaking appearance
- Twitter/Mastodon: @n0x08

Agenda

Firmware 101

Firmware attack trends

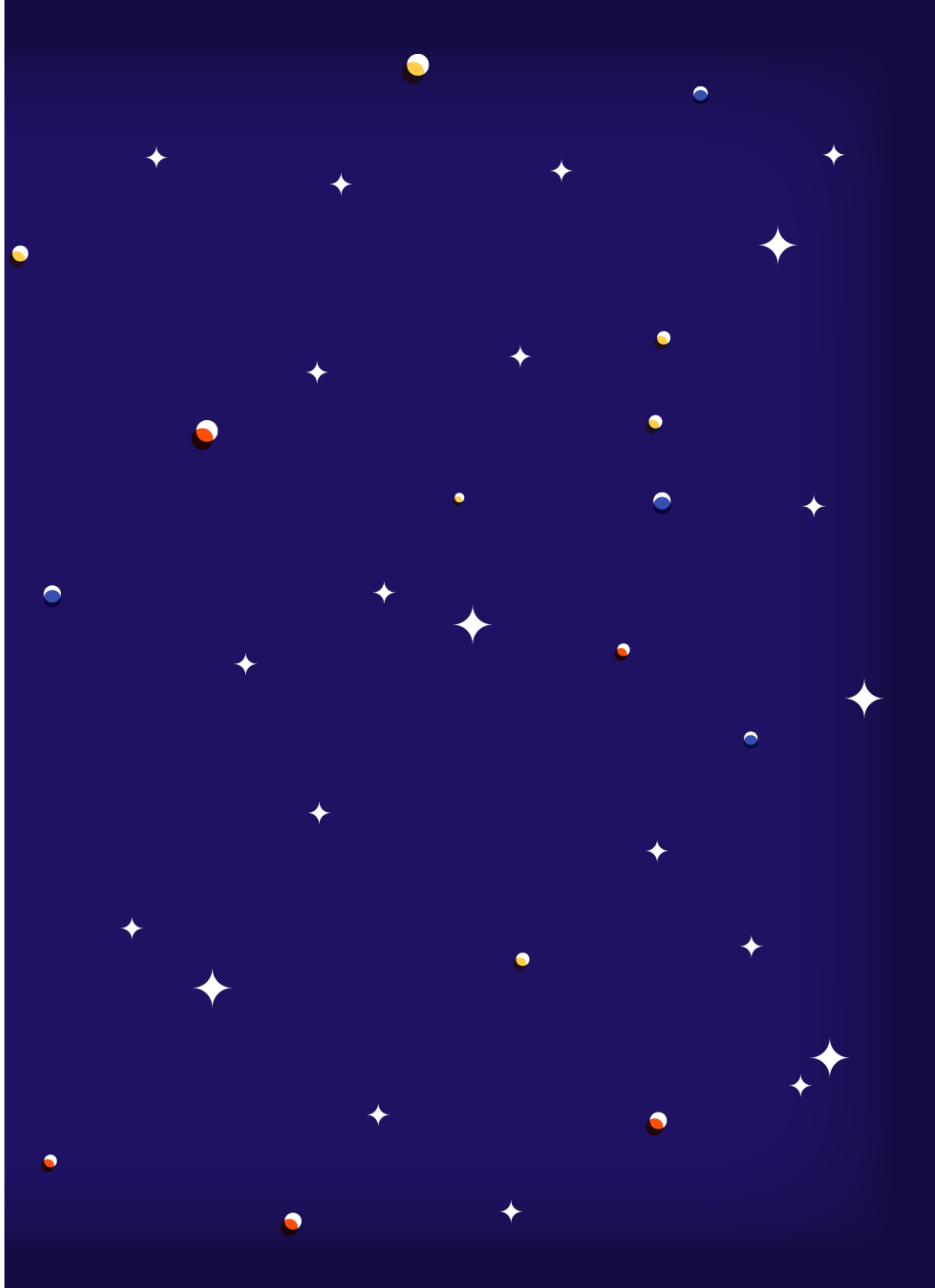
Implants and backdoors

MegaRAC vulnerability research

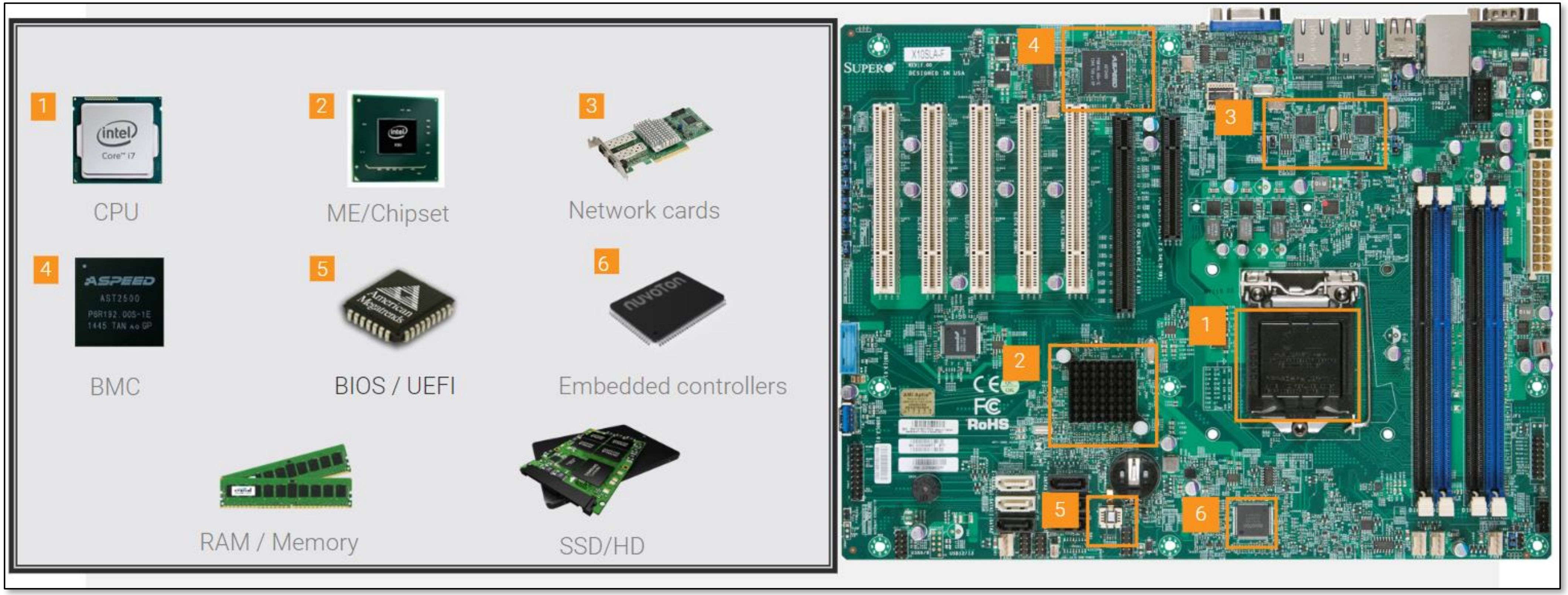
Analysis with FACT & EMBA

Enterprise connected systems

Takeaways

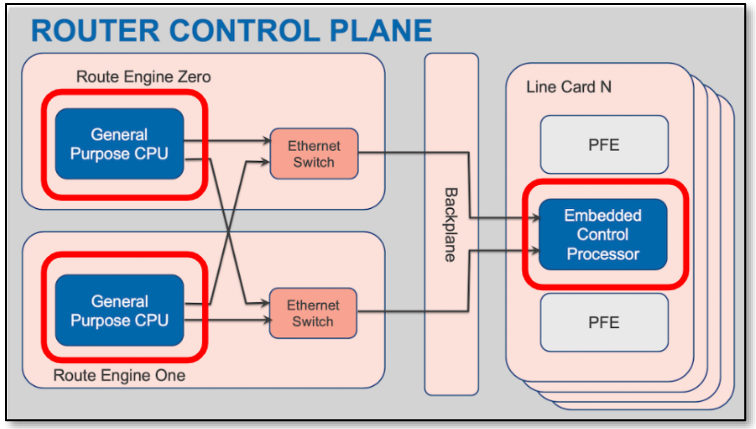


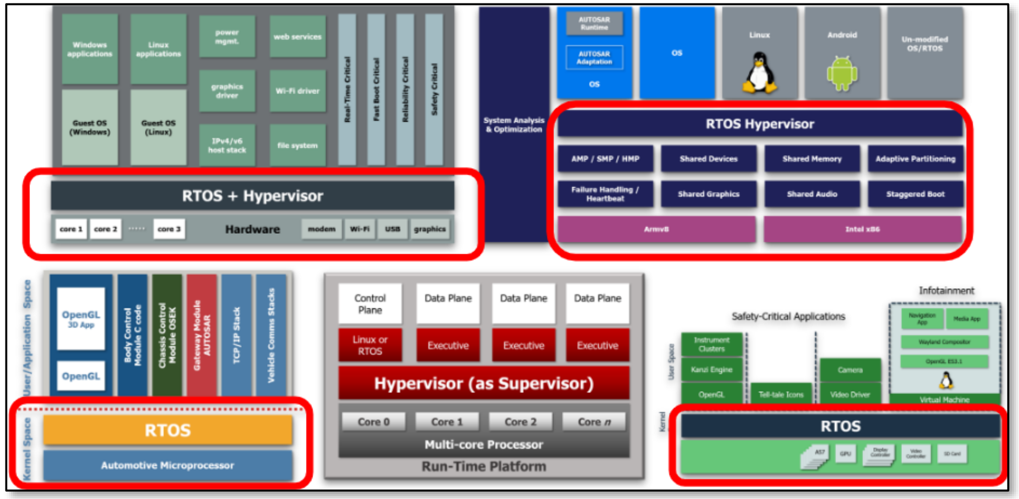
Firmware - Computing



Firmware – Network

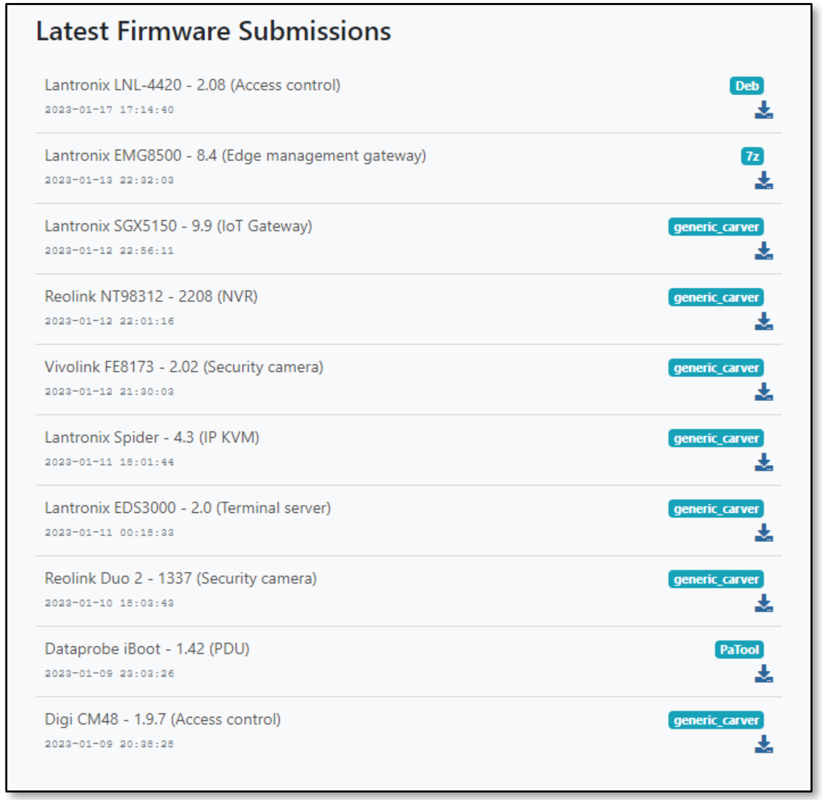
- Routers
- Switches
- Firewalls
- Load balancers
- Wifi AP
- iLO & BMC
- IoT





Firmware – Enterprise systems

- Power distribution
- IP KVM
- Ethernet->Serial adapters
- Door access controls
- Security cameras
- Network video recorders
- Fire suppression
