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

AOHell

“Basically, it is used to annoy others, get free service, and other things. You can knock people offline with it, you can Email bomb someone with it, and many other things.”

-AOHell v3.0 ReadMe

THE HACK

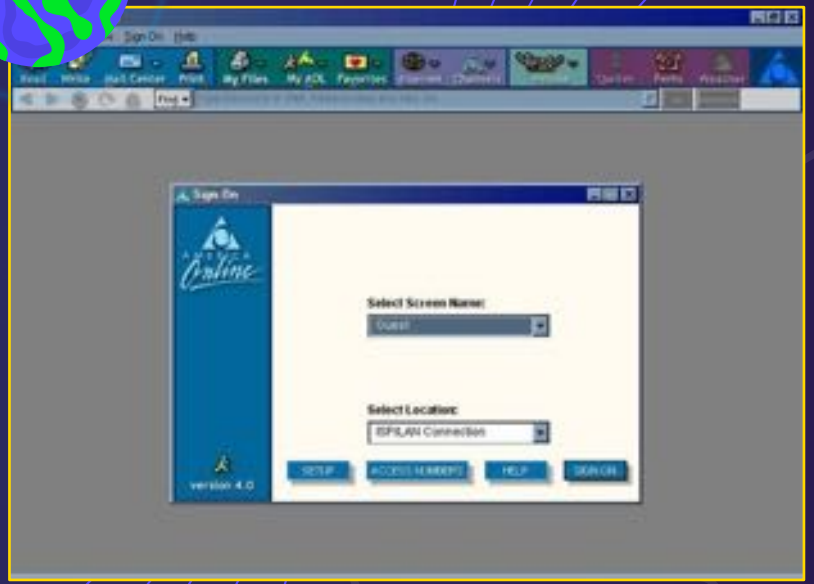
- v1 of toolset released in AOL chat rooms (1994)
- V2-3 and various betas released (1995)
- Notable Features:
  - Free AOL
  - Fake Account Creator
  - PW/CC Fisher

Free AOL

- v3 of tool added functionality to allow users to enter a free area (such as billing) which would pause accounting for use of time and then revealed the AOL ‘pay’ windows
- It enumerates all the Window Handles and send them a message to show themselves but doesn’t start accounting of time

Fake Account Creator

- Generates all needed info to sign up for a new account, including name, address, phone number, city, state, and a valid CC#, and pre-fills the form
- AOL was only validating the CC# checksum and that it was a valid credit card



PW/CC Fisher

- Provided functionality to mass IM users in a room with a pre-text such as pretending to be AOL stall and asking for PW or CC info
- Save responses in a file on disk

THE CONTROLS

Preventative:

Free AOL - Ensure time accounting starts with usage
Fake Account Creator – Verify CC#s are active and valid
PW/CC FIsher - User Education

Detective:

Free AOL - Audit/Alert on significant variation between logon time and free time

Corrective:

THEIR EFFECTS UPON US

POLITICAL

None

ECONOMIC

Unknown

SOCIAL

First phishing on a massive scale

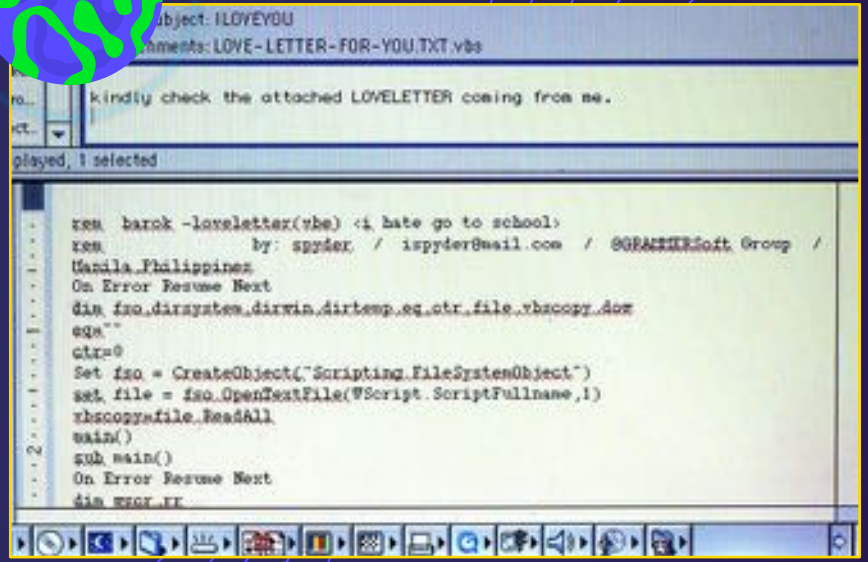
First use of term Phishing

02

ILOVEYOU

THE HACK

On May 4, 2000, a virus spread by email message with a .vbs attachment. Running the script overwrote random Office and image files and hid mp3 files and spread by copying itself and emailing all address book contacts in Outlook.



THE HACK

Caused outages due to email servers having to be taken offline.

- Ford Motor Company
- Microsoft

Police in Philippines identified computer student Onel de Guzman of Manila as the author but were unable to prosecute due to lack of laws against malicious computer use.

THE CONTROLS

Preventative:

User Education
Prevention of execution of attachments
Disabling hidden file extensions for known filetypes

Detective:

Anti-virus*

Corrective:

Anti-virus*
Backups

THEIR EFFECTS UPON US

POLITICAL

Philippine Congress enacts Republic Act No. 8792

ECONOMIC

$10B+

SOCIAL

“Windows users everywhere learned to never, ever, open unsolicited attachments”
-Kevin Poulsen

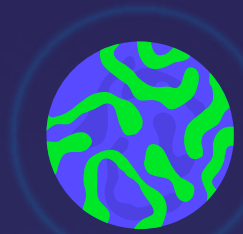
03

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

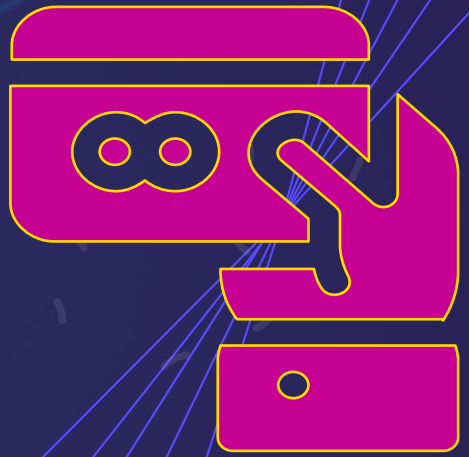
FOR IMMEDIATE RELEASE
December 23, 2009
www.usdoj.gov/usao/ma

