Cyber Warfare

Cyber Security Seminar Series

Part 2

January 2022

To View an audio recording of this seminar Use this link:

- No need to create nor use a Vimeo account.
- https://vimeo.com/665398251

Realization Phase

- MILNET split from ARPANET 1983
- FAREWELL dossier KGB French intelligence

  Request for USA software Canadian software

  Soviet pipeline explosion October 1982

  CIA test of French?
- *The Cuckoo's Egg* Cliff Stoll 1986

  German hackers Lawrence Berkeley Lab Star Wars 75¢

  Who pays for Germany trip? What damages? Creditable evidence

Realization Phase

- Morris worm November 1988
  Rapid spread Widespread Private sector contained
- Computer Emergency Response Team (CERT)
- Computer Fraud and Abuse Act 1986
- Zippies DOS UK ban on outdoor raves
- Vladimir Levin – Russian - $10M from Citibank extradited
- First Gulf War 1991 Information warfare Cyber elements
- Information has mass, motion, topography
- Air Force Information Warfare Center and others
- Defense & Offense (Offense classified SCIF)
  Sensitive Compartmented Information Facility

Realization Phase

- Holland teenagers -> 34 military installations 1990

  Gulf war leadup NOT sophisticated NOT classified NOT noticed
- If teenage hackers can… what could professionals with money do?

Takeoff Phase (1998 – 2003)

- Presidential Decision Directive 63 1998

  Military & economy reliant on critical infrastructure and cyber
- National Infrastructure Protection Center (NIPC)

  Warn industry Industry warns
- ELIGIBLE RECEIVER 1997 no notice interoperability exercise NSA
- INFOCON like DEFCON
- SOLAR SUNRISE first thought to be Iraq

  California teenagers mentored by Israeli

  “who’s in charge?”

Well, who is in charge? And in charge of what?

- Cyber defense Cyber offense
- Stealth entry into country's systems to alter information Offense/Defense?

Microsecond response

- Can be “over” before it “starts”
- Thus, response is automated
- What could possibly go wrong?

Recent Events

- Iran Stuxnet
- Iran Saudi Aramco
- Iran US Financial institutions

- Iran GPS lure oil tankers into Iran waters Gulf of Hormuz
- US Cyber command publish cyber attack on Iran's shipping database
- Iran shot down US drone $182M
- Iran (?) missile attack Saudi refinery
- Gas prices

Recent Events

- Cyber tools can “escape”
- Cyber lacks “precision”
- Cyber war lacks any rules

Hide in plain sight

- The $200 chip in circuit board
- Reverse engineering semiconductor chip circuit
- ~2B transistors on CPU chip
- Previous reverse engineering use Copying
- Current reverse engineering use Altering
- FACET
- Code sprinkles
- Self Modifying Code