- Environmental control



Latest Firmware Submissions

Lantronix LNL-4420 - 2.08 (Access control) Deb
2023-01-17 17:14:40

Lantronix EMG8500 - 8.4 (Edge management gateway) 7z
2023-01-13 22:32:03

Lantronix SGX5150 - 9.9 (IoT Gateway) generic_carver
2023-01-12 22:56:11

Reolink NT98312 - 2208 (NVR) generic_carver
2023-01-12 22:01:16

Vivolink FE8173 - 2.02 (Security camera) generic_carver
2023-01-12 21:30:03

Lantronix Spider - 4.3 (IP KVM) generic_carver
2023-01-11 18:01:44

Lantronix EDS3000 - 2.0 (Terminal server) generic_carver
2023-01-11 00:18:33

Reolink Duo 2 - 1337 (Security camera) generic_carver
2023-01-10 18:03:43

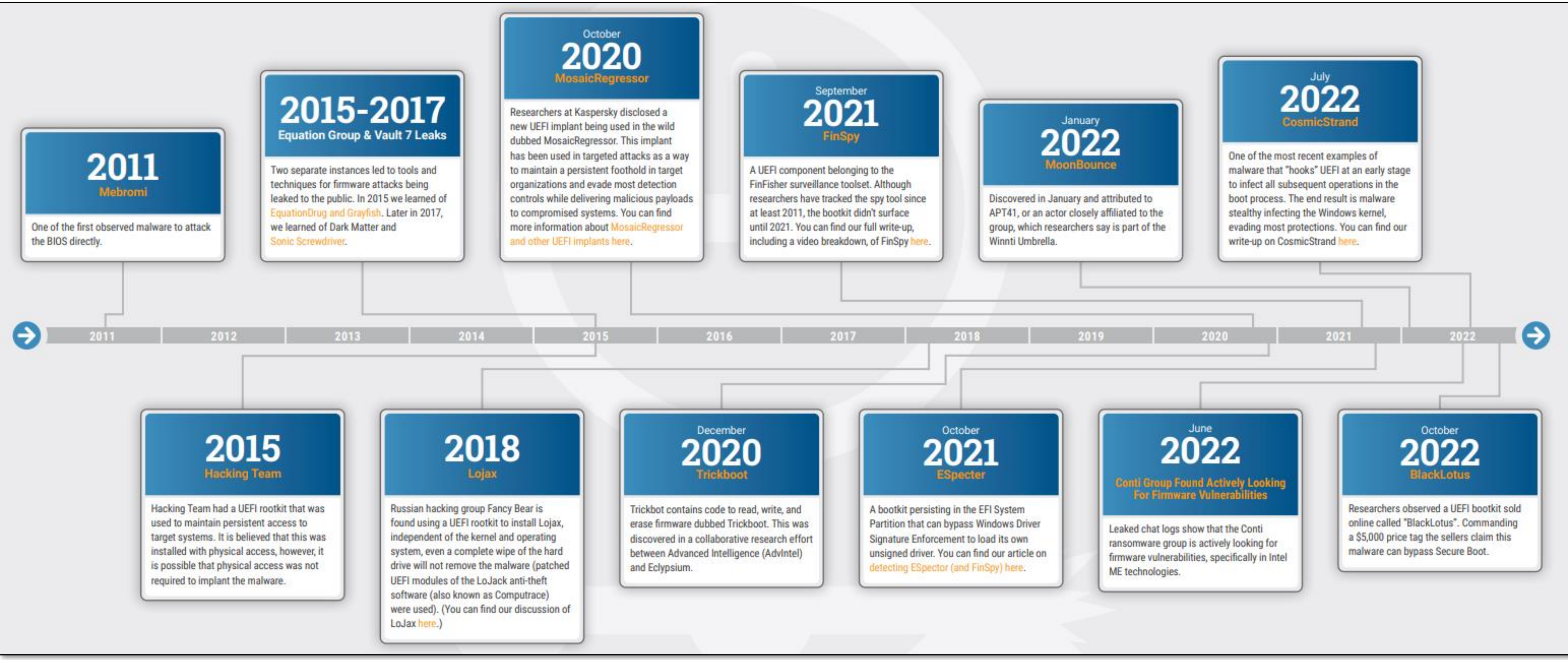
Dataprobe iBoot - 1.42 (PDU) PaTool
2023-01-09 23:03:26

