The Equation Group And GrayFish

How I learned to stop worrying and love the NSA

What Is The Equation Group

- Highly sophisticated threat actor
- Operating since 2001
- Only targets specific victims
- Multiple malware platforms
- Amount of technical expertise and resources suggest a nation-state backer
- “The Equation Group is probably one of the most sophisticated cyber attack groups in the world; and they are the most advanced threat actor we have seen”
  - Kaspersky Lab

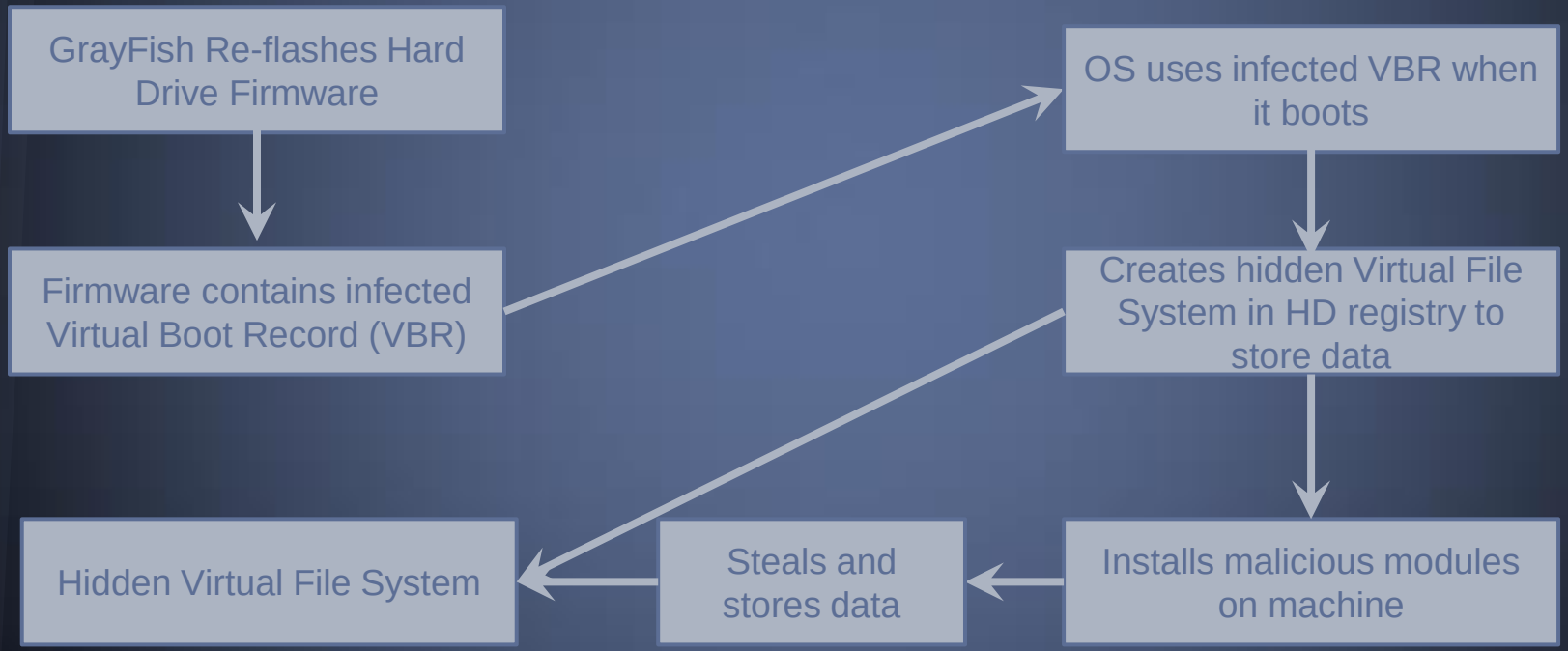
Tools And Malware

- Fanny
  - maps air-gapped systems using USBs
- Double Fantasy, Triple Fantasy
  - used to verify targets
- EquationDrug, GrayFish
  - attack platforms used to steal information from the victims
- Physical interception of packages
- Command & Control servers
  - issue commands to malware, and collect stolen data

