eclypsium

BELOW THE SURFACE

THREAT REPORT

SPRING 2023

NATION-STATE GRADE UEFI BOOTKIT BLACKLOTUS

SOFTWARE SUPPLY CHAIN ATTESTATION TIME IS HERE

BMC&C - TRUE LIGHTS OUT VULNERABILITIES

AND MORE ...

TABLE OF CONTENTS_

BELOW THE SURFACE_

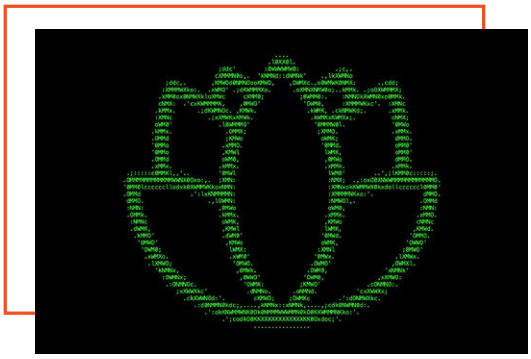
SPRING 2023

Welcome to the Spring edition of the Below the Surface Threat Report. We've made some adjustments to the way we're presenting the content this time around and we hope you like it! This issue covers threats in the wild, industry news, security advisories, security research, and educational tools. We offer insights and takeaways that are designed to help you be more effective in your job whether you're a CISO or a SOC analyst. If you're not already subscribed to Below the Surface, you can do so at Eclypsium.com.

THREATS IN THE WILD

Nation-State Grade UEFI Bootkit BlackLotus

While we've got a deeper-dive blog on this topic, there are a few things we absolutely must point out with this novel threat. Foremost, it marks the first time a low-level campaign like this has been able to summarily bypass the decades old Secure Boot process in order to install a malicious UEFI bootkit. When we first co-discovered this bootkit for sale last October, it was not yet in the wild, but marked a significant advance in the threat landscape, putting low-level tradecraft and tooling in the hands of anyone with $5000 to spend, an extremely low barrier to entry considering this type of fully documented and easy to use UEFI bootkit level malware is normally something we'd expect from nation-states with 'unlimited time and resources'.



Now, it has been discovered in the wild with 16 samples on VirusTotal, some of which have been analyzed. Unfortunately for all of us, the analysis is worrisome on a number of levels both technical and even 'structural'. Technical, because the bootkit disables primary Windows security controls meant to counter such threats such as Bitlocker, Hypervisor-protected Code Integrity (HVCI), and Windows Defender. Worse, it leverages a logic flaw in the Secure Boot process that allows attackers to bypass this core protection Windows relies on to trust the device, allowing any attacker that brings a vulnerable bootloader with them to install a UEFI bootkit like this, even on fully patched Windows 11 systems. This fundamentally breaks Secure Boot and the ability for Windows and any security controls built atop it (AV/EDR/etc) to operate in a trusted state.

Takeaways

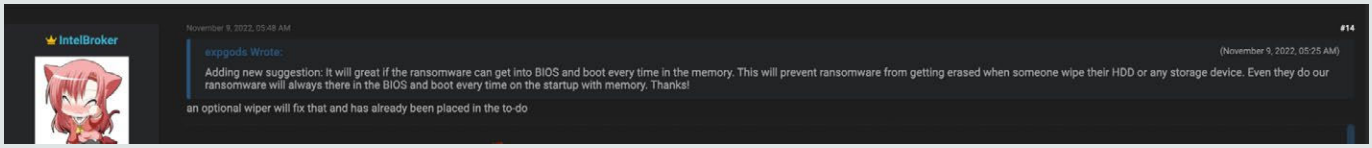
- BlackLotus fundamentally changes the game going forward: we have crossed the precipice security experts have long anticipated wherein low-cost, easy-to-use malware can be utilized by any actor with any motive(s) to gain indefinite, low-level persistence on a host, at the root of trust level of power and stealth.
- Effectively, we now have a 'forever-day' primary state to operate under going forward: Any actor with $5000 and a vulnerable bootloader can achieve low-level persistence under the operating system, with the ability to disable arbitrary security controls and evade detection in the majority of missions and enterprises.
- The only true fix would be for industry to revoke all known vulnerable bootloaders. Yet, this would render all related existing Windows installation/recovery media, and old backups, to fail to boot. "Well, in that case, can't I just disable Secure Boot and still restore?" Sadly, no. Boot failure would still occur due to the bootmgr still needing to check its own signature.
- Despite most AV/EDR tools being unable to detect BlackLotus, it is still possible with Eclypsium's solution and will even be denoted as such in the alert.
- BlackLotus represents a quintessentially ideal way for ransomware actors, nation-states, and criminal actors with any motive, to indefinitely evade and persist within any environment whether IT or OT. The time is now to gain low-level visibility into vulnerabilities and threats on devices, incorporate such tactics into DFIR and Recovery playbooks, and proactively mitigate the significant risks associated with them. These threats are those that *stand to cause the most impact* to safety, uptime, and revenue.
- Note that hackers have already ported the use of Baton Drop SB bypass to the Snapdragon ARM platform to be able to load unsigned bootloaders on Windows RT mobile devices. This is just the beginning of what is to come for Secure Boot bypass.

IntelBrokers Target Another IT Supply Chain Victim ... But Wait There's More

IntelBrokers have ransomed a large IT supply chain victim and posted their data for sale to the highest bidder. This would be the fourth ransomware data leak from the same manufacturer in only two years. Prior to the latest victim , they have targeted another large chip manufacturer. These IT suppliers make for ideal victims, given how valuable and coveted the data they have is to other threat actors, industry competitors, and nation states that compete with or want to attack the supply chain.

The current victim's data that is for sale contains dozens of firmware binaries, iso images, and vendor flash tools, along with extensive SOP (Standard Operating Procedures) for technicians to be able to service, repair, and update the myriad devices they produce. The data may further contain passwords, keys, default creds or other internal secrets that may be useful for follow-on activities of the attackers, or the buyer of the exfiltrated data.