Contact: Christina Diorio-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

04

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

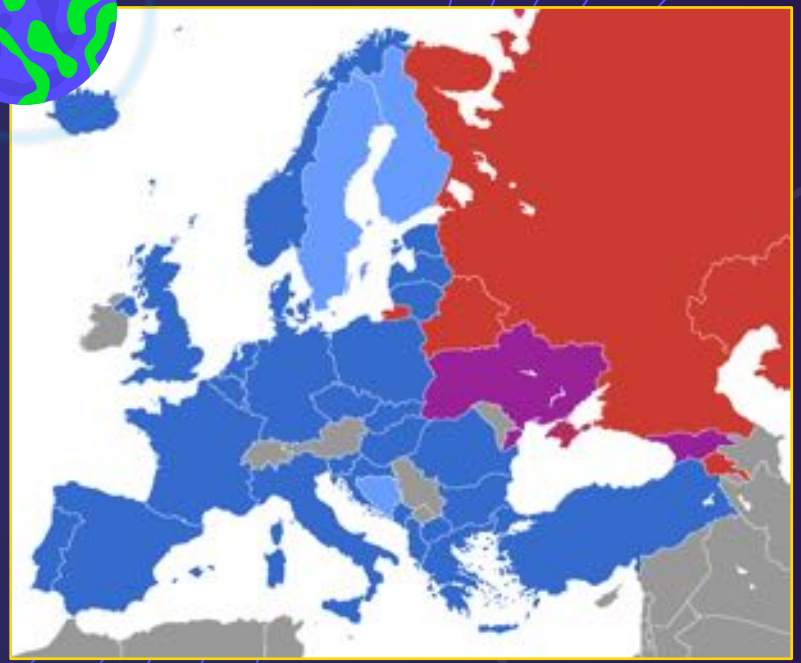
THE HACK

- 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

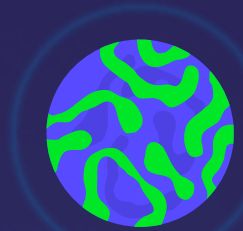
05

OPERATION AURORA

Industrial Espionage at Scale

Initial Vector

- Spear-phishing victims likely to have access to intellectual property
- Attack appears to come from a trusted source
- User opens file which exploited a 0-day in Internet Explorer

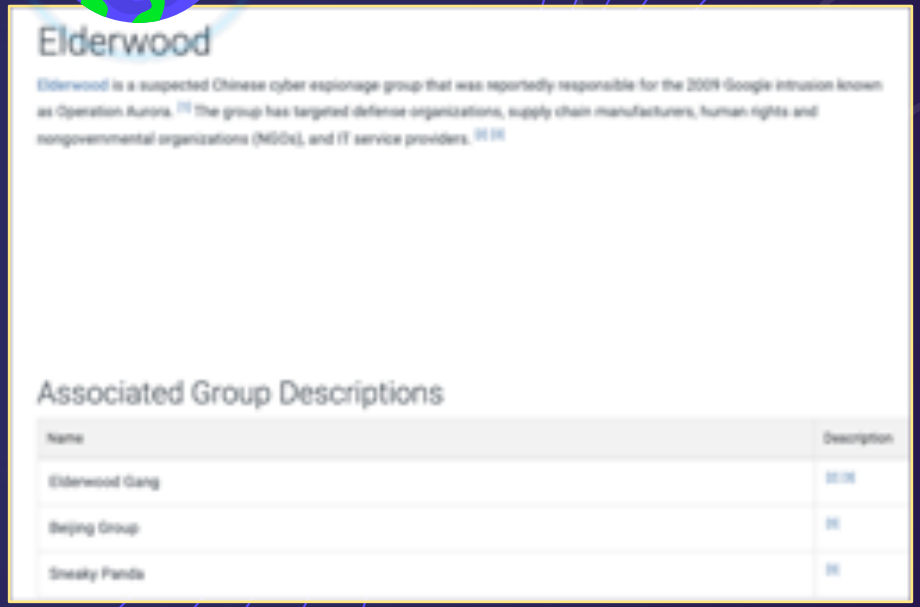


Google Attack

- Attack focused on two targets within Google
  - Email accounts of Chinese human rights activists
  - Source code for Google products
- Second zero-day used for SCM Perforce
- Contributing factor to Google “reviewing business operations in China”*

What's in a name?

- McAfee – Aurora
- Symantec – Elderwood
- CrowdStrike – Sneaky Panda
- Dell – Beijing Group



Elderwood

Elderwood is a suspected Chinese cyber espionage group that was reportedly responsible for the 2009 Google intrusion known as Operation Aurora. [1] The group has targeted defense organizations, supply chain manufacturers, human rights and nongovernmental organizations (NGOs), and IT service providers. [2] [3]

Associated Group Descriptions

Name	Description
Elderwood Gang	[2] [3]
Beijing Group	[3]
Sneaky Panda	[3]

Other Attacks

- Attackers used the same and other 0-days
- Targeted intellectual property
- Conducted watering hole attacks

THE CONTROLS

Preventative:

User Education
Run SCM software as a non-privileged user
Require authentication to create new users in SCM
Encrypt SCM data in transit

Detective:

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

Corrective:

Anti-virus*

THEIR EFFECTS UPON US

POLITICAL

Increased tensions between US and China

ECONOMIC

Unknown*

SOCIAL

Another indicator of China targeting Human Rights activists

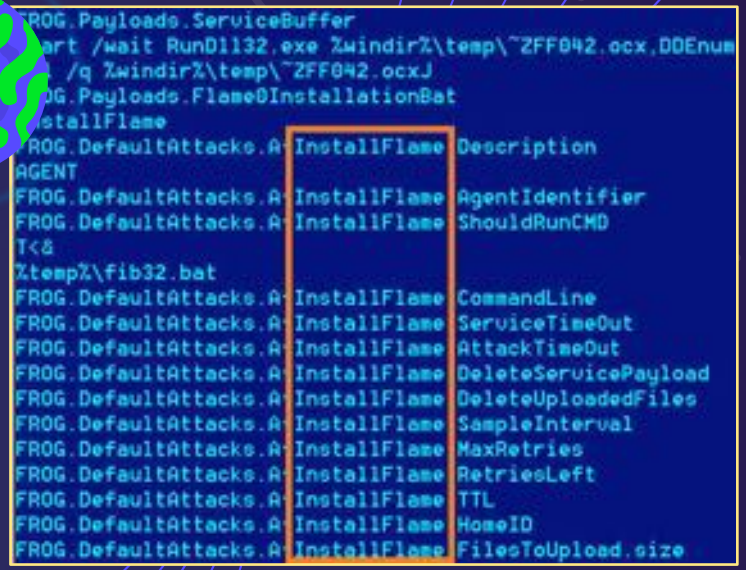
06

STUXNET

Cyberweapon Deployed

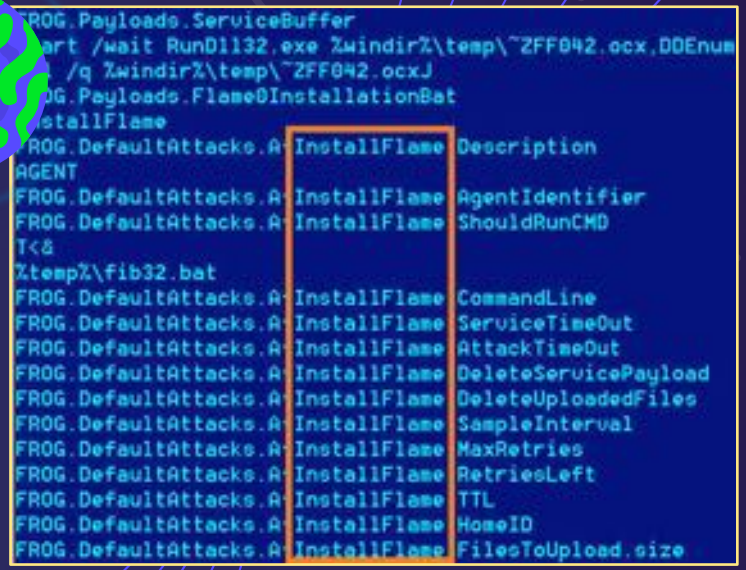
Initial Vector

- v1.001 of Stuxnet infects 4 organizations in June 2009
  - Foolad Technic
  - Behpajooh
  - Neda Industrial Group
  - CGJ (Control Gostar Jahed?)



Discovery

- Five months later Belarusian firm, VirusBlokAda, discovers a 0-day used and malicious use of RealTek Semiconductor cert to sign drivers
- 0-day used malicious .LNK files to spread via infected USB flash drives



THE HACK

- Targeted Windows via 4 0-day attacks
  - Malicious .LNK files on USB flash drives
  - Privilege escalation via vulnerable keyboard file
  - Windows print spooler vuln.
  - Windows task scheduler vuln.