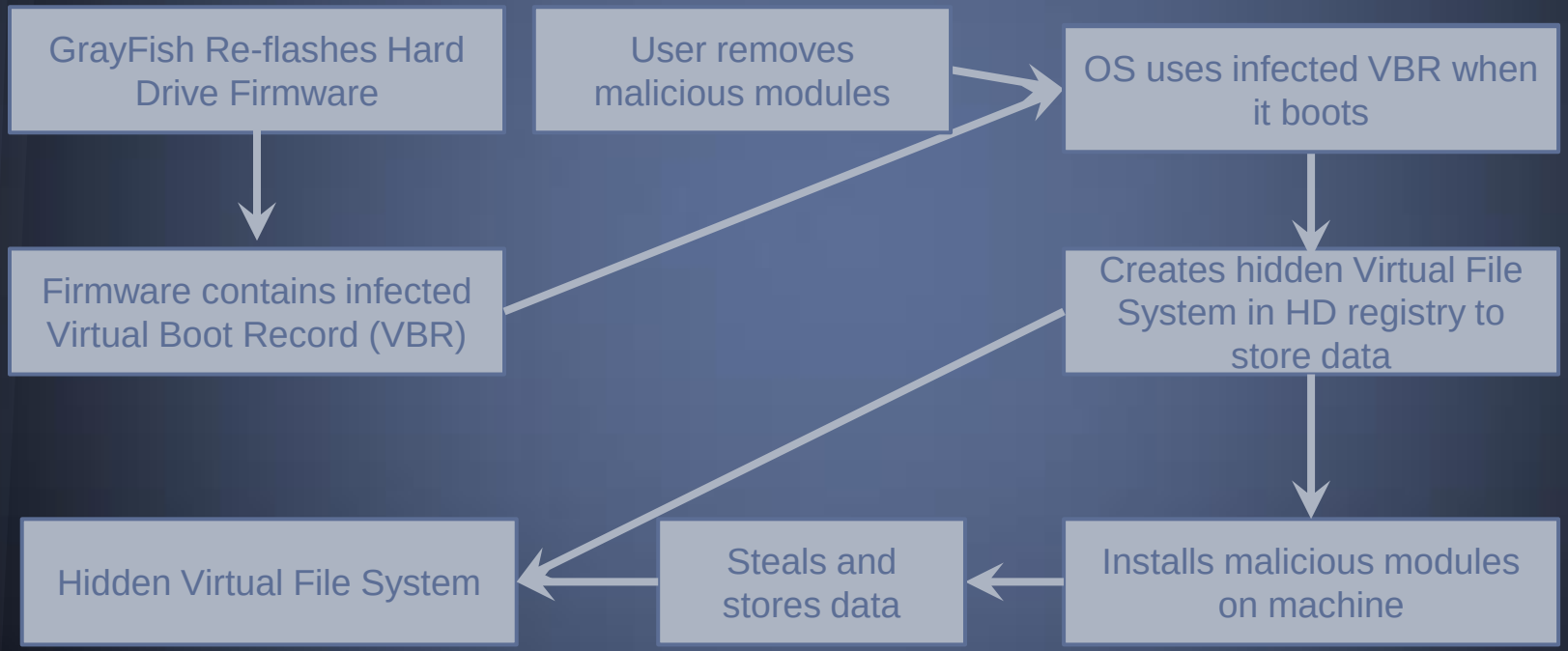
Grayfish Basics

- What is Grayfish?
  - flashes the firmware of HDs, and steals data
- How it works:
  - Grayfish inserts a ‘pill’ into the firmware, hijacking the boot sequence of the operating system and gaining complete control of the system to install a Virtual File System in the registry of the hard drive.
  - Afterwards, malware is installed in the Virtual File System, which steals information from the system and stores it in hidden areas.