But wait, there's more. The same author is also building wiper malware that destroys the MBR if the victim doesn't pay. As can be seen in the screenshot below, a comment posted by another member on the forum recommends the author build in the ability for the malware to hide in the BIOS in order to survive eradication and restoration efforts of the victim. The author's reply at the bottom shows they've already been thinking along the same lines, alluding to an alternative wiper that would 'fix that'. This doesn't bode well if the implication is that a BIOS level bootkit has destructive capability apart from the primary MBR wiper. It would give an attacker even greater leverage in the context of digital extortion, too.



Takeaways

- The stolen data contains technical manuals, software tools, backend infrastructure details, product model documentation for phones, tablets, and laptops, BIOS images, ROM files, ISO files, and replacement digital product keys (RDPK), a trove of data that may or may not have repercussions in terms of elevated cyber risk to users of these products. It may provide an infrastructure roadmap to future attackers, and some of the OEM tools themselves may be useful to conduct certain tactics related to BIOS flashing.
- As seen in this attack, the ransomware attack leading to AMI's source code leak, and in the latest developing ransomware attack by the "Money Message" group against a top-tier motherboard manufacturer (stay tuned for that story), criminal actors fully realize the significant leverage they gain by leaking source code of developers and OEMs up and down the IT supply chain. The net effect increases the attack-ability of devices in the IT supply chain.
- IT Supply Chain targets are not the only victims being extorted under the threat of leaked source code. It also happened to Canada's second largest Telco. Once attackers determine viable ways to harm organizations for the sake of leverage, the trend typically propagates across different campaigns and actor groups. DFIR teams should begin actively anticipating actors searching for activity related to developer account credentials and devices in the development environment.
- The best risk mitigation for end users and organizations using the IT supply chain devices whose tools and source code have been leaked, is the capability to verify known-good firmware images on these devices, and the ability to analyze them for high impact vulnerabilities and threats that manifest as the result of such leaked data and/or compromised development environments.

Another Anti-Invasion Whistle-Blower Shares "The Vulkan Files"

In a development reminiscent of the Conti and Trickbot leaks (tens of thousands of internal communications involving the developers, leaders, and operators of the group) a former employee of the Vulkan organization has come forward to reveal a treasure trove of data on Russian offensive cyber operations. The individual responsible for the leak, much like the anti-Putin member in the aforementioned leaks, has blown the whistle.

Рисунок 69 - Отображение на электронной карте интегрированной обстановки в режиме «объединённый», без указания количества элементов

While this information has not yet been made public beyond select media organizations and cyber consulting firms, the reporting thus far is a firm confirmation of the campaigns and strategies that Russian cyber intelligence operations are planning and/or utilizing against their perceived western enemies.

One of the discoveries is a powerful tool known as Scan-V, which collects vulnerabilities from an extensive database and scans the Internet on a routine basis for potential targets that can be exploited in attack campaigns. This tool has already been tested, most likely by the infamous Russian GRU "Sandworm" group, which is responsible for some of the most destructive attacks in recent history, such as NotPeya and the Ukrainian power grid attacks.

Another project connected to Russian cyber intelligence operations is the Amezit program, which includes a sub-component known as Crystal-2V. This is a cyber-offensive training program designed to simulate the attack methods used to target critical infrastructure, such as railways, airports, power grids, waterways, ports, and industrial control systems.

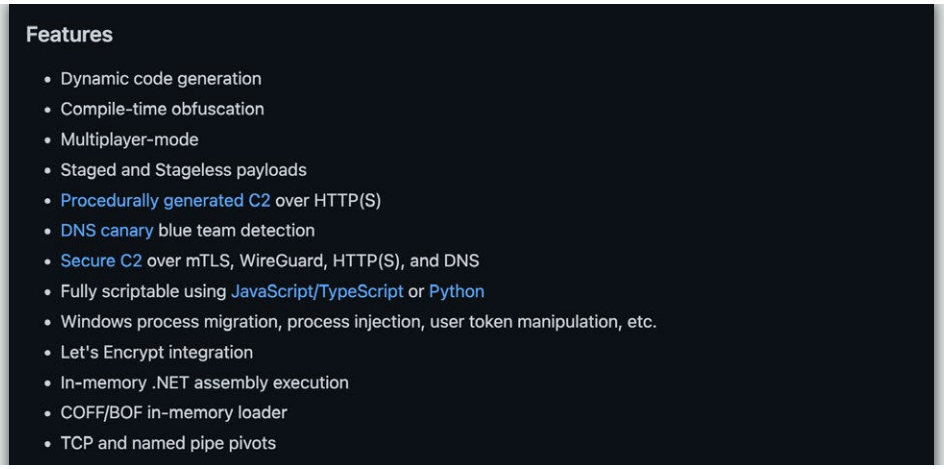
A dashboard, displayed above, seems to reveal Internet infrastructure in a given area. Operators can click on each area circle to get drill-down information on their intended targets.

Takeaways

- Taken as a whole, and extrapolating from what has been witnessed in Russia's strategy against Ukraine, the overall mission support for these programs may be to provide the capability to affect a population's morale by causing disruption of critical infrastructure, mass-automated disinformation campaigns on social media and overall cyber-warfare readiness in launching future cyber attack campaigns.
- This is only a glimpse into a single 3rd party developer of such capabilities. Sandworm has built other cyber weapons such as Cyclops Blink, a massive botnet residing on firewall firmware, capable of traffic manipulation, destruction of the infected host device, and further exploitation of downstream devices. It is also used to monitor Modbus SCADA protocols, indicating a mission objective of targeting ICS and critical infrastructure. A large portion of this capability has been disrupted by western intelligence agencies, but the campaign can easily be expanded to other network-connected devices beyond the initial test-phase of the discovered campaign targeting only WatchGuard firewalls.
- Knowing that nation state adversaries are continuously scanning externally facing devices for vulnerabilities, organizations should employ technology that does the same, and that goes beyond typical vulnerability management solutions in order to independently identify, patch, and validate that patches have been deployed quickly and that there are no threats residing on the devices themselves. Relying on traditional net sec ops or IT/platform ops to keep pace with the threat landscape has proven unsatisfactory for the majority of large enterprises, and is a primary reason threat actors target them.