Digi CM48 - 1.9.7 (Access control) generic_carver
2023-01-09 20:38:28

Attack trends

APT capabilities for all

- Low-level persistence
- Invisible to most security tools
- High privileges & rarely updated
- Historically nation state / APT
- Plenty of Open-Source tools exist
- Ransomware & cyber criminals
- Research proves circa 2000 vulnerabilities exist in 2022 code



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

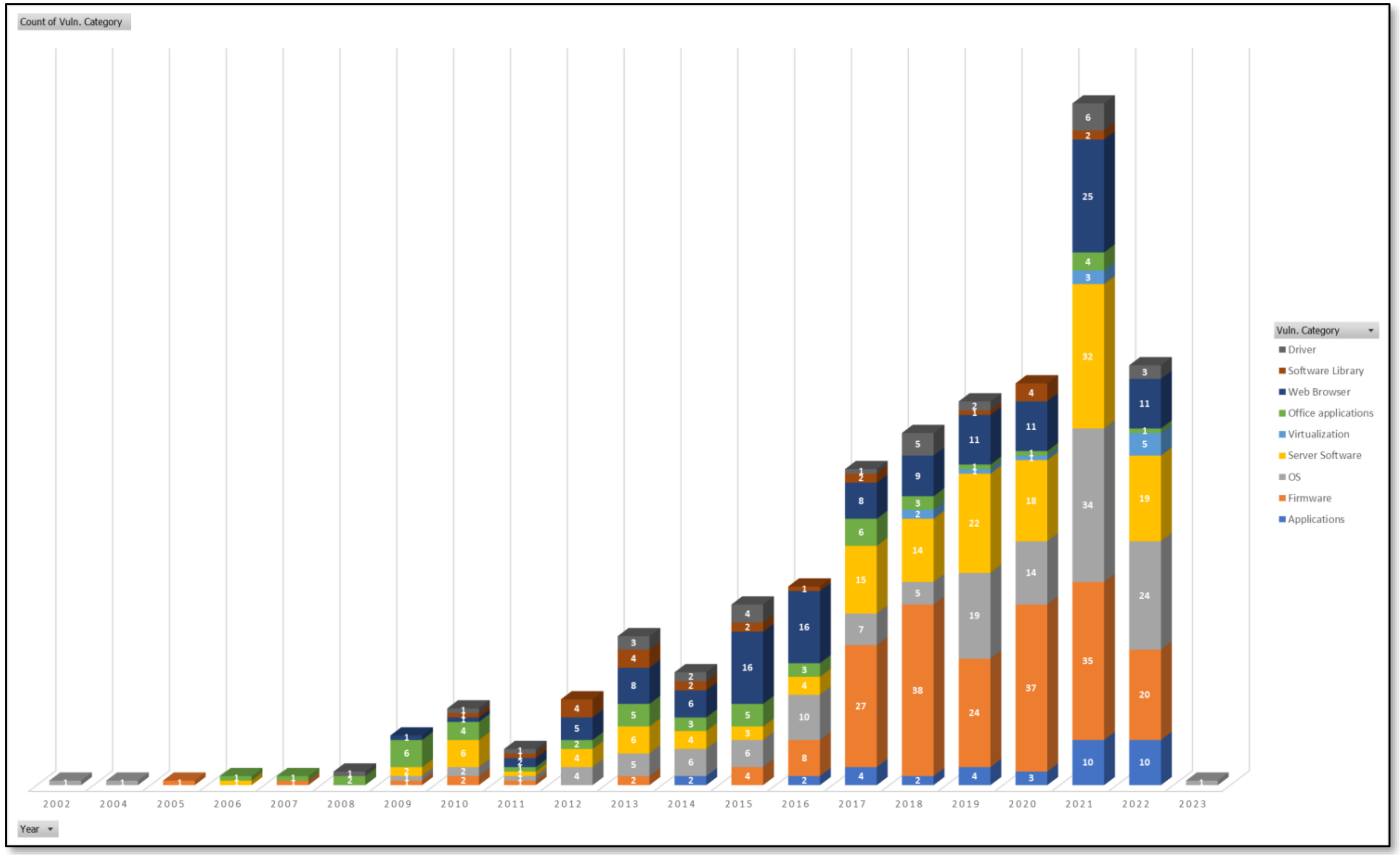
Leaked chat logs show that the Conti ransomware group is actively looking for firmware vulnerabilities, specifically in Intel ME technologies.

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.

Known exploited vulnerabilities (CISA)

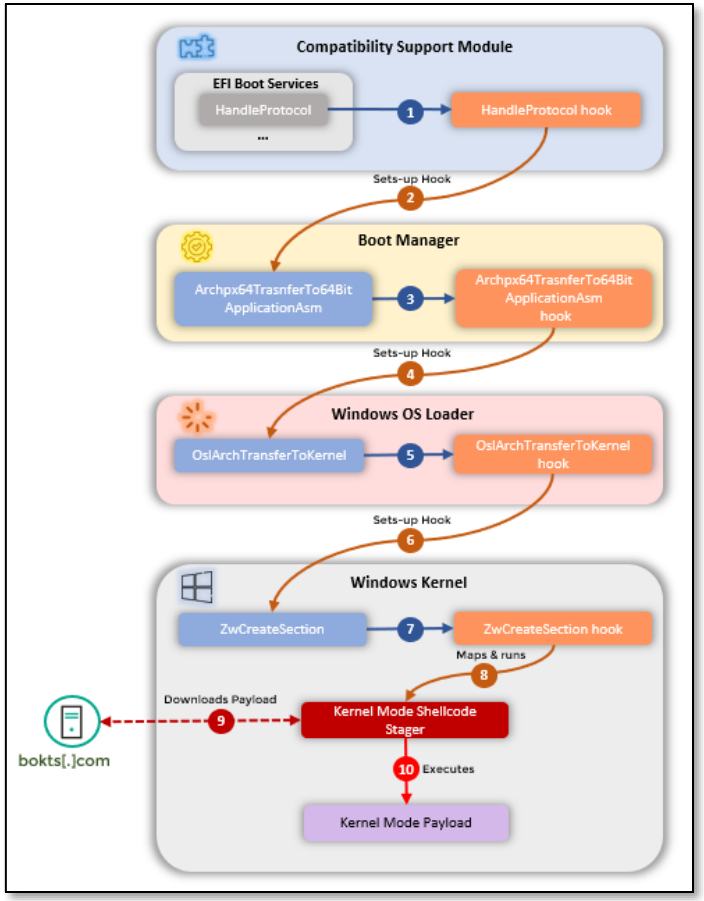
- Started 11/1/22
- Instructs US Gov. on patching deadlines
- Attacks increase over time
- Firmware vulnerabilities have become the most exploited