GrayFish Basics



GrayFish Persistence



Grayfish: why such a big deal?

- First instance of HD firmware hacking in the wild, extremely persistence
  - Reinstalling operating system or updating the HD firmware does nothing
  - Only possible way to get rid of it is to get a new hard drive.
- Nearly impossible for common criminal to replicate.
  - Need proprietary information of individual hard drive designs to construct malware
- Only way the equation group got a hold of so many major designs is if they stole them, or pressured the companies to hand them over.

Threat Models and Attack Vectors

- Two Threat models: Air Gapped and non Air Gapped
- Attack Vectors for non Air Gapped computer:
  - Cookie spoofing, spearphishing, csrf, xss and other
- Attack Vectors for Air Gapped Targets
  - Physically intercepting machines
  - USB infection
    - I.e. stuxnet hack, fanny

Attack Vector - Non Air Gapped

Victim

Infected With Web Based Attacks

Infected With Double Fantasy

Infected With Grayfish

Double Fantasy (Validator)

Interesting Victim! (personal data)

Infects With GrayFish

Sends data

Equation Group

Server

Attack Vector - Air Gapped

Victim

Infected with GrayFish

amazon.com Prime

UNITED STATES POSTAL SERVICE

Equation Group

Attack Vector - Air Gapped

Infected with GrayFish

Server

Equation Group

Stuxnet or
Fanny USB
Hack

Attack Vector - Air Gapped

Infected with GrayFish

All Files Encrypted

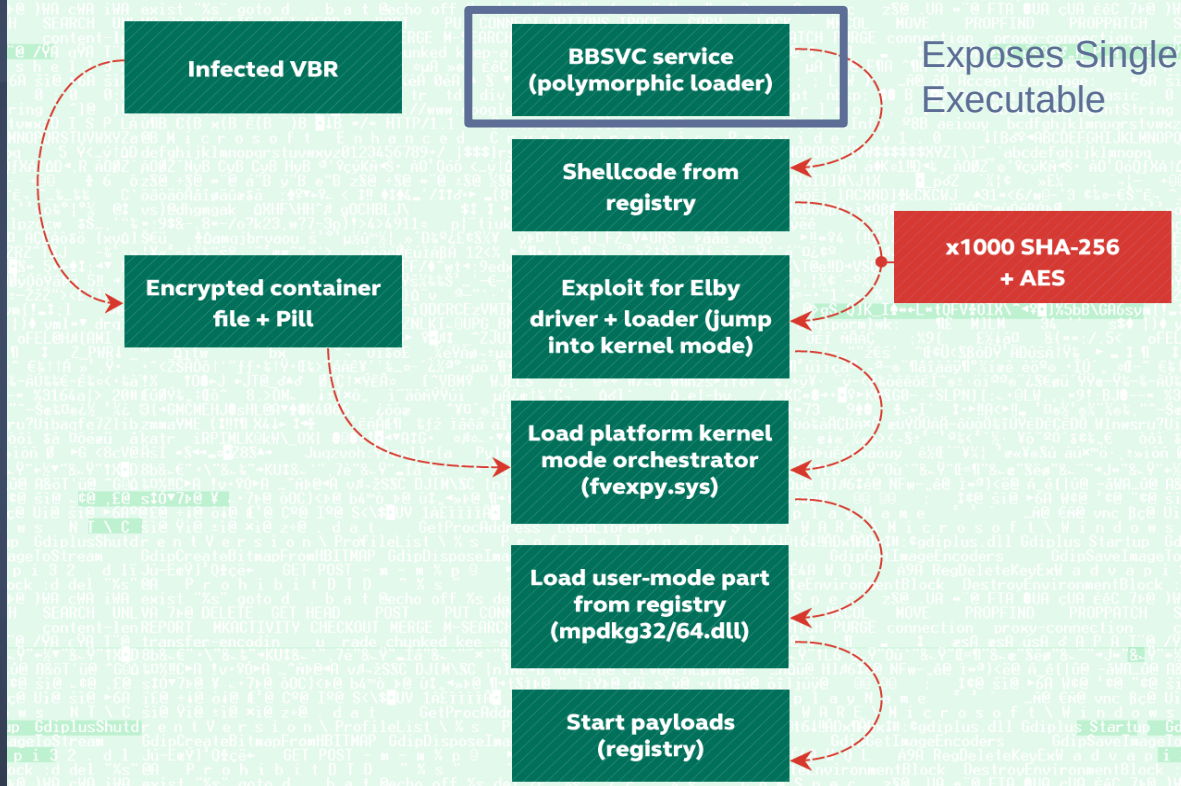
Will be able to read all files or keys hidden by GrayFish