BYOVD Yeah You Know Me

There is an unignorable trend for attackers of all ilk and motive: bringing with them vulnerable drivers (or even signed legitimate drivers) in order to perform Windows kernel level tasks from user space, allowing them to disable and bypass any number of OS-level cyber controls like AV and EDR, or built-in controls like Defender. Recent examples of this include a new campaign that exploits common vulnerabilities in externally facing services, and leverages powershell to load tools designed to leverage these vulnerable drivers, such as the one from Genshin Impact, a video game anti-cheat driver that has been used to great effect since the summer of 2022. This technique is allowing attackers to load powerful post-exploitation kits like Cobalt Strike or Sliver to perform network surveillance, command execution, reflective DLL loading, session spawning, process manipulation, and pretty much anything else an attacker wants to do:



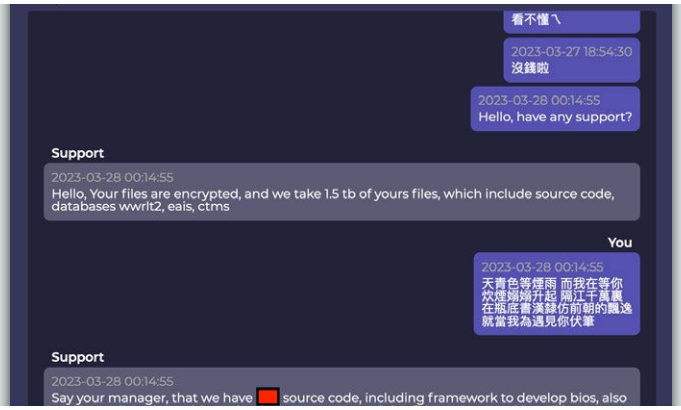
Takeaways

- Even when vulnerable drivers are discovered and patched by the vendor, attackers are simply bringing the older vulnerable versions that are still signed (and therefore still trusted by Windows). For example, the driver used by recent Scattered Spider attacks is signed by different certificates stolen from signing authorities NVIDIA and Global Software LLC.
- Though there are some ways to attempt to mitigate this Windows trust dynamic, in practice, very few target organizations are equipped and practiced in doing so. BYOVD (Bring Your Own Vulnerable Driver) attacks will be with us for a long time to come.
- For an excellent write-up of this problem, the seminal research done by Eclypsium in their Screwed Drivers report is an excellent read and an easy way to get up to speed.
- To make matters worse, in many cases the very drivers and tools that would be used to update device firmware are themselves vulnerable and provide a potential avenue for attack. As a result, organizations should not only continuously scan for outdated firmware, but also update to the latest version of device drivers when fixes become available from device manufacturers. Organizations should also keep their firmware up to date, scan for vulnerabilities, and monitor and test the integrity of their firmware to identify unapproved or unexpected changes resulting from the abuse of drivers.

A New Ransomware Actor "Money Message" Targets IT Supply Chain

A newer ransomware actor has hit the ground running leveraging a reportedly poorly written ransomware payload and data-theft extortion tactic. What's more relevant is what one researcher noticed in some files on VT that led to the discovery of a victim chat window in which a major IT supply chain vendor (MSI) that manufactures motherboards and other components for laptops, servers and IOT devices,has had their data leaked. The data includes sensitive private keys, development framework, and other tools. This dynamic harkens back to a similar situation in which source code from another top-level IT supply chain was leaked, which led to the discovery of high-impact vulnerabilities in that source code that Eclypsium researchers were able to safely disclose to the victim via an extensive CD effort.

Read the screenshot of the victim chat below, and take not of the specific leverage they are using in the context of extortion.



Takeaways

- Here the actor is explicitly threatening to 'spread' (leak or sell) source code, signing keys and their BIOS development framework, should the victim not pay the ransom. The victim is now forced to consider longer term business, competitive and reputational impacts as a result.
- Given the source code has been leaked, the impact may result in other threat actors finding backdoors, keys, and vulnerabilities that might allow them to author malware campaigns that leverage them.
- When considering Cyber SCRM threat modeling, it is important to factor in this criminal threat to the IT supply chain, and the additional risks, and broad impact potential of such attacks. It's a dynamic that will only grow over time, and re-enforces the need for organizations to be able to inventory and assess the threats and vulnerabilities that result from these criminal acts.
- This actor so far has been focused on Big Game Hunting, targeting an Asian airline with $1B in revenue as well, and asking for million-dollar payments.
- The only mitigation organizations have against potential follow-on attacks stemming from such critical leaks in the IT supply chain, is to baseline the firmware of the devices in their IT supply chain, and be able to detect vulnerabilities and threats resulting from the leaks. Without this critical capability, there is no way for an organization to proactively manage IT supply chain risks, let alone respond to subsequent attack campaigns stemming from it.
- To follow our ongoing research into this incident, and analysis of the leaked sourcecode and development tooling, along with potential impact scenarios, please see our blogs, part 1, and part 2.
- The Eclypsium platform will allow customers to know which makes and models are affected in their environment, and will be continuously updated with new detections based on our ongoing research.

.

Destructive PIPEDREAM Malware: Why It's in the News Again

A recent article in Politico titled "Russian-linked malware was close to putting U.S. electric, gas facilities 'offline' last year" highlights just how very close the US was to experiencing major disruptive outages related to a Russian state-sponsored actor group called Chernovite. While the discovery of this malware and campaign dates back to spring of 2022, it is drawing significant attention again given the recent escalation in the hybrid conflict between Russia and NATO allies. Why? Because a) the campaign is still active and represents a "wartime capability" and b) the operators are still potentially 'one click away' from being able to heavily disrupt operational environments within the energy sector.