Implants

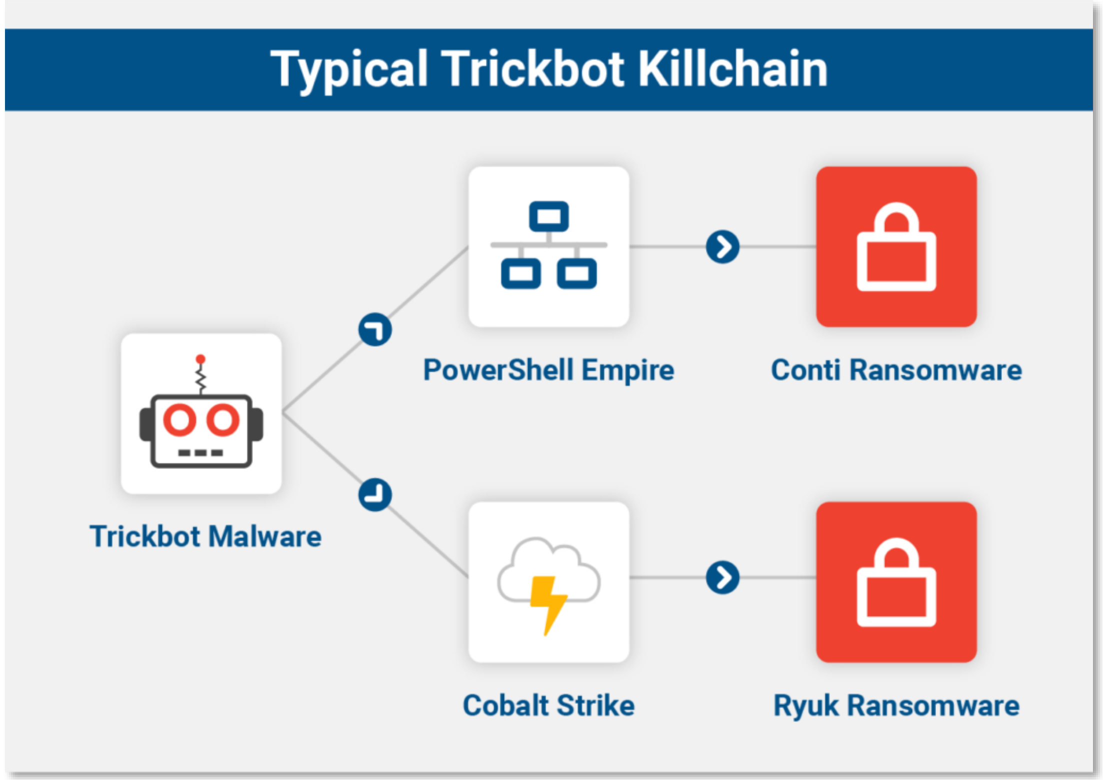
CosmicStrand

- 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



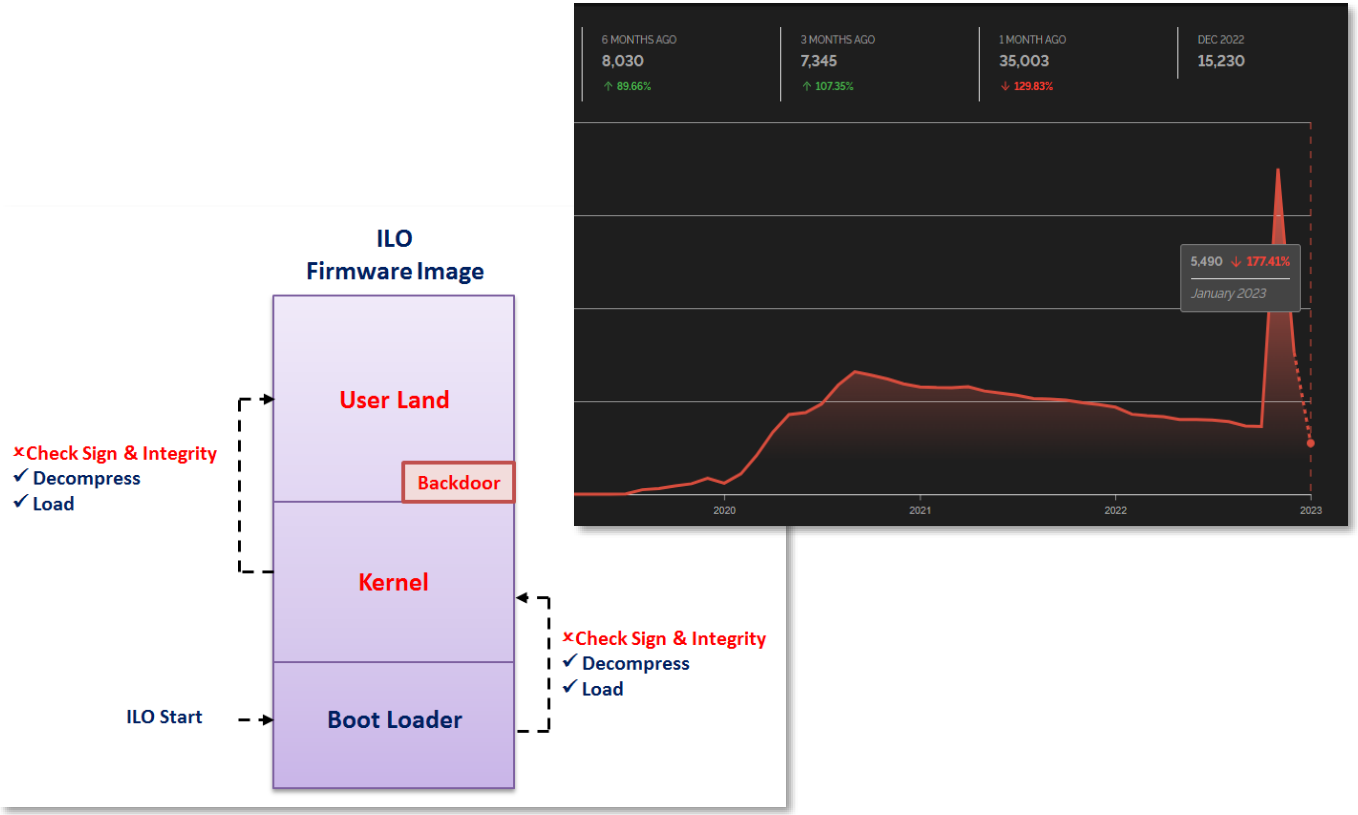
TrickBoot

- TrickBot banking trojan
- Ryuk delivery via Emotet
- 2020: UEFI capabilities
- Check BIOS WP in SPI
- Read, write, erase firmware
- Uses RWEverything, RwDrv.sys (like LoJax and Slingshot)



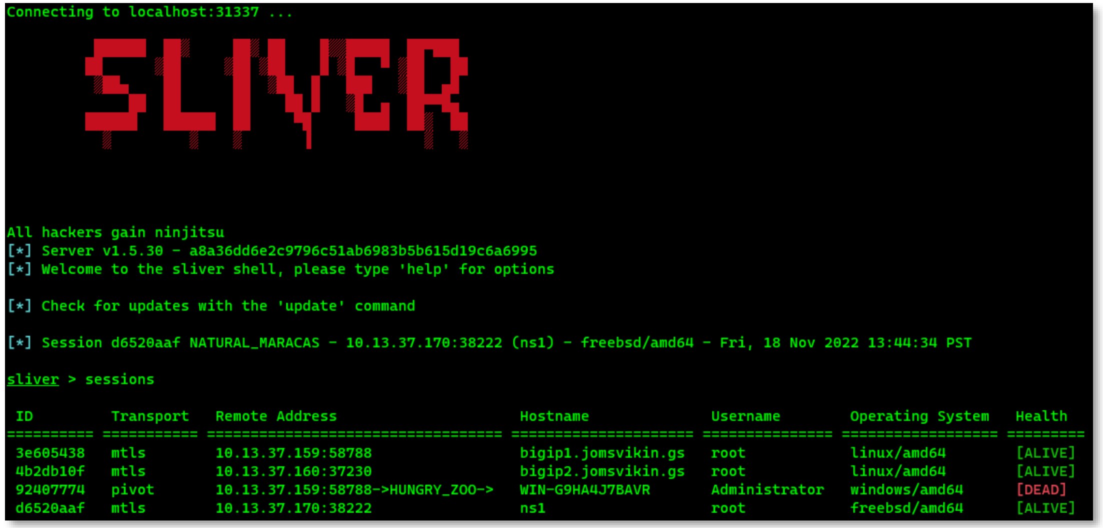
iLOBleed

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



Load balancer research

- UNC3524 (Mandiant)
- F5 Networks & Citrix
- Firmware is Linux/FreeBSD
- Full shells increase attack surface
- Reboot/patch/upgrade proof persistence



