The Hacks

THAT MADE US

WHOAMI

I am Alan Cook aka @cipherthink

- Sr. AppSec Engineer at a financial institution
- Focused on offensive security
- Background in Product Security, Sec. Engineering, Governance, etc.
- Experience across Financial Services, Healthcare, and Gaming verticals
- Interested in history, music, sports, and sailing

“There’s a war out there, old friend. A world war. And it’s not about who’s got the most bullets. It’s about who controls the information. What we see and hear, how we work, what we think ... It’s all about the information!”

—COSMO (SNEAKERS 1992)

RUNBOOK

- Introduction: structure, organization, and scope
- The Hacks!
- Q&A

THE HACKS

01

THE HACKS

Known technical details about the hacks

02

CONTROLS

Security controls that could have prevented the hacks and/or have been implemented since

THEIR EFFECTS UPON US

POLITICAL

Governmental/Regulatory effects and policies resulting from hack

ECONOMIC

Micro/Macro economic effects resulting from hack

SOCIAL

Cultural effects resulting from hack

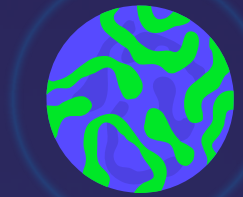
01

OPERATION GET RICH OR DIE TRYIN’

The Great Cyberheist

THE HACK

- Series of hacks in mid-2000s targeting credit card data
- Green Hat Enterprises crew led by Albert Gonzalez
- Gonzalez was a Secret Service informant for Operation Firewall



Initial Vectors

- Weak WiFi networks at retail locations
- SQL injection on web-commerce sites

Pivot!

- Initially, so much old transaction data was identified it was hard to find card data that had not expired
- So, Stephen Watt created a “sniffer” program to find good data, encrypt it, and exfiltrate it out

United States Attorney's Office District of Massachusetts

United States Attorney

PRESS RELEASE

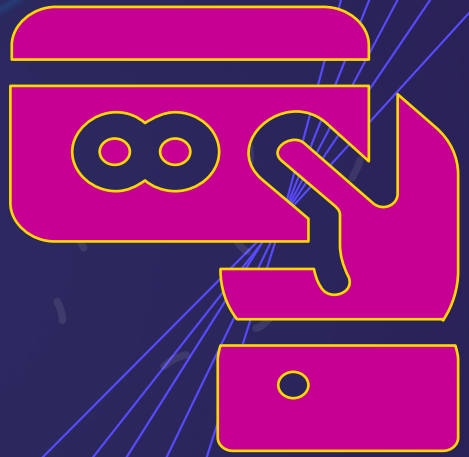
FOR IMMEDIATE RELEASE
December 23, 2009
www.usdoj.gov/usao/ma

Contact: Christina Diiorio-Sterling
Phone: (617) 748-3356
E-mail: usama.media@usdoj.gov

Hacker Sentenced For Providing Data Theft Tool in National Identity Theft Case

Jackpot

- HPS corporate network compromised via SQLi on website
- HPS identified the activity and thought all malware had been eradicated
- Attackers jumped to the payment processing network



The Take

- This led to the compromise of millions of CC#s and cardholder data
- Some cashout was done directly by crew
- Other dumps were fenced through a reseller

THE CONTROLS

Preventative:

Ensure strong encryption is used for all WiFi communication
Isolate wireless networks transmitting card data
Change default passwords/secrets on wireless network devices
Purging sensitive data when no longer needed

Detective:

Logging and Monitoring with alerting for anomalous activity

Corrective:

Use a WAF to monitor and block HTTP requests for SQLi
Implement WIDS/WIPS

THEIR EFFECTS UPON US

POLITICAL

Creation of PCI DSS Wireless Guidelines

ECONOMIC

$400MM+*

SOCIAL

None

02

WEB WAR I

Rehearsal for Cyberwar

THE HACK

- DDoS attack begins April 28, 2007
- Estonia was highly connected
- Only way to mitigate attack was to implement a denylist to deny international traffic to websites
- Estonia’s CERT works with ISPs around the world to filter out malicious traffic
- A week after DDOS starts it stops