Among a plethora of capabilities the malware has, is the ability to run DDOS attacks from within the OT environment to target ICS systems. Once such a payload is deployed, there isn't much operators can do to prevent a material impact to safety systems. The malware also leverages an signed and trusted exploitable supply chain driver from motherboard manufacturer ASRock, in order to facilitate privilege escalation and lateral movement, allowing the malware to spread to more than just the host it lands on. The malware is further meant to support a scalable operation, allowing even non-ICS skilled attackers to use graphical interfaces to change settings or launch attacks. There's even a 'Packet of Death' button that with a single packet brings down a targeted ICS device and requires reboot and restoration to recover from. That amount of tooling and UI is reminiscent of what was observed in the ShadowBrokers leak of US intelligence hacking tool sets, further affirming this is a Russian state-sponsored campaign.

As far as attribution into which APT specifically is behind the campaign, the answer is even less clear, but Occam's razor points to Russian GRU war-time operations. However, likely not the Sandworm contingent, infamous for Not-Petya and the more recent Industroyer2 campaign that also targets ICS infrastructure. Perhaps it is a newer group akin to FROZENVISTA (UNC2589), responsible for the WhisperGate wiper attacks. Right now, we just don't know..

Takeaways

- Increasingly destructive attackers continue to take advantage of 'insecure by design' flaws in devices. A study by Vedere Labs found 56 such vulnerabilities in devices from 10 manufacturers, including those targeted by INCONTROLLER. One in five of those vulnerabilities allow for manipulation at the firmware level. This mimics the current trend we see across the entire IT supply chain, where one out of every four CISA Known Exploited Vulnerabilities (KEVs) is a firmware vulnerability.
- The call to arms here remains the same: Now is the time to get ahead of destructive motive attacks by gaining low-level visibility into threats and vulnerabilities being targeted at the device supply chain level. This is critical both in terms of proactive risk management, as well as being able to respond effectively in the case of an incident.
- CISA has an advisory on the INCONTROLLER malware that includes important recommendations to proactively put in place. Among them is the need to conduct hashing and integrity checks on firmware of devices, and the monitoring of systems for loading of unusual drivers like the ASRock motherboard driver.

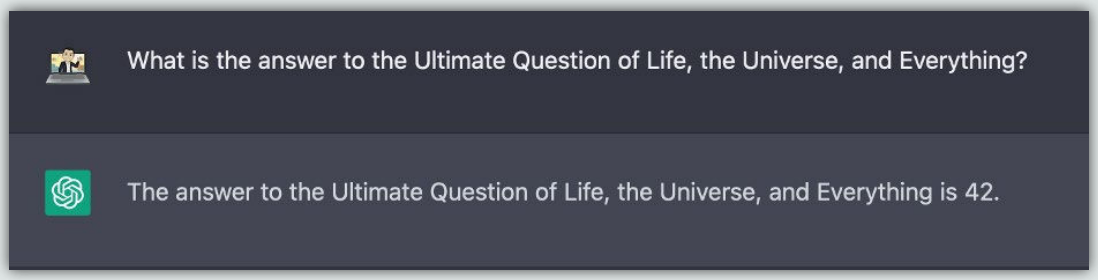
ChatGPT - The Newest Tool in the Bad Actor's Arsenal

ChatGPT seems to be all the buzz lately with commentary ranging from "It will destroy the world!" to "It's the greatest thing since sliced bread!" One thing for certain is the explosive growth of the multitude of models, uses, and capabilities without a plateau in sight.

Recently, industry experts and executives called for a halt of advanced AI development citing irreparable risks to society, research has been showing a dramatically reduced cost to train additional models using previous generations for feedback, and self-hosted models appear within a matter of weeks.

In the same time that positive and impactful uses of the technology are discovered, nefarious individuals and researchers are quickly finding alternative strategies to advance their tactics, techniques, and procedures. Phishing, business email compromise, and social engineering can now be performed at scale with a level of realism that will surprise even savvy users. Even polymorphic malware can be generated with the intent and capability to bypass current EDR solutions.

This leads to trying to find ways to evade the rules and capabilities of the models in question. Malicious prompting allows abusers to manipulate the models to respond in ways they shouldn't, allowing these threat actors to generate malicious code more expeditiously without being an expert programmer.



Our own researchers have been heavily leveraging ChatGPT in the context of developing tactics attackers might use throughout a novel attack chain to target software below the operating system at the firmware level, with great success, and efficiency gains. The power it provides to the attacker is realized when the attacker's creative instincts are combined with ChatGPT's resourceful ability to both explain 3rd party code quickly and simultaneously output code to perform specific functions quickly. This allows the attacker to move more quickly through roadblocks that would otherwise require a full pause in order to learn a new language, or research a specific way something works before being able to progress further.

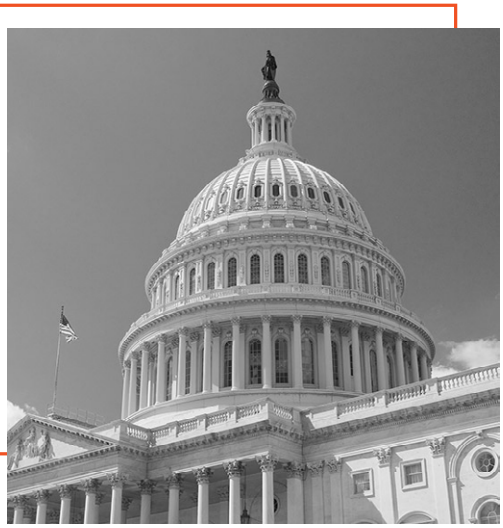
Takeaways

- ChatGPT is just the beginning with other models being made available daily, techniques to rapidly evolve and improve learning time, and adoption of similar technologies skyrocketing.
- As AI becomes more integrated into society and industry, there continues to be growing concerns around the ethical implications and use.
- Attackers are attuned to the technology and are leveraging it to become more efficient, use more directed and advanced tactics, and scale operations.
- Our defenses need to adapt in response to the new opportunities attackers have available, and this will need to be a rapid adjustment to controls and capabilities. Those that are not ready will likely fall prey with ever increasing regularity.