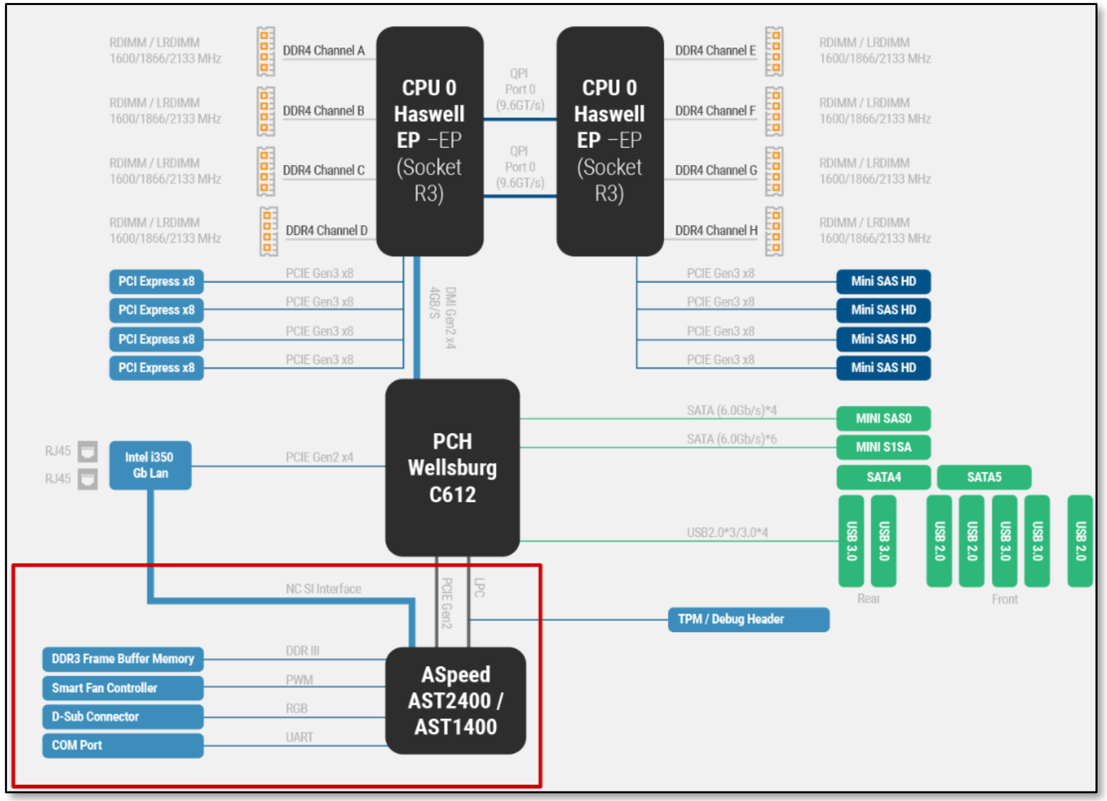
```
Connecting to localhost:31337 ...

    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]
```

Ekoparty 2022: I am become loadbalancer, owner of your network
https://www.youtube.com/watch?v=6T4QsltcZ6k

AMI MegaRAC

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

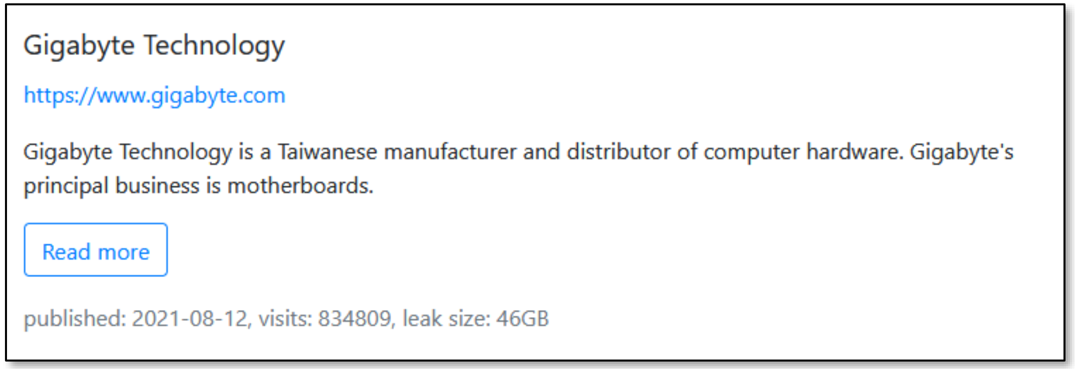


BLUEHAT 2023

Microsoft

Research process

- RansomEXX IP leak
- Top of the supply chain
- Remotely accessible APIs
- Redfish API
- Default user accounts
- Command injection

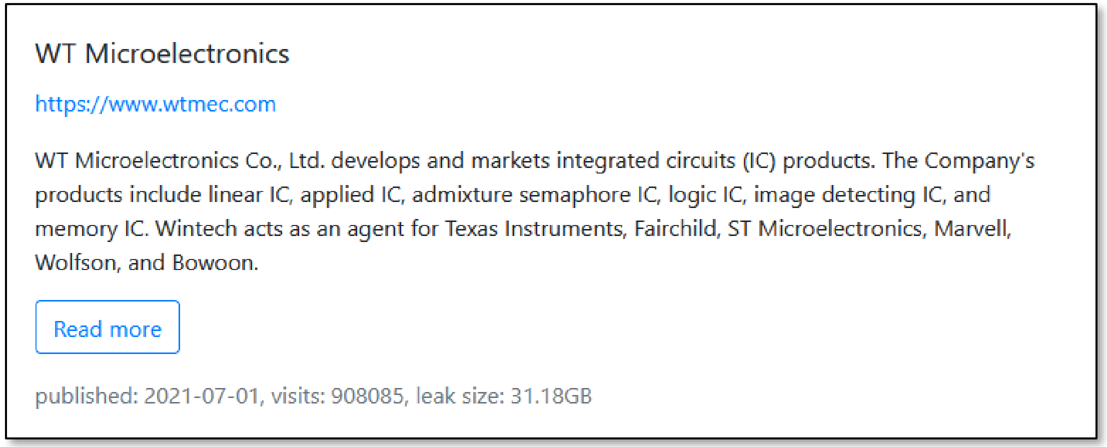


Gigabyte Technology

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

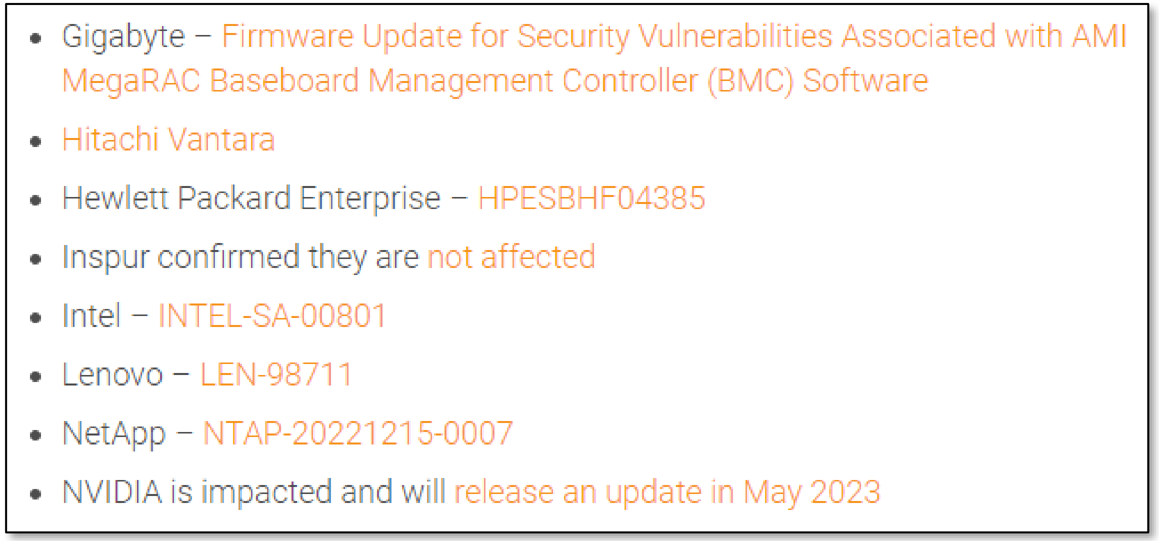
https://www.wtmec.com

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

Vulnerabilities (December 2022)

- CVE-2022-40259 – Arbitrary Code Execution via Redfish API (CVSS 9.9)
- CVE-2022-40242 – Default credentials for UID = 0 shell via SSH (CVSS 8.3)
- CVE-2022-2827 – User enumeration via API (CVSS 7.5)
- CVE-2022-32265 – RCE in qDecoder (fixed by maintainer)
- Low exposure on Shodan
- False negatives due to OEM rebranding
- Higher risk inside a datacenter
- Zero exploitation to date (Greynoise)



- Gigabyte – Firmware Update for Security Vulnerabilities Associated with AMI MegaRAC Baseboard Management Controller (BMC) Software
- Hitachi Vantara
- Hewlett Packard Enterprise – HPESBHF04385
- Inspur confirmed they are not affected
- Intel – INTEL-SA-00801
- Lenovo – LEN-98711
- NetApp – NTAP-20221215-0007
- NVIDIA is impacted and will release an update in May 2023

Vulnerabilities (January 2023)

CVE-2022-26872 - Password reset interception via API (CVSS 8.3)

MegaRAC devices that expose normal HTTP API, for which SMTP integration is also configured, are vulnerable to a password reset interception. Due to how the password reset is implemented, the API does not require any sort of a token in addition to OTP code sent to email.