THE HACK

- Attack consists of
  - DDoS attacks
  - Website defacement
  - DNS attacks
  - Mass email spam

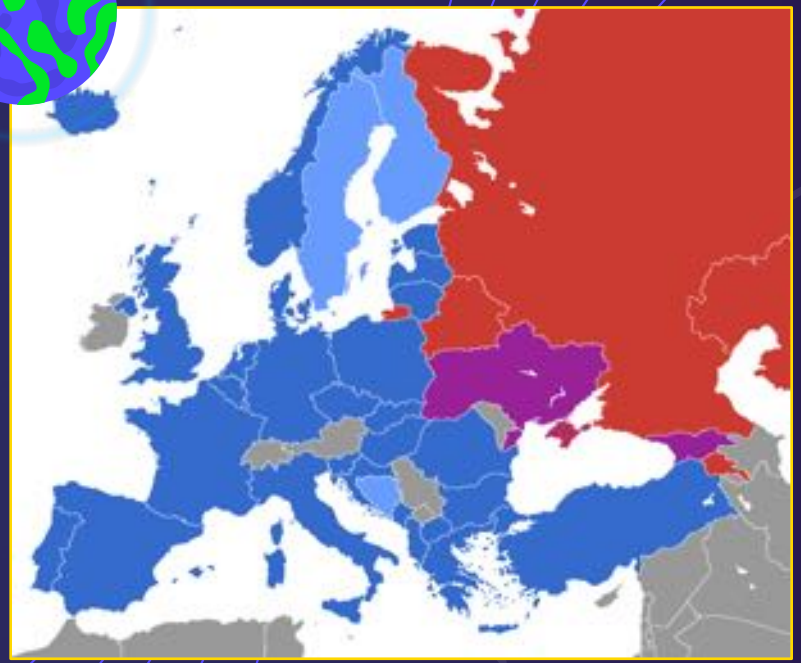
THE HACK

- Second wave of attacks begin at midnight Moscow time on May 9, the Russian Victory Day
- "Those who are trying today to... desecrate memorials to war heroes are insulting their own people, sowing discord and new distrust between states and people”

  -President Putin
- Attacks disappear by end of May

THE HACK

- NATO declines to consider an Article 5 or Article 4 response



THE CONTROLS

Preventative:

CDN w/ DDOS Protection*

Detective:

Use dashboards to monitor bandwidth utilization and alert on spikes

Corrective:

THEIR EFFECTS UPON US

POLITICAL

Attacks sped up establishment of NATO Cooperative Cyber Defence Centre of Excellence (CCD COE)

