A Look Into Hard Drive Firmware Hacking

Khai Van

November 5, 2015

3rd International Cryptographic Module Conference

Gossamer Laboratories

Topics

- Background
- How to replace the firmware
- Risks/Hurdles
- Questions

Background

- **Malware:**
  - **Malicious Software**
  - **Used to gain unsolicited access to computers**
- **Many forms:**
  - **Trojan Horses**
  - **Viruses**
  - **Bots**
  - **Adware**
  - **Worms**

Background

- Overwriting hard drive firmware with a custom one allows unwanted software to execute
- Why care about overwriting firmware?
  - Attackers gain backdoor access to all data
  - One of the Equation Group's malware creates a virtual file system that hides data the malware has saved off, allowing the data to survive "military grade hard drive wiping"
  - Hard drive encryption can be bypassed

Background (EquationGroup)

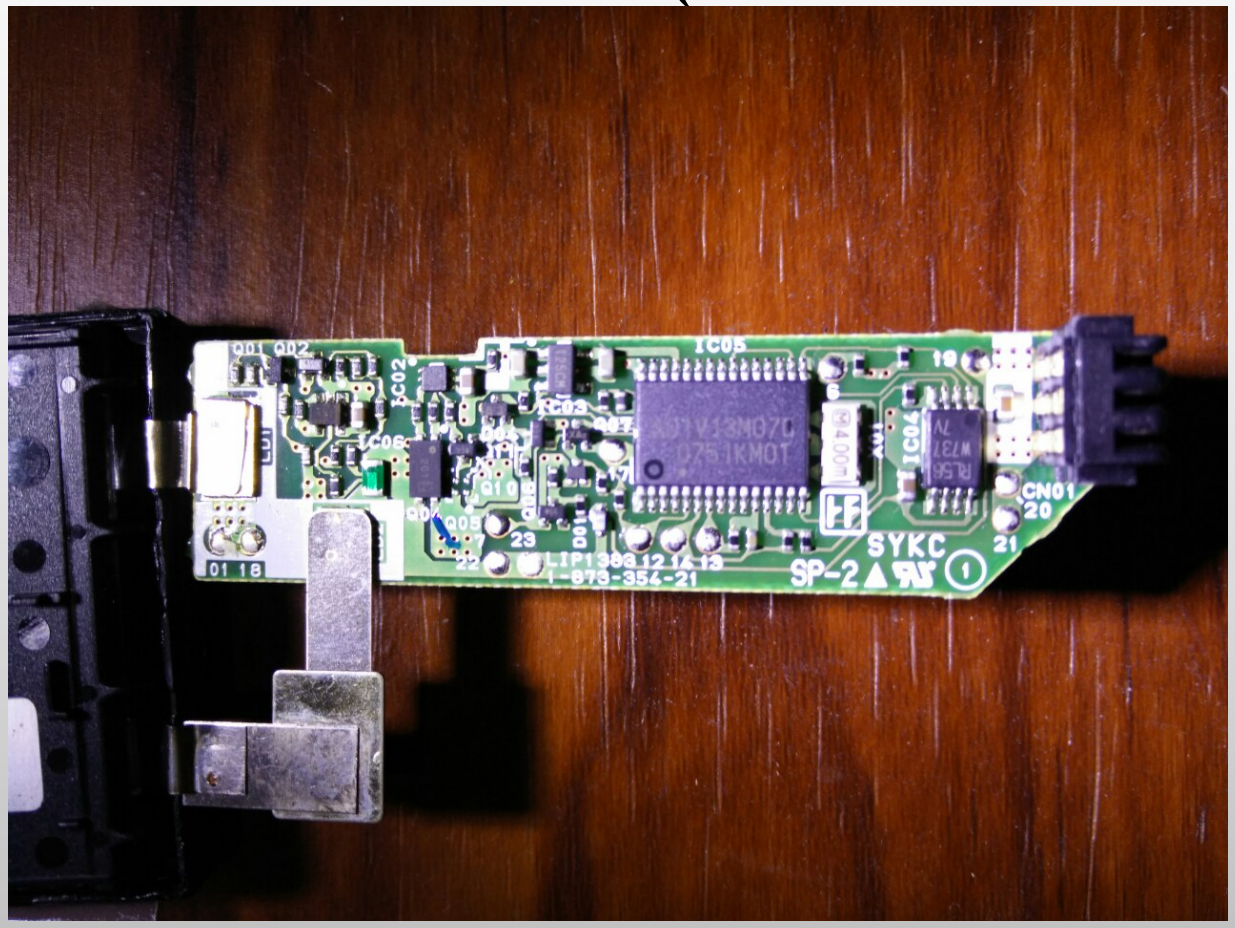
- Unearthed by Kaspersky Labs
- Named "Equation Group"
  - Named because of the malware's cryptography
- More than a decade in existence (at least 14 years)
- Many countries affected
  - India
  - China
  - Russia
  - Egypt
  - Mexico