CVE-2022-40258 - Weak password hashes for Redfish & API (CVSS 5.3)

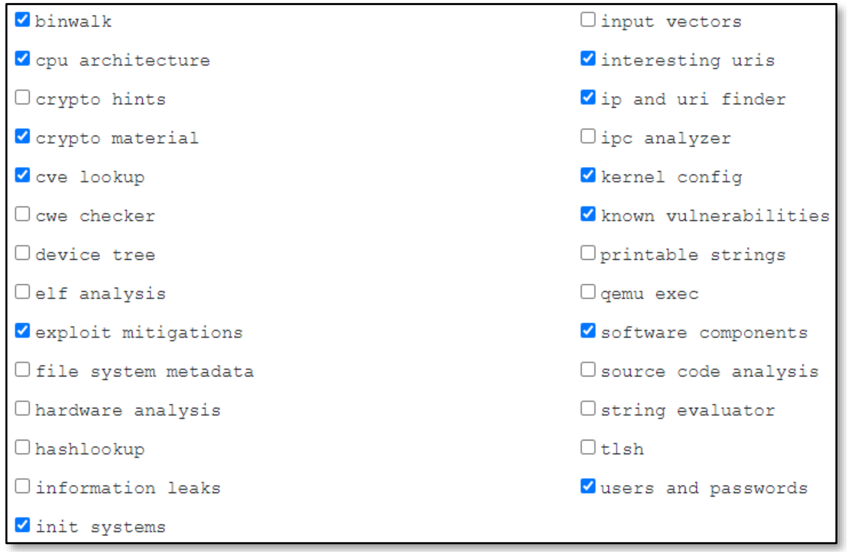
MegaRAC uses either md5 hashing with a global salt (same salt for all passwords) for older devices, or sha512 with unique salts (which is called “Strong” hashing internally) for newer devices.

[redacted]
COMMAND & CONTROL
BMC&C
CVSS v3.1 Score : 9.9 Critical (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

Analysis tools

Firmware Analysis & Comparison Tool (FACT)

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

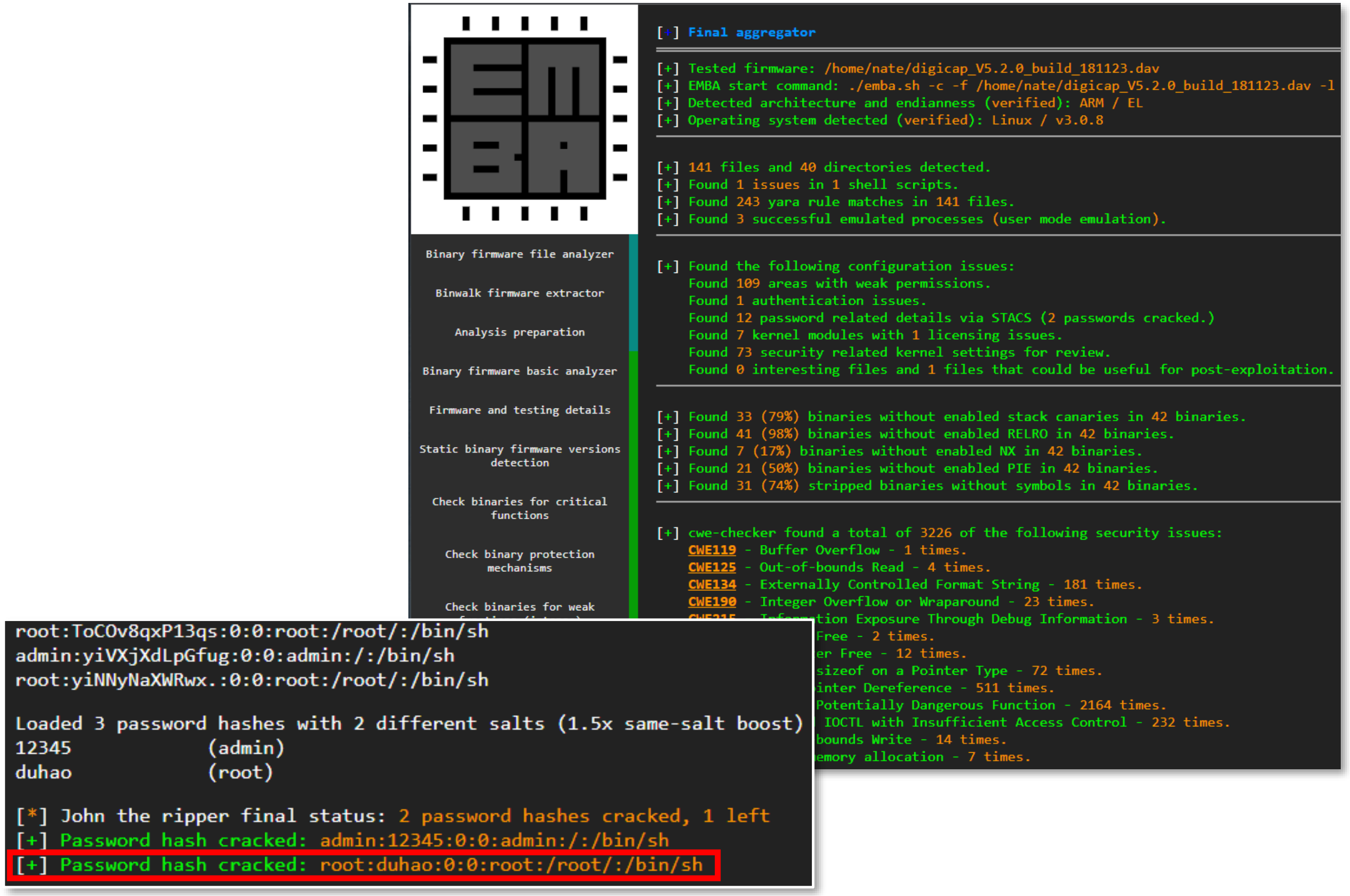


☑ binwalk
☑ cpu architecture
□ crypto hints
☑ crypto material
☑ cve lookup
□ cwe checker
□ device tree
□ elf analysis
☑ exploit mitigations
□ file system metadata
□ hardware analysis
□ hashlookup
□ information leaks
☑ init systems

□ 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

EMBedded Analyzer (EMBA)

- CLI; no database
- More tests than FACT
- KEV data
- Exploit information
- Finds things FACT misses (sometimes)
- Resource intensive
- More complex but tunable



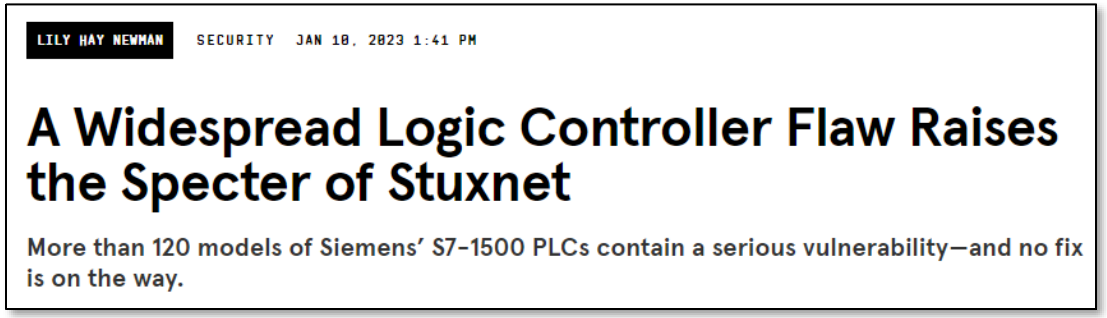
Binary firmware file analyzer
Binwalk firmware extractor
Analysis preparation
Binary firmware basic analyzer
Firmware and testing details
Static binary firmware versions detection
Check binaries for critical functions
Check binary protection mechanisms
Check binaries for weak

```
[+] 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.
           - Information Exposure Through Debug Information - 3 times.
                                                     Free - 2 times.
                                                     er Free - 12 times.
                                                     sizeof on a Pointer Type - 72 times.
                                                     inter Dereference - 511 times.
                                                     Potentially Dangerous Function - 2164 times.
                                                      IOCTL with Insufficient Access Control - 232 times.
                                                     bounds Write - 14 times.
                                                     emory 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
```