Tallinn Manual published

ECONOMIC

$750MM

SOCIAL

Better understanding of cyber attacks

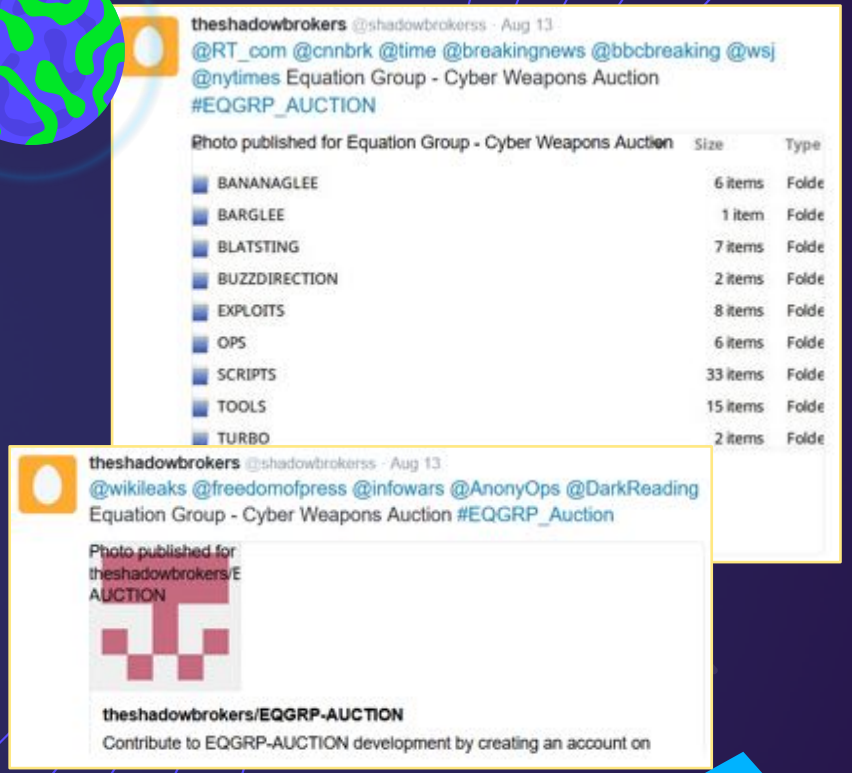
03

THE SHADOW BROKERS

Spy vs. Spy

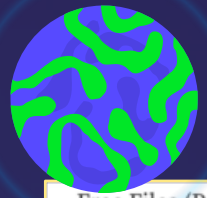
Leak Timeline

- In August 2016, the Shadow Brokers tweet claiming to have hacked the Equation Group
- Posts to GitHub/Pastebin include gpg encrypted files



Auction

- Encrypted files uploaded to GitHub include indication as to what key is used within the filename (free/auction)
- Posts publish a btc address and announce an auction for the remaining files



Free Files (Proof)

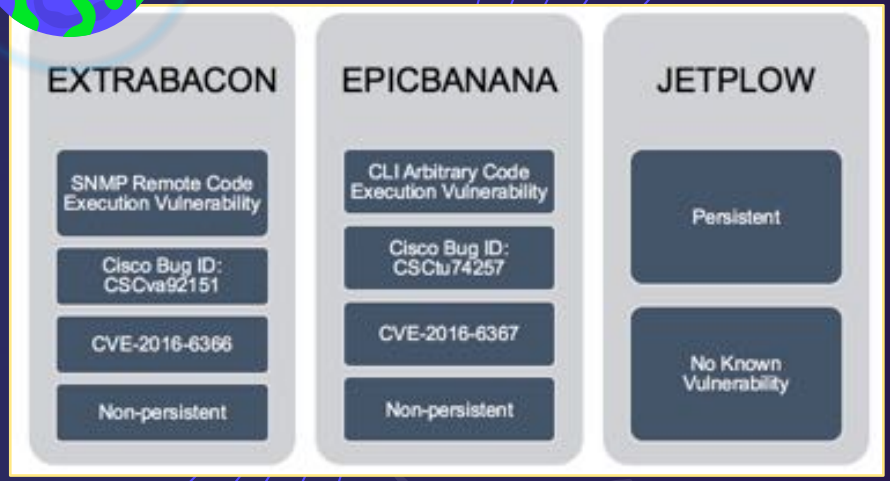
eqgrp-free-file.tar.xz.gpg
sha256sum =
b5961eee7cb3eca209b92436ed7bdd74e025bf615b90c408829156d128c7a169
gpg --decrypt --output eqgrp-free-file.tar.xz eqgrp-free-file.tar.xz.gpg
Password = theequationgroup

Auction Files

eqgrp_auction_file.tar.xz.asc
sha256sum =
af1dabd8eceec79409742cc9d9a20b9651058bbb8d2ce60a0edcfa568d91dbea
gpg --decrypt --output eqgrp-auction-file.tar.xz eqgrp-auction-file.tar.xz.gpg
Password = ????

Initial Exploits

- Free files include exploits for Cisco/Fortinet/Juniper/TopSec FWs
- Some filestamps indicate that some of the exploits file creation dates were in 2013
- Security researches confirm that some of the exploits still work



https://storage.googleapis.com/blogs-images/ciscoblogs/1/Screen-Shot-2016-08-17-at-11.32.59-AM.png

Information Op?

- Subsequent posts include laments about inability to reach btc goal
- Post about Bill Clinton/Lorreta Lynch conversation leading up to 2016 election
- October 2016, dumps list of IPs Equation Group has operated from

All Your Base are Belong to Eternal!