Background

- **Which hard drives affected?**
  - All major brands
    - E.g. Samsung, Western Digital, Seagate, Maxtor, Toshiba and Hitachi
- Of the drives researched, it seems the only ones that were tested are HDDs with physical plates
- At this time, it seems PCB layout in SSDs are still being researched

Hack It Up!

- Physical access = All Access Ticket (unless device is encrypted)
- PSP-2000



Hack It Up! (PCB Layout)

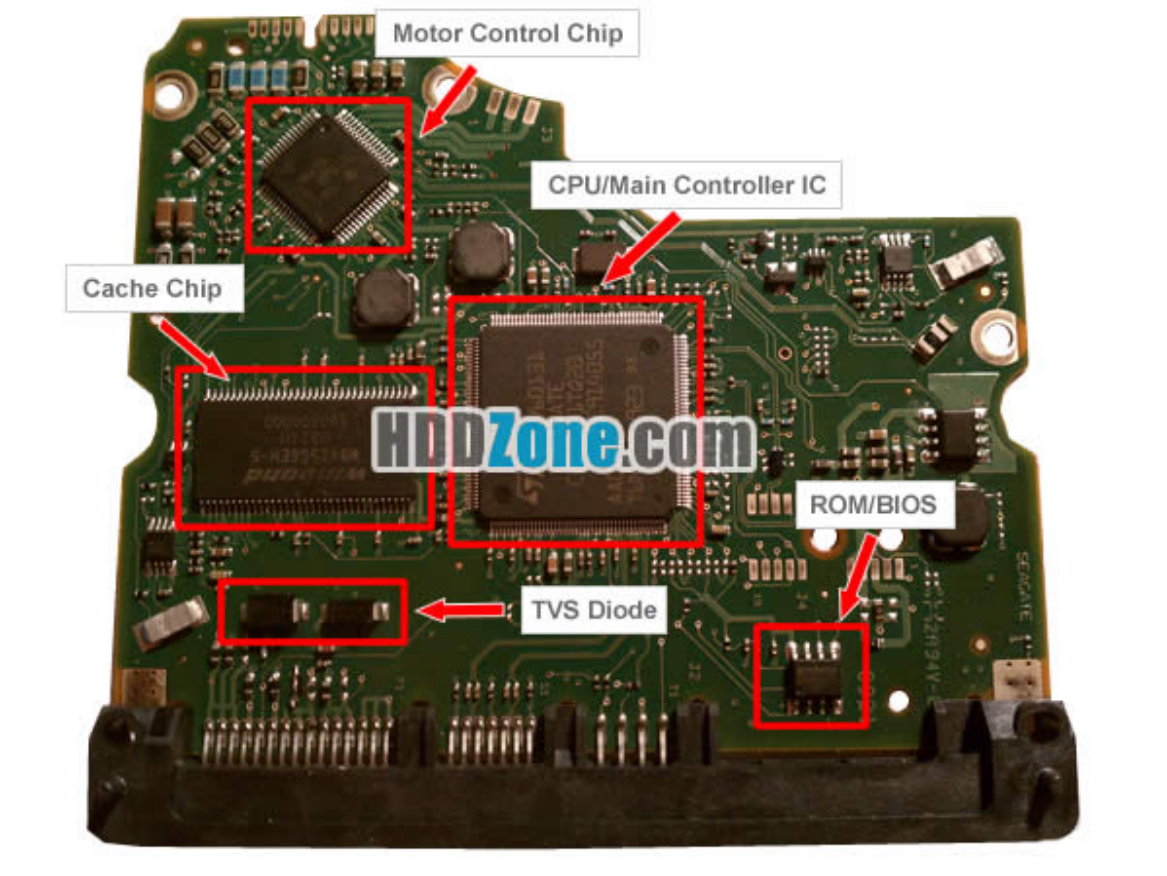
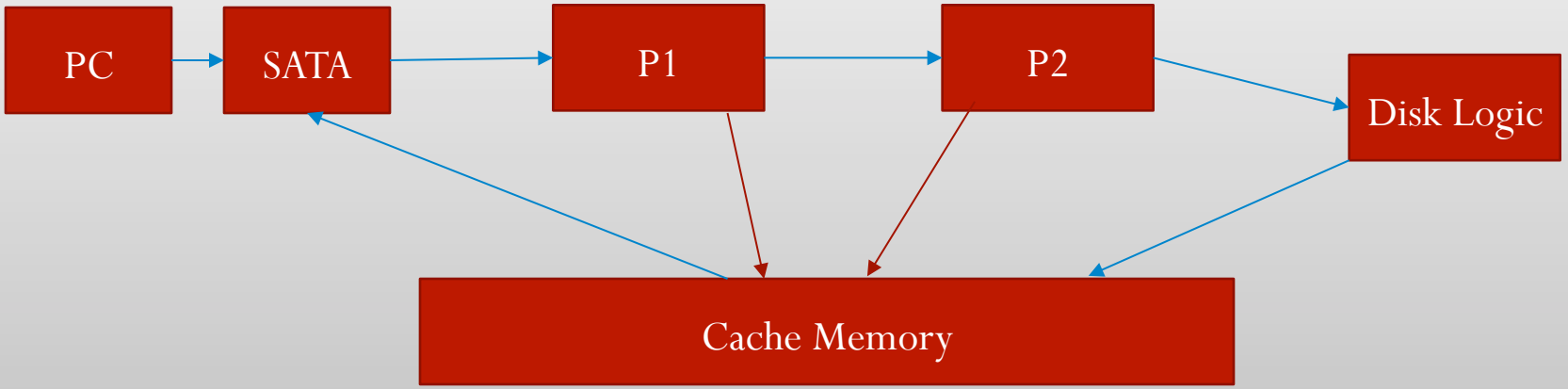