INDUSTRY NEWS

Software Supply Chain Attestation Time Is Here

In response to the extensive supply chain attacks over the last several years, Executive Order (EO) 14028, Improving the Nation's Cybersecurity was created and directs the National Institute of Standards and Technology (NIST) to publish software supply chain security guidance that Federal agencies are required to follow.



More recently, OMB issued M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, which effectively says that Federal agencies must only use software that complies with Government-specified secure software development practices.

Vendors will be required to fill out a common form from CISA, and these will be collected sometime before June 2023. These attestations will be a formal part of the Federal Acquisition Regulation itself.

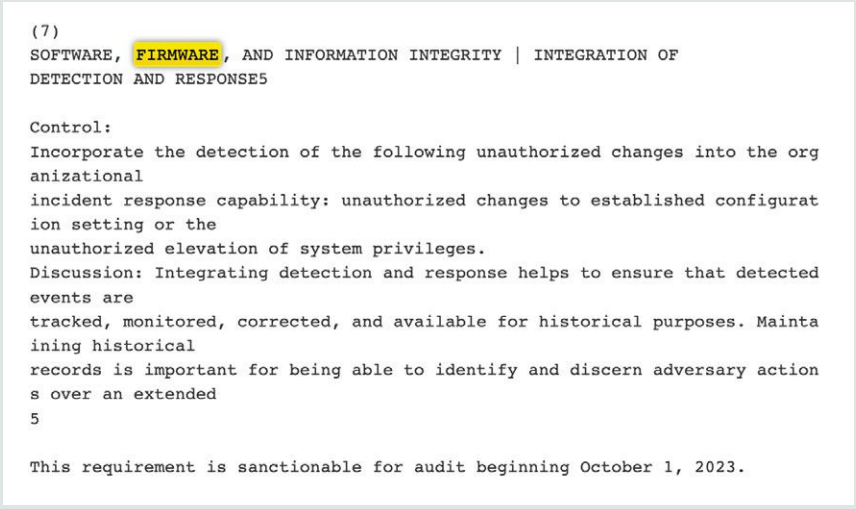
For more background and perspective on this, check out our blog.

Takeaways

- Jen Easterly sums up this recent momentum by the government like this: "Consumers and businesses alike expect that cars and other products they purchase from reputable providers will not carry risk of harm. The same should be true of technology products. This expectation requires a fundamental shift of responsibility. Technology providers and software developers must take ownership of their customers' security outcomes rather than treating each product as if it carries an implicit caveat emptor. To achieve this, every technology provider must begin by creating products that are both "secure by default" and "secure by design."
- The M-22-18 memorandum includes a comprehensive definition of software that must be attested for, which explicitly includes firmware:
- "The term "software" for purposes of this memorandum includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software".
- This means the firmware running Below the Operating System (BIOS/UEFI/BMC's, etc) as well as the firmware powering network devices such as VPNs, Load Balancers, File Transfer Devices, NAS, etc., is also required to have attestation that the vendor has followed the NIST Guidance via SP 800-218, Secure Software Development Framework (SSDF), and via NIST Software Supply Chain Security Guidance.
- Separately, the US National Cyber Security Strategy was recently unveiled and discussed by CSIS with remarks from Acting National Cyber Director Kemba Walden, and Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger. One of the primary goals is reducing systemic technical vulnerabilities in the foundation of the Internet and across the digital ecosystem while making it more resilient against transnational digital repression.
- While attestation from vendors is a great first step, it will not mitigate the IT supply chain risks (threats and vulnerabilities) already within the existing IT supply chain in operational environments. To meaningfully address such risks, federal organizations must be able to scan and baseline their devices at the firmware level, and proactively patch critical high-impact flaws. They also need to be able to detect active threats at the IT supply chain level, using the latest in low-level "Below the Operating System" (BtOS) detection technologies.

Latest Criminal Justice Information Services (CJIS) Security Policy Pays Heavy Attention to Firmware Threats

More and more, firmware is being directly called out in some of the most important guidance across many sectors. NERC-CIP and NIST 1800-34 both call out the need to protect and patch firmware already. Recently, the CJIS Security Policy was updated to also include direct and overt firmware security related requirements. Everything from access controls to firmware, retention of data related to threat activity involving firmware, vulnerability management, routine interval firmware scans, and more. Mentioned a dozen times, firmware security is now firmly embedded in the requirements, and in some cases, not following this policy can result in sanctionable audits related to firmware security.

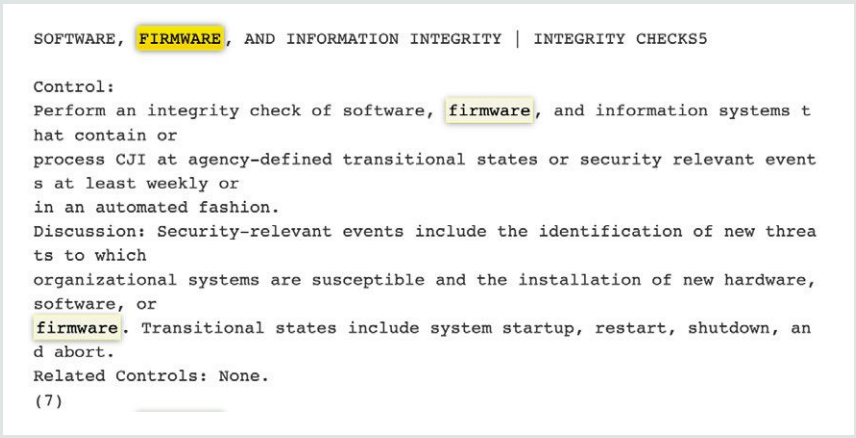


(7)
SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE5

Control:
Incorporate the detection of the following unauthorized changes into the organizational
incident response capability: unauthorized changes to established configuration setting or the
unauthorized elevation of system privileges.
Discussion: Integrating detection and response helps to ensure that detected events are
tracked, monitored, corrected, and available for historical purposes. Maintaining historical
records is important for being able to identify and discern adversary actions over an extended
5

This requirement is sanctionable for audit beginning October 1, 2023.