Equation Group

How To Detect Grayfish?

- Very difficult
  - all malware hidden in service area of the HD
- If there is some issue in rebooting the Operating System, the backup plan for Grayfish kicks in.

GrayFish architecture



Exposes Single Executable

GREAT KASPERSKY lab

Prevention In the Future

- Simple way to prevent firmware from being hacked
  - Manufactures sign firmware
- If anyone attempts to tamper with the firmware, the verification will fail.
  - Problem is firmware was not designed with security in mind

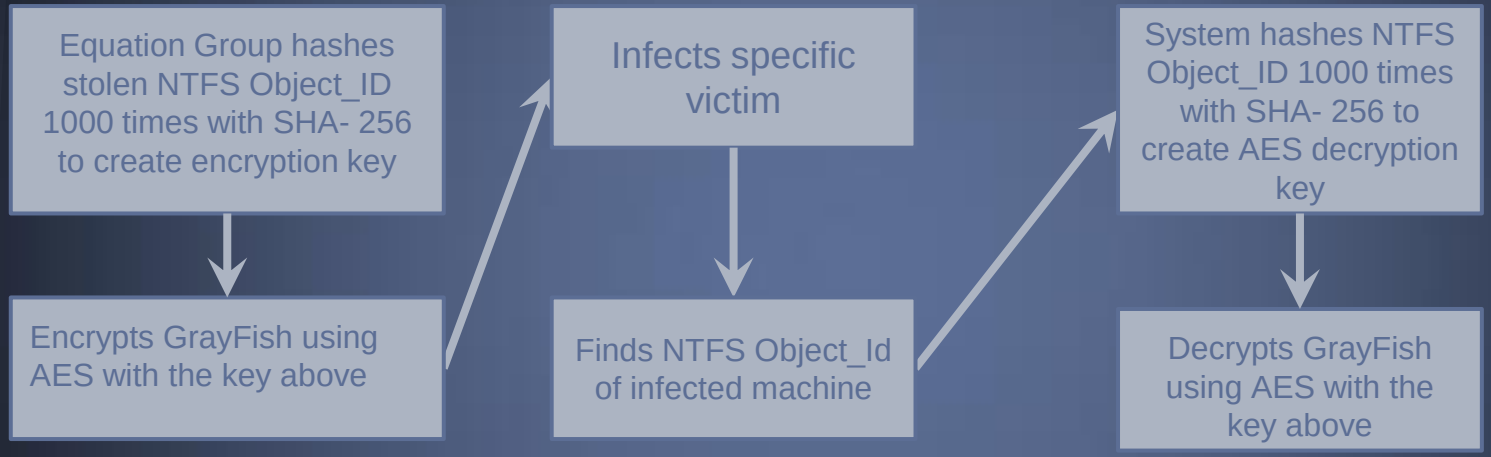
Source Code

- Almost no information available
- High Level of encryption
- Tied malicious payload to specific machines
- Easy to trigger self-destruct
  - If both boots fail, will remove itself from the system

Victim Specific Attack

- NTFS Object_Id is a id corresponding to a specific folder, that allows referencing without knowing the path.
  - System Folder Object_Id acts as a unique identifier for the system

Victim Specific Attack



How Did Kaspersky Find Grayfish?