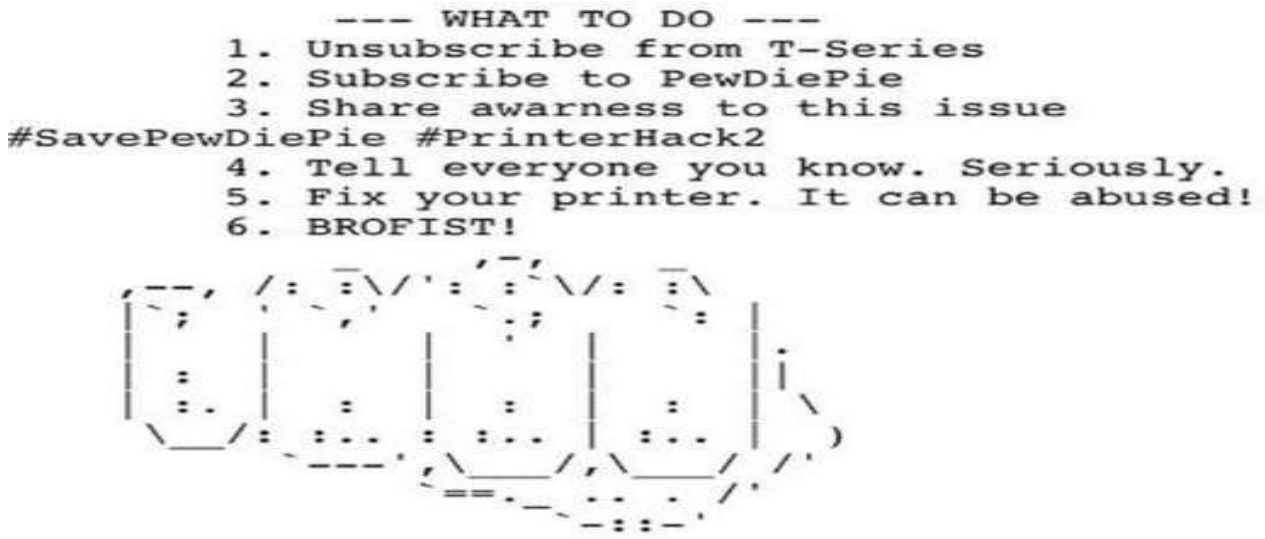
Not Petya

- MEDoc 27 June 2017
- Update compromised
- Similar to earlier attack using same vector
- EternalBlue
- WannaCry “kill switch”

Printer hack

- WSJ web site

"Wall Street Journal would like to apologize to pewdiepie. Due to misrepresentation by our journalists, those of whom have now been fired, we are sponsoring pewdiepie to reach maximum subscribers and beat Tseries to 80 million."



Facial Recognition

- AI
- China millions of AI enabled surveillance cameras

  Social Credit Score
- UK surveillance cameras
- Grocery store shelves
- Dragon flies don’t swarm

Information warfare Mis Information warfare

- Israel air strike Syrian nuclear facility “false sky picture”
- 6 day war Egyptian air defense radar
- GPS

  Jamming kits

  Spoofing Putin location NATO North Sea exercise

  1st Calvary Ft. Hood presentation cyber battlefield

Critical Infrastructure

- Electrical power

  Brazil - cyber but who?

  Ukraine - twice

  Russia June 2019 issues warning

  DoE Boise Idaho Generator 2006
- Waste water & water supply
- MAD
- Mutually Assured Disruption

Critical Infrastructure

- Financial
- 92% currency is electronic
- Coronal Mass Ejection 1859

Political

- Snowden 2013
- 2nd Snowden
- Pentagon Papers, Chelsea Manning, Benjamin Franklin
- 1777 first whistleblower protection law
- 2014 Nuland phone call “green men”
- Internet Research Agency Glavset
- NYT June 2019 US Russia power grid

COURTESY OF DEPARTMENT OF JUSTICE

- October 19,2020
- Ukraine
- French elections
- NotPetya
- Olympic Destroyer
- Novichok
- Georgian Government

Breaking News

- Energetic Bear NYT
- State & Local government probing/prowling
- US west coast airports Wi-Fi portals
- Thousands could be targets about 10 were
- Malware downloaded then looks for energy sector employees
- Possible election outcome confidence outcome steer

Breaking news

- US stepping up Russia power grid incursions
- New authorities under Trump Cyber offence US Cyber Command
- Classified National Security Presidential Memoranda 13
- Military Authorization Bill
- “Message-sending” operations
- Safety systems attacks
- Russia Internet isolation tests Deadman switch

- The leap NotPetya
- June 27, 2017
- Cadbury factory Tasmania Merck stopped vaccines production
- Maersk Largest shipping company paralyzed
- Ukraine No ATMs, no mass transit, no Chernobyl monitoring, computers wiped
- Cassandras predictions coming true?
- 2007 Russia hackers Estonia geopolitical

- Ukraine Power grid test lab?
- Dec 23, 2015

  BlackEnergy malware

  SCADA remote substations off

  Infrastructure UPS, modems, RTUs, commutators

  KillDisk

  DOS against call-centers

  Watching the mouse move the mouse was not moving
- Dec 2016 again a “tune-up” 00:00 exactly
- Aurora 140 KB

0-day

- Unpatched vulnerability
- eMail, WEB sites, Office suites, drive-by, security suites, etc.
- Great power e.g. PowerPoint
- Scripting ex. Java
- Port knocking
- SCADA summit Idaho National Labs
- Vulnerability scanners Virtual Machines C&C obfuscation
- Signature based defenses
- Sandworm signature

