Who's in your firmware? And why should you care?

ROGER THOMPSON – TCSL RESEARCH LLC

PLATFORM SECURITY SUMMIT 2019

OCTOBER 1, 2019 – OCTOBER 3, 2019

Topics

- The problem
- Quick explanation of modern boot process (secure boot)
- Quick explanation of UEFI
- What we’ve found so far
- How we get left of bang

The problem

- There are of the order of a million new and unique bits of malware each day
- Nearly everyone is focused on that.
- Sometimes our opponents are simple, albeit cunning, criminals.
- Sometimes our opponents are nation states.
- We are at war, and people don’t know
- Think Stuxnet
- Remember that the Pres has suggested that there might be a cyber strike against Iran.
- We are in a constant race to get lower in the machine.

The problem in a little more detail

- Firmware is still just software
- All software has a weak underbelly if you probe hard enough
- For example, Black Hat Europe 2017, researchers showed how to connect to a powered off machine, through the IME,and make it do things
  - Intel said, "Yes. All manufacturers have to patch their firmware, and everyone has to flash"
- Manufacturers have no way to tell people they need to re-flash
- Most of the world has no idea how to re-flash their firmware, so they don't
- Then Spectre and Meltdown were announced, and everyone forgot about IME
- The attack surface only grows

Modern boot process

- It used to be BIOS to MBR to operating system
  - BIOS is hand-written assembler
- Now it's BIOS to IME (generally) to UEFI to operating system
  - BIOS is still hand-written assembler
  - IME is a separate computer that controls the rest of the boot process.
  - IME runs MINIX
  - UEFI is 300 to 400 compiled C programs, in Windows format
  - UEFI is a complete OS in its own right, and runs below the OS, and has complete control over the OS
- It is actually pretty secure, but it can be updated by the Good Guys (and if they can… guess what?"

UEFI

- UEFI – Unified Extensible Firmware Interface
- It looks like old PCDOS
- Think 64-bit, real mode DOS
- If you boot into an EFI shell, you find familiar commands like mkdir, edit, cd…
- It's got its own network stack
- It's a whole operating system underneath the operating system
- This makes it super-powerful if it can be abused.

Modern firmware is secure, but ...

- It is still just software, and all software has a weak underbelly, if you probe hard enough.
- For example, the UEFI programs are cryptographically signed, but we have found that typically 50-60% of the certificates in any given firmware blob are expired, or marked something like “Test certificate – do not trust”
- It turns out that this is only checked at flash time. After that, nothing checks.
- What this means is that if something can get write access to the firmware, some programs could be infected, virus-like, by re-vectoring entry points.
- Couldn’t happen, right?

Nothing could get write access, right?

- It already has
- RWEverything was a legit, signed program, used in the Lojax attack, reported by ESET in September 2018
- RWEverything is now reported as potential malware, I think, but still …

Factory planted malware

- In 2015, Lenovo got pinged for sending out what was regarded as a rootkit in their firmware. It was clearly meant to be an updater, and meant to be a positive thing.
- They said, "Oops. Sorry. We bought it from a third party, and assumed it was ok."
- They re-issued the firmware, and told people to re-flash their computers
- That means it should have been extinct since about 2016
- About every two weeks, we get a fresh upload that still contains the rootkit

Lenovo rootkit/updater

- Interestingly, it was signed by Symantec, and …. Lenovo Bejing
- On VirusTotal, only one scanner out of sixty recognizes it today, four years on.
- That's Endgame
- Interestingly, we have found five other variants of it, so far.
- No one recognizes them, other than us.
- As far as we know, it was never used maliciously, but still …
- It was only noticed because it was noisy
- Seems to have screenshot and privilege escalation capability

Asus rootkit/updater

- Noticed because a system accessed the internet before an OS was installed
- Again, not meant to be malicious, but was abused in the Shadow Hammer attack reported by Kaspersky in about March 2019
- Functionally very similar to Lenovo
- We’ve found twelve variants so far
- Nothing on VirusTotal recognize any of them last time I checked.

Computrace/Lojack

- Meant to be a security product
- Functionally very similar to Lenovo and Asus rootkits/updaters
- Modified version used in Lojax attack
- We’ve found about 50 variants so far
- Nothing on VT recognizes them
- In 2014, Kaspersky showed this could be compromised.
- No one knows if this hole has been plugged.

Other bits to watch for

- One manufacturer has software that has email capability
- Another one has a module that has email capability, and update capability.

What other firmware rootkits exist?

- We don’t know, but it’s highly likely there are more.
- Hacking Team rootkit seems to exist, although we haven’t got a copy yet.
- Energetic Bear seems to play in this space, having attacked the German energy sector a year or two ago

What other problems exist?

- Typically, if we upload a firmware blob to VIrusTotal, out of 400 exes, there will be fifteen to twenty that get detected by one or another antivirus, and five or six that get detected by more than one
- Probably, most of these are false positives, but the ones with multiple detections are worth a closer look.
- What about backdoors in IoT devices?
- What about backdoors in critical infrastructure devices?
- We want to get Left Of Bang

Bang

- This reminds me of the very early av days
- No one cared, until they got a virus
- Viruses are kid stuff compared to this
- Bang here could be power stations, nuclear stations, water systems, financial systems… etc

How do we get left of bang?

- The first hard bit is gathering the firmware image
  - You either have to
    - (1) Turn off secure boot
    - (2) Boot into an EFI shell from a thumb drive
    - (3) Dump the firmware using something like Chipsec
    - (4) Turn secure boot back on
  - Or we have a signed driver that can run from Windows on Win 10x64 or Win 7x64 (so does Kaspersky)

Getting left of bang

- Next hard bit is analyze the firmware
- There are a bunch of open source tools
- We have a program called RomAnalyzer

Getting left of bang

- If I could wave a magic wand, I’d have someone in each organization collect all their firmware, and start analyzing it
- The nice thing about having collected it, is that you can easily re-analyze it, when you learn new things.

Let’s get Left Of Bang

- https://armor.ai
- Roger Thompson
- roger@armor.ai
- roger@ThompsonCyberSecurityLabs.com