- The set up a server in the Middle East that does everything possible to look like a target
- Called the Magnet of Threats
- While looking for a similar type of malware called Regin, Kaspersky found several different kinds of Equation Group malware
- Sinkholed Equation Group C&C servers
  - unite3tubes[.]com

Who Is The Equation Group?

- Highly sophisticated malware packages
- Target specific groups/individuals
- Indicates the backing of a Nation-State
- SO WHO COULD IT BE???
- The NSA

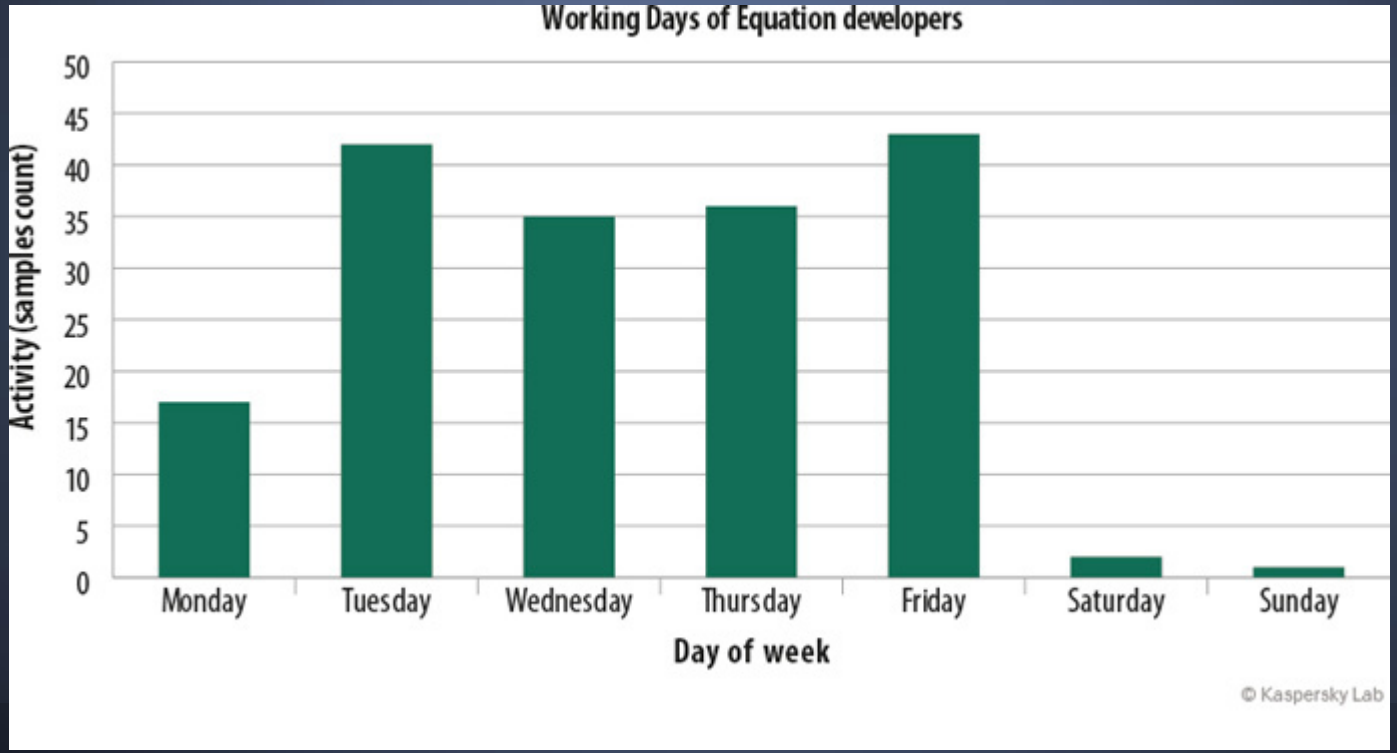
NSA: The Evidence

- Hours worked by the hackers are nearly exactly compatible with government employee work hours.
- Majority of targets are in Middle Eastern Countries, Russia, and China
- Code artifacts from the malware show several different names of operations(STRAITACID, STRAITSHOOTER, DRINKPARSLEY, BARKSNARF, etc) and a single line username “rmgree5”)
- Most important evidence is...