Research challenges

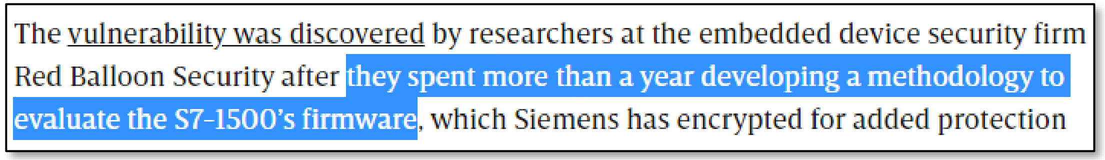
- Proprietary formats
- AES-SBox
- Password protection
- Encrypted images
- Reseller-only access
- App-based updating
- VXWorks



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

A Widespread Logic Controller Flaw Raises the Specter of Stuxnet

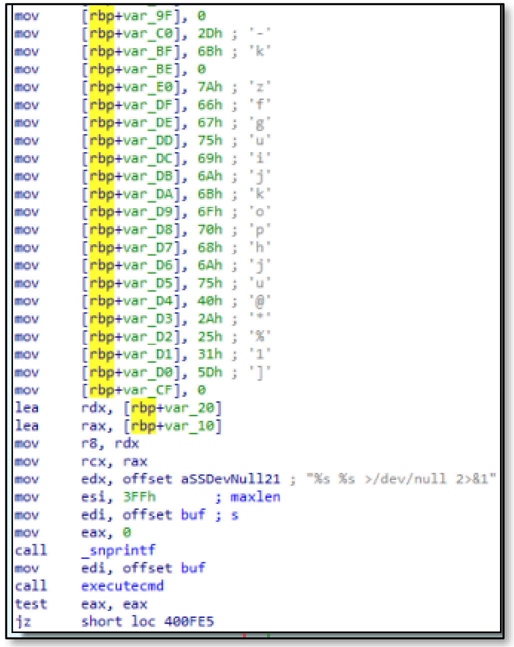
More than 120 models of Siemens' S7-1500 PLCs contain a serious vulnerability—and no fix is on the way.



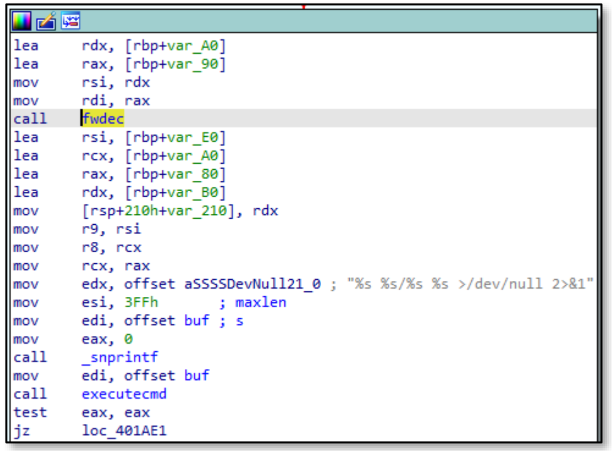
The vulnerability was discovered by researchers at the embedded device security firm Red Balloon Security after they spent more than a year developing a methodology to evaluate the S7-1500's firmware, which Siemens has encrypted for added protection

ChatGPT + IDA

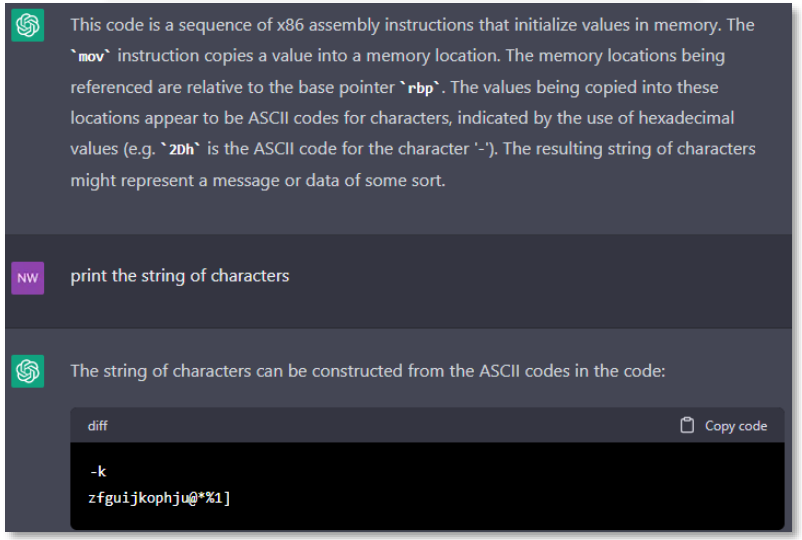
- Cisco ISO images
- Linux tool to decrypt FW
- IDA Free
- ChatGPT
- 1 hour



```
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 aSSDevNull21 ; "%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
```



```
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
```



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.

print the string of characters

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

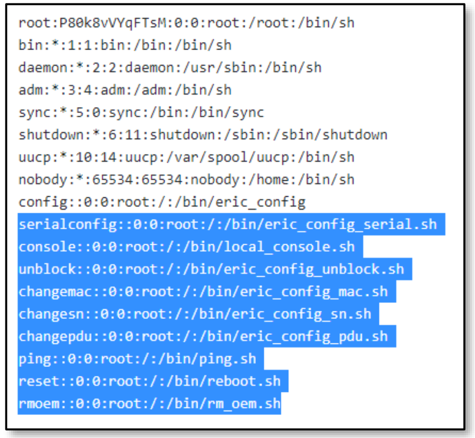
```
-k
zfguijkophju@*%1]
```

https://alperovitch.sais.jhu.edu/an-experiment-in-malware-reverse-engineering/

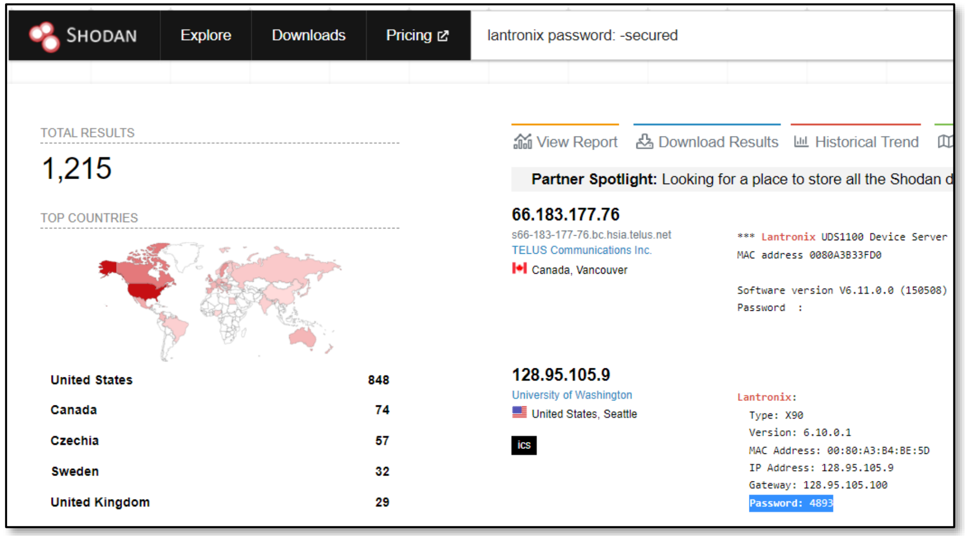
Here be dragons

IP KVM / Terminal servers

- Passwordless accounts
- Shell scripts as shells
- Serial to Ethernet
- Passwords displayed in banner
- Vulnerable OpenSSL



```
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
rmoem::0:0:root:/:/bin/rm_oem.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

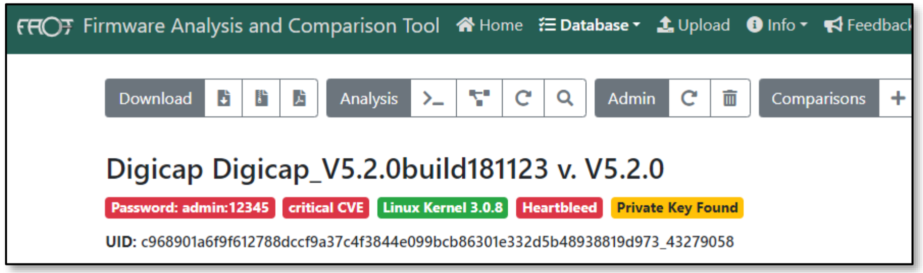
```
*** Lantronix UDS1100 Device Server
MAC address 0080A3B33FD0