Photo courtesy of HDDZone.com

Hack It Up! (Accessing Cache)

- Jeroen Domburg
  - Creator of SpritesMods.com
- Domburg's Demo Quick Rundown:
  - Accessing data via JTAG inteface
  - Two processors -



Hack It Up! (JTAG)

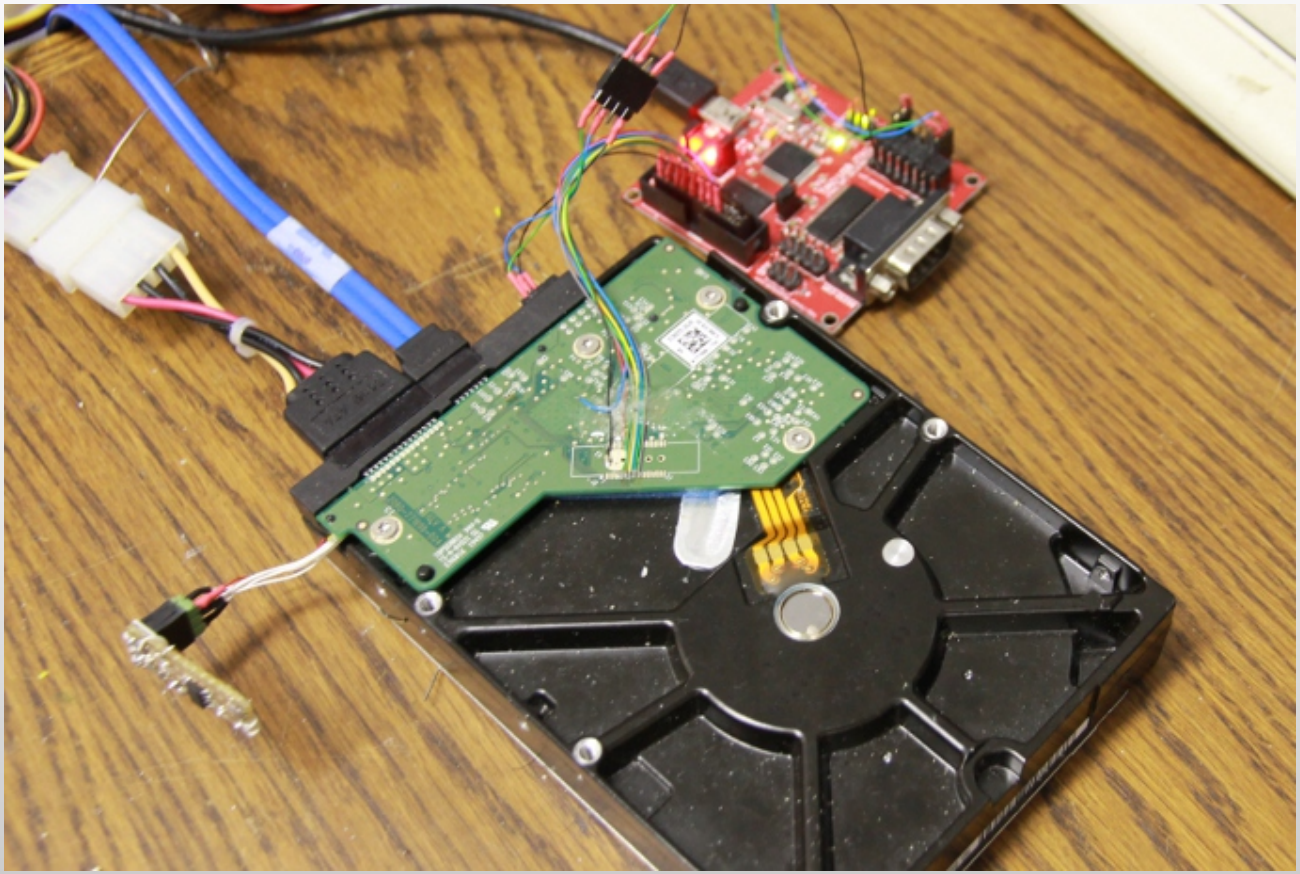


Photo courtesy of Jeroen Domburg (spritesmods.com)

Hack It Up! (Dumping data)

- Using an On-Chip Debugger (OpenOCD), one is able to dump data and commands from the JTAG interface
  - Processors have read/write access to the cache memory
  - Data in cache memory can be read/modified
  - Can run injected programs in memory
  - Flash can be dumped/replaced
  - Malicious programs can be written to flash memory to remain persistent
    - How is this done without hardware modifications?

Hack It Up! (VSCs)

- Firmware Updates
- VSC – Vendor Specific Commands
- Each manufacturer (Samsung, Maxtor, Hitachi, etc.) has a set of commands used to communicate with the hard drive controller
  - These are proprietary, closed-source
- Question: Given enough time and resources, can these commands can be recovered by reviewing disassembled flash images from the JTAG interface?

Hack It Up!

- MalwareTech blog states the following allows a hacker to infect the hard drive's firmware:
  - Create a portable SPI (Serial Peripheral Interface) programmer that can flash the firmware by being pressed against the test points on the bottom of the hard drive (would only take about 5 seconds)