Documents from Snowden Files

- Product page from ANT product catalog for NSA mentions a program called IRATEMONK which “provides software application persistence on...computers by implanting hard drive firmware to gain access by MBR substitution”
- This description matches the functionality of Grayfish

Working days of Equation Devs



Equation group victims map

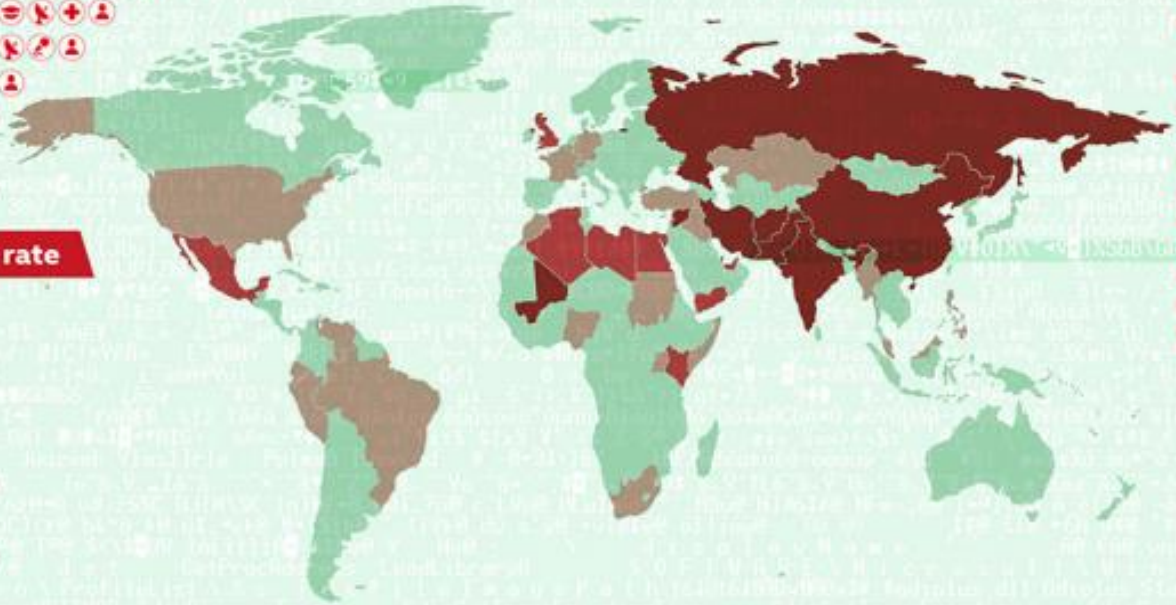
- Finance
- Government
- Diplomatic / Embassies
- Research institution
- Energy / Infrastructure
- University
- Military
- Aerospace
- Telecommunications
- Medical
- Islamic Scholars
- Media
- Other / Unknown

High infection rate

- Iran
- Russian Federation
- Pakistan
- Afghanistan
- India
- China
- Syria
- Mali

Medium-level infection rate

- Lebanon
- Yemen
- United Arab Emirates
- Algeria
- Kenya
- United Kingdom
- Libya
- Mexico
- Qatar
- Egypt