THE HACK

- Payload – Step 7 software
  - Infects project files to MitM comms between Windows and Siemens PLCs
- Payload – PLC
  - Checks for specific criteria, modifies the frequency of the motor to change rotational speed

THE CONTROLS

Preventative:

Disabling use of USB flash drives in sensitive trust zones
Harden all devices by disabling unnecessary services
Use application whitelisting to limit code execution
Implement HIDS

Detective:

Logging and monitoring with alerts for anomalous activity
Use of honeypots (both desktop/server and SCADA)
Anti-virus*

Corrective:

Anti-virus*

THEIR EFFECTS UPON US

POLITICAL

Slows advancement of Iran's nuclear program

ECONOMIC

Unknown

SOCIAL

Multiple references in popular media: Castle S8E18, Trojan Horse, Ghost in the Shell: Arise, Tom Clancy's Splinter Cell: Blacklist

THANKS!

Do you have any questions?

@cipherthink

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

https://github.com/cipherthink/TheHacksThatMadeUs

REFERENCES

1. AOHell v3.0 ReadMe: http://www.aolwatch.org/chronic2.htm
2. Early Phishing: https://arxiv.org/pdf/1106.4692.pdf
3. AOL Underground – Da Chronic – Creator of AOHell and Automated Phishing: https://anchor.fm/aolunderground/episodes/Da-Chronic--Creator-of-AOHell-and-Automated-Phishing-e1ic74b/a-a7tfsc3
4. May 4, 2000: Tainted 'Love' Infects Computers: https://www.wired.com/2010/05/0504i-love-you-virus/
5. The 20-Year Hunt for the Man Behind the Love Bug Virus: https://www.wired.com/story/the-20-year-hunt-for-the-man-behind-the-love-bug-virus/
6. Top Ten Most-Destructive Computer Viruses: https://www.smithsonianmag.com/science-nature/top-ten-most-destructive-computer-viruses-159542266/
7. This 20-Year-Old Virus Infected 50 Million Windows Computers In 10 Days: Why The ILOVEYOU Pandemic Matters In 2020: https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in-2020/?sh=1a6aa9943c7c
8. 'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on: https://www.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html

REFERENCES

9. The Great Cyberheist: https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html

10. 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/

10. TJX Hacker Gets 20 Years in Prison: https://www.wired.com/2010/03/tjx-sentencing/

11. USA vs. Albert Gonzalez Sentencing Memo: https://www.wired.com/images_blogs/threatlevel/2010/03/gonzalez_gov_sent_memo.pdf

12. US Attorney Press Release about Sentencing of Stephen Watt: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/wattSent.pdf

13. A Famous Data Security Breach & PCI Case Study: Four Years Later: https://www.secureworks.com/blog/general-pci-compliance-data-security-case-study-heartland

14. PCI DSS Wireless Guidelines: https://listings.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

15. 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/

16. Hackers Take Down the Most Wired Country in Europe: https://www.wired.com/2007/08/ff-estonia/

REFERENCES

17. A Critical Evaluation of the Estonian Cyber Incident: https://openaccesspub.org/article/1489/jafs-20-3601.pdf

18. A New Approach to China: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

19. Darknet Diaries – Ep 19: Operation Aurora: https://darknetdiaries.com/episode/19/

20. Operation "Aurora" Hit Google, Others: https://web.archive.org/web/20120911141122/http://blogs.mcafee.com/corporate/cto/operation-aurora-hit-google-others

21. 'Google' Hackers Had Ability to Alter Source Code: https://www.wired.com/2010/03/source-code-hacks/

22. Leaked Cables Offer Raw Look at US Diplomacy: https://www.nytimes.com/2010/11/29/world/29cables.html

23. Protecting Your Critical Assets - McAfee write-up on Perforce: https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf

24. Elderwood project, who is behind Op. Aurora and ongoing attacks?: https://securityaffairs.co/wordpress/8528/hacking/elderwood-project-who-is-behind-op-aurora-and-ongoing-attacks.html

REFERENCES

25. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon: https://www.penguinrandomhouse.com/books/219931/countdown-to-zero-day-by-kim-zetter/

26. The History of Stuxnet: Key Takeaways for Cyber Decision Makers: https://www.afcea.org/committees/cyber/documents/thehistoryofstuxnet.pdf

27. Stuxnet Mitigation: https://scadahacker.com/resources/stuxnet-mitigation.html