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

128.95.105.9
University of Washington
United States, Seattle

```
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
```

Security cameras & cell routers

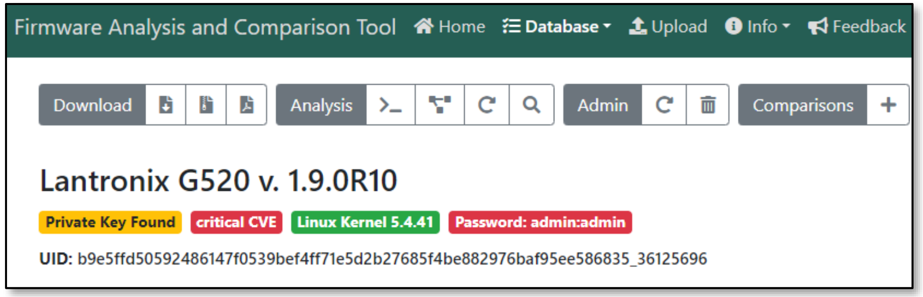
- Shellshock (!)
- Heartbleed
- Default creds
- SMB vulnerabilities



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



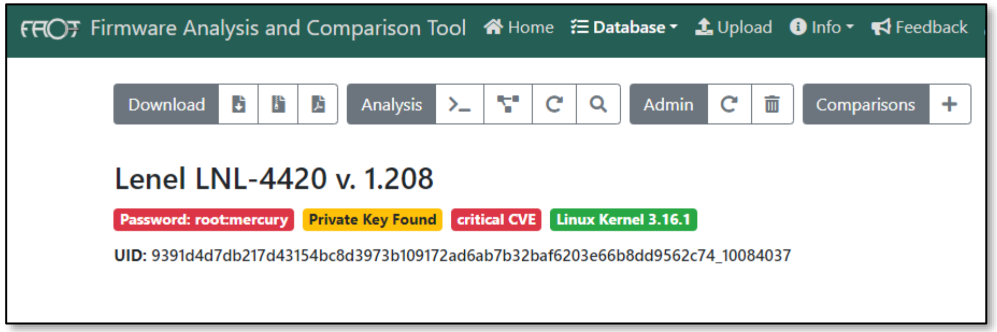
Lantronix G520 v. 1.9.0R10

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

UID: b9e5ffd50592486147f0539bef4ff71e5d2b27685f4be882976baf95ee586835_36125696

Access control systems

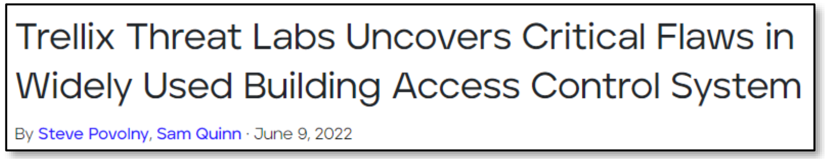
- Busybox CVEs
- Default credentials
- Ancient Linux kernels
- Extremely hard to obtain firmware images



Lenel LNL-4420 v. 1.208

Password: root:mercury | Private Key Found | critical CVE | Linux Kernel 3.16.1

UID: 9391d4d7db217d43154bc8d3973b109172ad6ab7b32baf6203e66b8dd9562c74_10084037



Trellix Threat Labs Uncovers Critical Flaws in Widely Used Building Access Control System

By Steve Povolny, Sam Quinn · June 9, 2022

Untestable vendors

APC by Schneider Electric
CRESTRON
EATON
TRIPP·LITE
HID
Honeywell
Johnson Controls
Liebert
Mitel
Powering connections
Raritan
A brand of legrand

Takeaways

Everything runs firmware

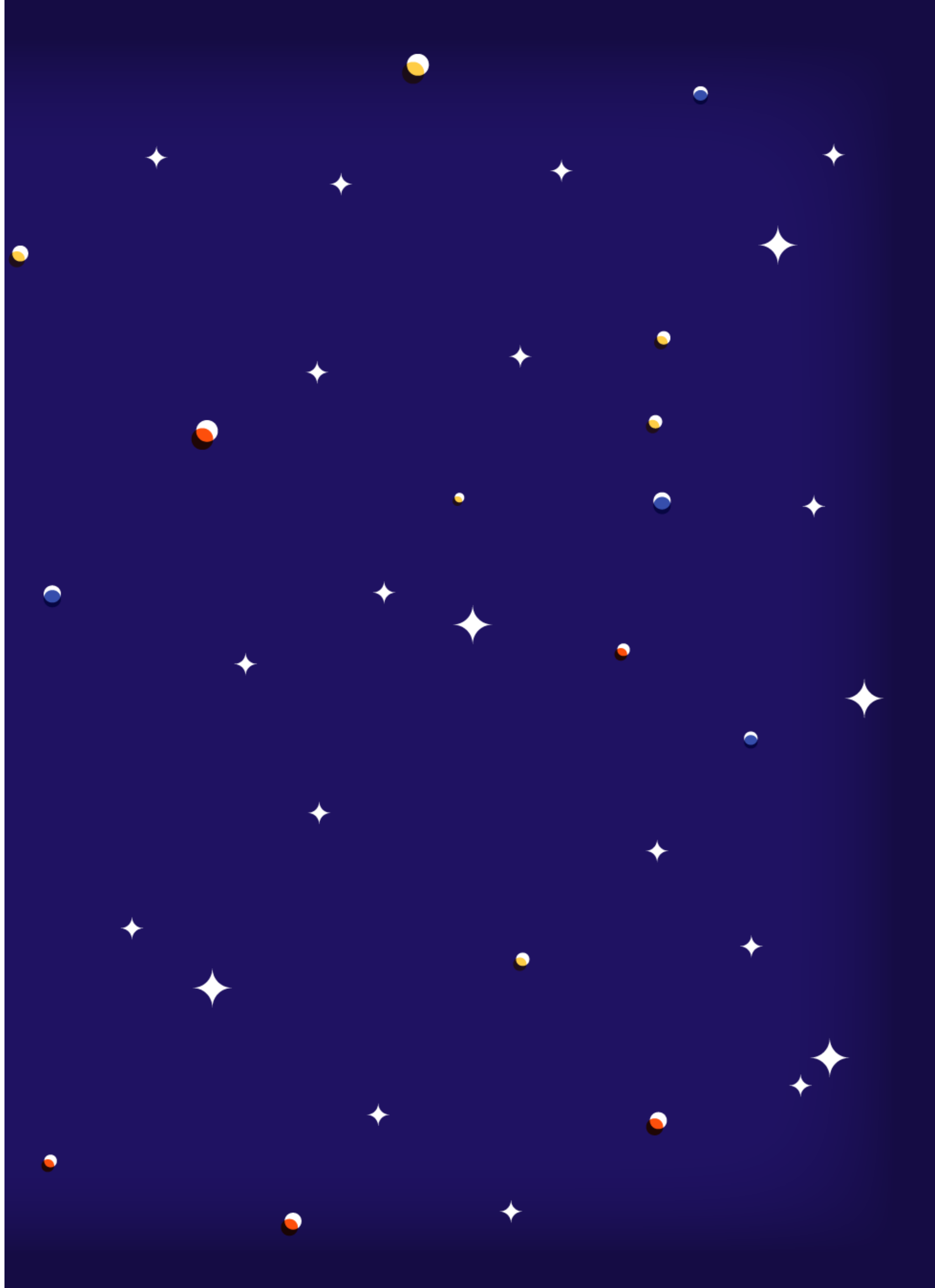
Anything on a network is a target

Attack cadence is increasing

Attackers are always a step ahead

Visibility & research are hindered

Vendors need better accountability



MICROSOFT SECURITY RESPONSE CENTER
BH 23
BLUEHAT 2023 • REDMOND, WA USA

Microsoft