- In April 2017 a post titled “Don’t Forget Your Base” ostensibly offering advice for President Trump releases the key to the auction files
- Files include exploits for vulnerabilities that had been patched by Microsoft

Code Name	Solution
“EternalBlue”	Addressed by MS17-010
“EmeraldThread”	Addressed by MS10-061
“EternalChampion”	Addressed by CVE-2017-0146 & CVE-2017-0147
“ErraticGopher”	Addressed prior to the release of Windows Vista
“EsikmoRoll”	Addressed by MS14-068
“EternalRomance”	Addressed by MS17-010
“EducatedScholar”	Addressed by MS09-050
“EternalSynergy”	Addressed by MS17-010
“EclipsedWing”	Addressed by MS08-067

https://arstechnica.com/information-technology/2017/04/purported-shadow-brokers-0days-were-in-fact-killed-by-mysterious-patch/

THE CONTROLS

Preventative:

Patch Management
Disable SMB

Detective:

Anti-virus/EDR*
Logging and monitoring and alerting on anomalous activity

Corrective:

Anti-virus/EDR*

THEIR EFFECTS UPON US

POLITICAL

Exposed publicly Equation Group hacking

ECONOMIC

Unknown*

WannaCry
NotPetya

SOCIAL

WannaCry impacts NIH
NotPetya impacts Maersk

THANKS!

Do you have any questions?

@cipherthink

https://www.linkedin.com/in/davyalancook2/

https://github.com/cipherthink/TheHacksThatMadeUs

REFERENCES

1. The Great Cyberheist: https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html
2. Havard Law School Case Study – Albert Gonzalez:L Get Rich or Die Tryin': https://casestudies.law.harvard.edu/albert-gonzalez-get-rich-or-die-tryin/
3. TJX Hacker Gets 20 Years in Prison: https://www.wired.com/2010/03/tjx-sentencing/
4. USA vs. Albert Gonzalez Sentencing Memo: https://www.wired.com/images_blogs/threatlevel/2010/03/gonzalez_gov_sent_memo.pdf
5. US Attorney Press Release about Sentencing of Stephen Watt: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/wattSent.pdf
6. A Famous Data Security Breach & PCI Case Study: Four Years Later: https://www.secureworks.com/blog/general-pci-compliance-data-security-case-study-heartland
7. PCI DSS Wireless Guidelines: https://listings.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf
8. Sandworm – A New Era of CyberWar and the Hunt for the Kremlin's Most Dangerous Hackers: https://www.penguinrandomhouse.com/books/597684/sandworm-by-andy-greenberg/
9. Hackers Take Down the Most Wired Country in Europe: https://www.wired.com/2007/08/ff-estonia/

REFERENCES

10. A Critical Evaluation of the Estonian Cyber Incident: https://openaccesspub.org/article/1489/jafs-20-3601.pdf
11. Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal': https://www.forbes.com/sites/thomasbrewster/2015/02/16/nsa-equation-cyber-tool-treasure-chest/?sh=28c049f8417f
12. China Hijacked an NSA Hacking Tool in 2014—and Used It for Years: https://www.wired.com/story/china-nsa-hacking-tool-epme-hijack/#:~:text=More%20than%20four%20years%20after,hands%E2%80%94still%20haunts%20the%20security
13. The Shadow Brokers publishing the NSA vulnerabilities (2016): https://cyberlaw.ccdcoe.org/wiki/The_Shadow_Brokers_publishing_the_NSA_vulnerabilities_(2016)
14. Equation Group – Cyber Weapons Auction: https://imgur.com/gallery/sYpyn
15. Darknet Diaries: Episode 53: Shadow Brokers: https://darknetdiaries.com/transcript/53/
16. Implications of the newest Shadow Brokers offerings: http://malwarejake.blogspot.com/2017/01/implications-of-newest-shadow-brokers.html
17. Shadow Brokers: NSA Exploits of the Week: https://medium.com/comae/shadow-brokers-nsa-exploits-of-the-week-3f7e17bdc216
18. Mysterious Microsoft patch killed 0-days released by NSA-leaking Shadow Brokers: https://arstechnica.com/information-technology/2017/04/purported-shadow-brokers-0days-were-in-fact-killed-by-mysterious-patch/