  - Sending firmware update commands over the SATA interface from the host computer (requires root/admin)

Hack It Up!

- Using a portable SPI programmer requires physical access
- Firmware updates are more practical
  - “updates” sent out to numerous harddrives
  - Can be done remotely

- Hurdles of firmware updates?
  - VSCs need to be used
  - Each hard drive model is different

Consumer Risks?

- Undetectable by traditional antivirus software
- Hack is persistent
- Not a big threat (yet)
  - Each firmware replacement is vendor specific
  - High cost of infection on each harddrive
    - Reverse engineering VSCs require a lot of time and effort
  - Complex
- Specific hard drives targeted
  - Kaspersky hints toward disjoint systems (or systems connected to a closed network)

References

- Jeroen Domburg's OHM2013 Presentation on hard drive hacking - http://spritesmods.com/?art=hddhack
- http://www.malwaretech.com/2015/04/hard-disk-firmware-hacking-part-1.html
- Equation Group - http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/
- More Equation Group – https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/
- https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf
- http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage
- http://www.reuters.com/article/2015/02/17/us-usa-cyberspying-idUSKBN0LK1QV20150217

Questions? Comments?

Contacts:

- Khai Van
  - KhaiVan@gossamersec.com

www.gossamersec.com
www.facebook.com/gossamersec
@gossamersec