Low infection rate

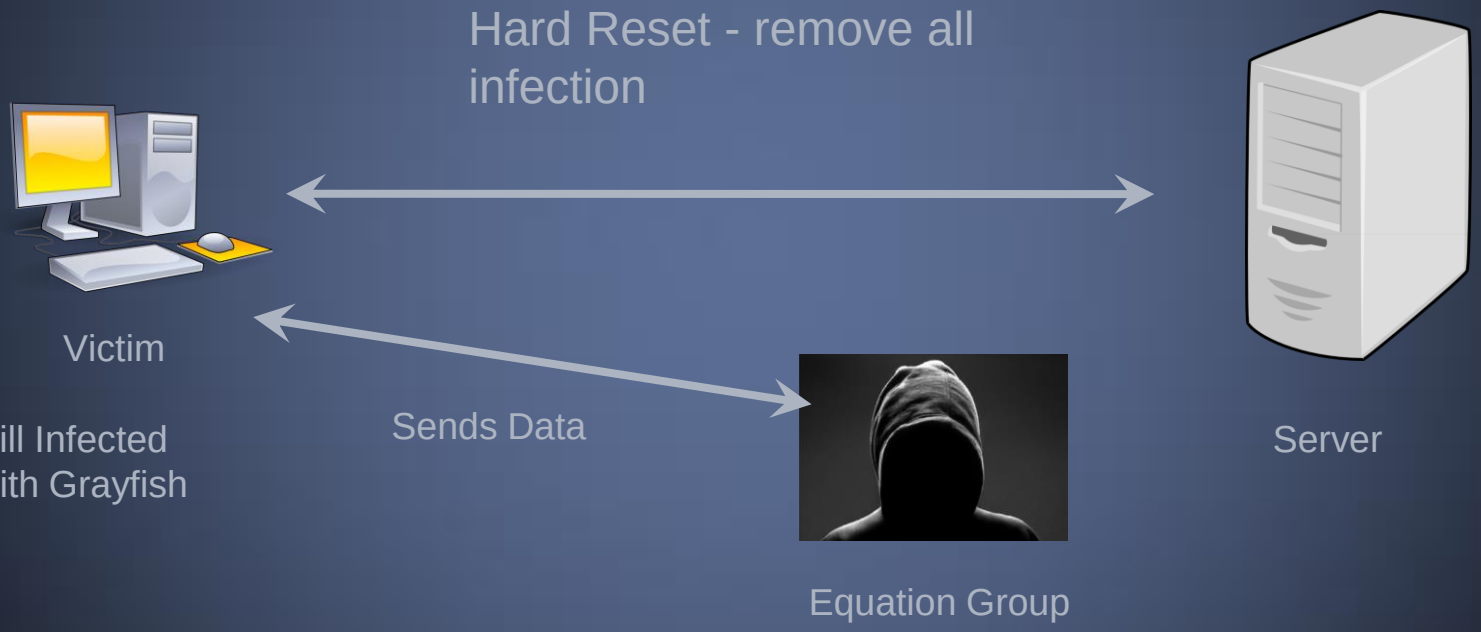
- Turkey
- Somalia
- Myanmar
- Germany
- South Africa
- Nigeria
- United States
- Venezuela
- Sudan
- Palestinian
- Morocco
- Malaysia
- Kazakhstan
- Iraq
- Brazil
- Uganda
- Switzerland
- Singapore
- Philippines
- Peru
- France
- Equador
- Belgium
- Bahrain

GREAT KASPERSKY

Sources

- https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf
- http://rt.com/usa/239933-equation-group-nsa-links-backsnarf/
- http://www.wired.com/2015/02/nsa-firmware-hacking/
- https://www.schneier.com/blog/archives/2015/02/the_equation_gr.html
- http://www.theregister.co.uk/2015/02/17/kaspersky_labs_equation_group/
- http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/3/
- http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage
- http://www.wired.com/2015/02/kapersky-discovers-equation-group/
- https://leaksource.files.wordpress.com/2013/12/nsa-ant-iratemonk.jpg

Attack Vector - Non Air Gapped



How Did Kaspersky Find Grayfish?

- Noticed that several Command & Control addresses hadn't been renewed
- Kaspersky bought domain names of several C&C servers
- Created sinkholes so that any EG malware still using compromised C&C servers could be traced
- Example C&C servers
  - newjunk4u[.]com
  - phoneysoap[.]com
  - dowelsobject[.]com
  - unite3tubes[.]com