This requirement means systems storing or processing CJIS data must be able to detect and respond to firmware level threats and unauthorized configuration settings of firmware.



SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS5

Control:
Perform an integrity check of software, firmware, and information systems that contain or
process CJI at agency-defined transitional states or security relevant events at least weekly or
in an automated fashion.
Discussion: Security-relevant events include the identification of new threats to which
organizational systems are susceptible and the installation of new hardware, software, or
firmware. Transitional states include system startup, restart, shutdown, and abort.
Related Controls: None.
(7)

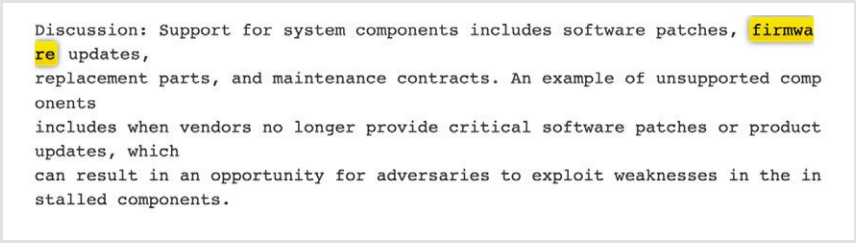
Taken at face value this requirement means CJIS systems must be able to check for integrity changes to firmware every time the system rebooted, shut down or started up, and any time a threat is identified that has the means and opportunity to target the firmware. In a post-BlackLotus world, this means any time an actor gains Admin or root level privilege on a system, firmware integrity must be checked, given the many ways modern adversaries can attack firmware from the user operating system. Whether nation state sponsored or criminal, the TTPs for doing so are readily available, easy to deploy, and pose a direct threat to the firmware attack surface.

```
FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS 5

Control:
Determine if system components have applicable security-relevant software an
d firmware
updates installed using vulnerability scanning tools as least quarterly or f
ollowing any security
incidents involving CJI or systems used to process, store, or transmit CJI.
Discussion: Automated mechanisms can track and determine the status of known
flaws for
system components.
Related Controls: CA-7, SI-4.
SI-3
```

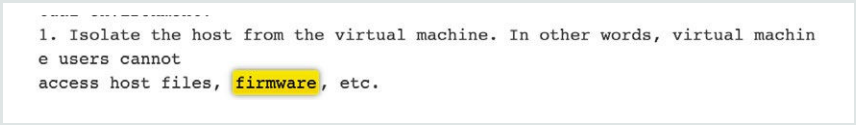
Whether in the context of the required quarterly firmware vulnerability management interval, or in the context of an active or recent incident, a firmware vulnerability scanning technology must now be in place on all systems processing CJI.

```
Test software and firmware updates related to flaw remediation for effectiv
eness and
potential side effects before installation; 5

c.

Install security-relevant software and firmware updates within the number o
f days listed
after the release of the updates;

d.

•

Critical – 15 days5

•

High – 30 days5

•

Medium – 60 days5

•

Low – 90 days; and5
```

Most striking in this requirement are the time-bound requirements to perform firmware updates, ranging from 15 days for critical systems to 3 months for Low priority systems. Organizations will also need a way to verify whether the update may have resulted in lessened security, or firmware versions that are known to have high failure rates.



Organizations will need a way to determine if the firmware on a device processing CJI has been deprecated and will no longer receive support updates.



This requirement speaks to threats such as CloudBorne that are able to move from guest virtual machine OSes down to the UEFI or BMC of the host server.

Takeaways

- Suffice it to say that presently, very few CJIS environments have the necessary tools and technology to meet these new firmware requirements. Luckily, the Eclypsium Platform exists to explicitly address these requirements, and can provide the necessary vulnerability discovery, integrity monitoring, threat detection, forensic insights, and firmware versioning insights required to meet the above requirements. It is likely the only purpose built platform that can do so.
- Requirements are usually derived and turned into policy based on an unacceptable risk to a mission or sector that an evolving threat landscape presents. These are non-arbitrary requirements that serve specific operational objectives in protecting criminal justice information.
- CJIS systems are targeted by some of the most advanced nation-state sponsored and criminal threat actors, all of which have the means, opportunity, and motive to directly target firmware.

EPA Guidance Now Includes Firmware Throughout Cyber Security Water System Sanitary Surveys

The guidance explicitly calls out firmware in a number of sections, covering everything from configuration control, vulnerability and patch management, and table-toping between IT and OT operations. The following guidance sections double down on the critical role firmware plays in the context of safety and uptime for this critical public service:

> **2.5: Does the PWS maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets?**
>
> [...] Maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets? Recommendation: Maintain accurate documentation of the original and current configuration of OT and IT assets, including software and firmware version."
>
> "Attackers often exploit vulnerabilities (i.e., weaknesses) that only exist in certain versions or settings of the software and firmware used to control assets. Therefore, a PWS should be aware of its asset configurations to know whether a newly found vulnerability could be used in an attack on its network."
>
> To fully document asset configurations, include the following details, as applicable: owner (e.g., Engineering Department), physical and network location, vendor, asset type, model, asset name, firmware and/or software versions, patch levels, asset configurations, active services (i.e., automated processes), communication protocols, network addresses (e.g., IP and MAC), asset value, and criticality to PWS operations.
>
> **4.5: Does the PWS offer regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors?**
>
> Develop an agenda in advance of the meeting to allow time for OT and IT personnel to prepare their discussion points. Topics can include new PWS OT/IT hardware, firmware, and software updates; changes in network architecture; reports on updated plans, policies, or procedures; changes in personnel; roles and responsibilities; planned future cybersecurity activities; and emerging cybersecurity threats.
>
> **5.1: Does the PWS patch or otherwise mitigate known vulnerabilities within the recommended timeframe?**
>
> [...]A vulnerability is a weakness in a piece of software or firmware running on a hardware asset. Vulnerabilities can come from mistakes in code or oversights in the software design process, or attackers may intentionally place vulnerabilities in software as a vendor writes the code (i.e., a supply chain attack). An exploit is either a set of actions or a piece of malicious code that attackers use against the vulnerability, helping them breach a computer system or damage an asset.

Takeaways

- Critical infrastructure continues to be a primary target for nation-state actors and hacktivists with disruptive and destructive motives, and guidance is finally addressing those vulnerabilities that stand to do the most harm to public and worker safety.
- Cyber security guidance for other critical infrastructure services has been steadily incorporating device level firmware directly into its latest guidance, including recent guidance for US railways, in the context of vulnerability management, for example.
- These new requirements require organizations to have the low-level visibility to detect threats and vulnerabilities in the IT supply chain, and the associated reporting necessary to validate having met the requirements. Eclypsium is best suited, and purpose-built for doing just that.

SECURITY ADVISORIES

BMC&C - True Lights Out Vulnerabilities Affecting Over A Dozen Vendors

Eclypsium's BMC&C report is one of the most impactful Cyber Supply Chain vulnerability research efforts in recent times. Analyzing leaked source code from a ransomware operation, our researchers found three vulnerabilities in AMI's firmware affecting millions of down-stream devices found in data centers and server environments around the world. The impact potential combined with the low technical skills needed to exploit them profoundly changes the threat landscape and represents a quintessential example of the modern day IT supply chain challenge and how shared vulnerable code propagates to top-tier OEMs—in this case, well over a dozen of them! Threat actors leveraging the vulnerabilities will enjoy omnipotent power, stealth, evasion, and persistence. Worse still is the ability to cause catastrophic downtime and material impact to data centers by rendering devices inoperable and further preventing victims from being able to recover.

The fives vulnerabilities are:

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-2022-26872 – Password reset interception via API
CVE-2022-40258 – Weak password hashes for Redfish & API

Importantly, the first two of the vulnerabilities leads to an Admin level linux shell on the BMC itself, such that actors can further script and automate actions that would cause indefinite disruption by continuously powering off the machine and/or spreading laterally in homogenous environments to do the same to servers on the same logical network segment.

Ironically, the BMC here serves as all three: a) an easy initial vector in b) the power to perform impactful or disruptive actions and c) the last line of remediation in recovering servers, which would be inaccessible and unusable by victims once the attacker disables listening services on the BMC. The only recovery option would then be re-flashing every BMC on the downed segment, or potentially an entire data center environment.

Takeaways

- Top OEM vendors AMD, HP, Asus, Dell, EMC, Lenovo, Qualcomm, NVidia, Quanta, Ampere Computing, ASRock, ARM, Gigabyte, Hitachi, Vantara, Huawei, Inspur, NetApp, and Tyan have all be affected by these vulnerabilities. There are varying degrees of patches available from many, but not all. Many data center operators may only choose to patch BMC firmware during occasional planned-downtime windows, or only ad-hoc when and if absolutely needed. However the potential impact of not detecting and patching these vulnerabilities, in this case, far outweighs the temporary operational impact of doing so proactively.
- Given the ease of exploitation, the massive blast radius across so many top-tier OEMs, and the key advantages afforded to attackers in targeting them for persistence, evasion, espionage or disruption/destruction, organizations should revisit their DRP, DFIR, and BC assumptions and associated playbooks going forward. BMC-level threats no longer reside in the 'acceptable risk' or 'offsettable risk' category in the context of the enterprise risk register or mission assurance.
- The research effort behind BMC&C was coordinated with AMI, CISA, and others, and was one of the most challenging and complex CD efforts in our team's history, owing to the complexity and operational challenges of the IT supply chain itself, and the sheer number of affected downstream vendors and OEMs. Such is the nature of cyber supply chain dynamics, and the broader geo-political, economic and wartime motifs of late via technology sanctions, chip wars, supply chain inventory challenges, and the cyber threat landscapes' recent focus on device-level attack tactics.
- BMC vulnerabilities, when exploited, also provide attackers a direct path to the UEFI/BIOS, and allow attackers to flash the BIOS or modify its settings with malicious code and/or configurations. In order to mitigate, or even detect adversary actions at this level, organizations must have high-confidence low-level visibility into device firmware running underneath the user operating system and the rest of the entire security stack built atop it. Needless to say, this is where Eclypsium shines best.

SECURITY RESEARCH

Just How Many Externally-Facing Devices are Vulnerable to Known-Exploited Vulnerabilities? The Answer Will Shock You

New research has answered the question many of us have had when it comes to knowing just how large the blast radius is for CISA's curated list of Known Exploited Vulnerabilities (KEVs). Turns out, there's over 15 million publicly facing services with one or more of the 896 KEVs tested for.

The company behind the research, Rezilion, used Shodan and Greynoise in their research. Below is a table from their report showing the top non-Windows CVE's that are vulnerable. Four out of six of them are over five years old. 800,000 known-exploited vulnerabilities are just sitting there for half a decade, unpatched. .

CVE	Shodan appearances	Vulnerabilities Types	CVSS Score
CVE-2021-40438	6,453,785	Information Disclose	6.8 MEDIUM
CVE-2019-0211	2,128,033	Privilege Escalation	7.2 HIGH
CVE-2012-1823	450,640	Remote Code Execution	7.5 HIGH
CVE-2019-11043	223,730	Remote Code Execution	7.5 HIGH
CVE-2014-0160 (Heartbleed)	190,257	Information Disclose	5.0 MEDIUM
CVE-2015-1635	120,156	Remote Code Execution	10 CRITICAL
CVE-2020-0796 (SMBGhost)	103,734	Remote Code Execution	7.5 HIGH
CVE-2019-10149	55,435	Remote Code Execution	10 CRITICAL
CVE-2019-0708 (BlueKeep)	52,692	Remote Code Execution	10 CRITICAL
CVE-2018-6789	51,968	Remote Code Execution	7.5 HIGH

Takeaways

- Many of the top exploited vulnerabilities are in Cisco devices (25 KEVs) and Pulse Secure devices (8 KEVs), often left unpatched due to the disruption caused by patching them.
- CISA KEV's act as an actionable, defensible, urgent and concise list for every organization to prioritize. While not a comprehensive list of all exploited vulnerabilities, it should serve as a baseline starting point for prioritization and to effect immediate action.
- The mere fact that there are 15 million easily-attackable devices exposed to the Internet is startling. Imagine, then, how many devices on internal networks are equally exploitable. It is no wonder threat actors have incorporated tactics to scan for and exploit devices once inside a network, using them for data exfiltration, lateral movement, C2, hidden persistence, and credential stealing activities.
- One consideration pointed out by our own Nate Warfield is that the top four vulnerabilities in the table above would require further manual verification to determine if they are exploitable, as they are context dependent based on specific configurations or components being in place. This is a limitation of basing vulnerability analysis on Shodan searches which use the vuln:CVE-YYYY-NNNN query command.
- The Eclypsium platform is purpose-built for finding vulnerabilities in many of these types of IT supply chain devices that have externally-facing services.

TOOLS & EDUCATION

The NSA has Published Comprehensive Guidance Related to Cyber Supply Chain Vulnerabilities, Threat Actors, and Firmware Hardening

The NSA has recently put out detailed guidance to help DoD entities address the growing threats targeting vulnerabilities in the cyber supply chain, with specific focus on UEFI/BIOS level attacks and hardware/firmware vulnerabilities. They've posted specific guidance Spectre, Meltdown, Speculative Store Bypass, Rogue System Register Read, Lazy FP State Restore, Bounds Check Bypass Store, TLBleed, and L1TF/Foreshadow hardware vulnerabilities as well as general firmware security guidance covering threats against the UEFI/BIOS and related campaigns like LoJax, Ryzenfall, Chimera, Fallout, and Masterkey.

Of note is this section regarding Microsoft Secure Boot Bypass guidance, which covers a 2020 vulnerability that was initially patched by Microsoft and subsequently pulled back due to operational friction when applying it. The guidance implies that there still exists a trusted bootloader that ignores the Secure Boot process and breaks the trust chain in the process. Effectively, systems are still exposed whose owners have not explicitly added the SHA-256 hash below into the DBX manually on their own.

Microsoft Secure Boot Bypass | CVE-2020-0689

Microsoft plays a prominent role in the assigning of UEFI Secure Boot signatures. Most modern machines ship with a Microsoft Windows Key Exchange Key (KEK) and a Microsoft Third-Party UEFI Marketplace KEK. Sometimes signatures are issued to bootable binaries by mistake. Rather than revoke the KEK and invalidate thousands of products, Microsoft can issue a Blacklist Database (DBX) hash for a specific signed binary.

Microsoft's patch KB4524244 issues a DBX record for a bootloader with the ability to bypass UEFI Secure Boot Protections. Initial boot firmware begins the Secure Boot process. After the Boot Device Select (BDS) phase of UEFI boot, execution control and responsibility for Secure Boot enforcement transfers to the software environment -- specifically the bootloader. The bootloader identified by Microsoft's DBX update is known to ignore Secure Boot and break a chain of trust that should extend to Microsoft's kernel. However, some endpoints have had difficulty applying the DBX update record which has caused Microsoft to pull back KB4524244.

To mitigate the threat of the dangerous bootloader, add the following SHA-256 hash to each system's DBX records if it is not already present:

> 81d8fb4c9e2e7a8225656b4b8273b7cba4b03ef2e9eb20e0a0291624eca1ba86

Future Microsoft software patches and system vendor firmware patches may also add the hash to the DBX. NSA is working to identify the ideal contents of DBX and share information to help partners maintain and customize UEFI Secure Boot. See UEFI Secure Boot Customization.

Takeaways

- The NSA guidance is comprehensive and even vendor-specific, covering everything from how to customize UEFI to addressing hardware vulnerabilities down to the affected vendor. Taken as a whole, the body of guidance is indicative of just how much emphasis NSA and DOD are placing on IT supply chain threats and vulnerabilities.
- The bootloader in the example above calls to light the fundamental challenges of trust during boot time. Authority is handed off to a 'trusted' boot manager, yet the word trust here is no one tied to a holistic cryptosystem. It is merely a 'nod' of trust that a 3rd party's provenance, at one point in time, was sufficient enough for both the

Secure Boot process itself, and Microsoft operating system relying upon it, to trust that its binary integrity is intact. Trust, here, speaks nothing to vulnerabilities, let alone malicious bootmanagers that purposely ignore the secure boot process by design. The chain of trust, in other words, is not cryptographically protected. “Trust” here is the equivalent of someone saying “I trust this car to be reliable because it is made by a manufacturer that I think is probably trustworthy”. And then when you start the car for the first time, the engine blows up.

- The trust problem at this level isn’t confined to only this example. Even two of the three vulnerable bootloaders discovered by our researchers and demonstrated at DefCon 30 in the One Bootloader to Load Them All talk, were incorrectly revoked by Microsoft, and still remain in play nearly a year after their discovery, allowing any attacker to leverage them for UEFI level access. These types of attacks are easily scriptable and adapted into any malware campaign that wants to use them.
- The Eclypsium platform derives much of its unique capabilities from the tradecraft and decades long expertise of its researchers and founders. Many of the threats, vulnerabilities and tactics discussed in this new NSA guidance have long-since been incorporated into our technology’s advanced analysis engine.