SCADA

- Air-gapped until it isn't constant scan
- PLCs ladder logic 24x7 Safety focus not easily isolated
- Reconnaissance
- Industrial Control Systems Cyber Emergency Response Team ISC-CERT
- They are in place Travelling SCADA technicians?
- SCADA technicians need access emergency access
- "we see you" methods and resources kept secret

Ukraine

- Slavic “borderland” long history of conquest, occupation, war
- 1918 grain 1932 starvation increased genocide to high degree
- 1980’s independence April 25, 1986 Chernobyl news suppression
- Feb 2014 Invasion July 2014 Malaysian passenger jet
- May 2014 CyberBerkut Central Election Commission Fancy Bear
- IRA
- Power pylons to Crimea
- Nov 2015 Pentagon meeting – warning “turn out the lights”
- SANS analysis placed on hold NERC

Moonlight Maze

- Hacking from Russia ≠ Hacking for Russia
- Russian general “those intelligence so-and-sos”
- No more Russian general less hacking then better hacking
- Joint Task Force-Computer Network Defense JTF-CND
- If power grid is at risk, everything is at risk

Estonia

- VERY Internet connected
- April 2007
- Statue relocated → Riots President moved
- Domestic network crippled
- Hackers enlist help from any/everyone “here it comes”
- Fight for days Cut off from outside
- Victory Day May 9 00:00
- NATO Article 5
- WEB War I

Georgia

- Aug 2008 Kinetic 25,000 troops 200 planes naval blockade
- Hybrid War I

North Korea

- North Korea develop cyber hackers
- North Korea steals large amounts of funds
- North Korea not part of IMF
- Dec 2014 Sony attacks
- We will respond proportionally, in a place & time we choose
- Nationwide internet outage days later
- Blame of misconfiguration
- North Korea has 1 class C network routed through China

Ukraine again

- Ukraine pension system
- Ukrzaliznytsia railway system holiday travel
- Historians do not need to talk to PLCs
- DHS DOE “road show”
- Taking US down harder Keeping it down easier


CRASHOVERRIDE
Analysis of the Threat
to Electric Grid Operations

What about U.S.

- Crashoverride report to congress
- Perfect storm timing
- “we’re fine, go away”
- Protective relays
- Sun City transformer fire
- Protection relays

0-day

- ShadowBrokers summer 2016 NSA Eternalblue
- Vault 7 2017 CIA
- How security suites work
- 0-days hoard or alert?


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


Ooops, your important files are
u see this text, but don't see the "Wan
your antivirus removed the decrypt soft
om your computer.
u need your files you have to run the d
find an application file named "@Wana
older or restore from the antivirus qua
BOARDWAY
King
ถ.วิทยุ
Witthayu Rd.

Wannacry

- Island hopping Just takes one
- Any/everywhere
- Uncontrolled NSA-zero-day worm
- Iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea
- North Korea
- Kaspersky Moscow based
- How security suites work
- How virtual machines work

THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Northern District of California under the authority of 18 U.S.C. § 981(b) as part of coordinated law enforcement action by:

The United States Attorney's Office for the Northern District of California

Federal Bureau of Investigation

For additional information, see https://www.justice.gov

Work From Home WFH

- Twitter hack Trump twitter passphrase
- Certificate Authority
- Mimikatz Pass the hash
- Credential stuffing
- Financial legacy theft MFA
- US Cyber command “hunt forward”

Other Russia ??

- France 2015 TV5Monde
- France 2017 20,000 emails Presidential campaign
- Germany 2015-2017 Election interference
- Kyrgyzstan 2009 ISPs offline US air base
- Poland Facebook dis-information campaign
- South Korea Olympic Destroyer 2018 Winter Games
- UK Brexit
- Tokyo Olympics

NotPetya

- Week 1
- WannaCry on steroids Administrator rights & privilege
- No kill switch no decryption keys
- Eternal Blue + Mimikatz
- Escaped from Ukraine
- Ukraine hard hit
- Maersk 1 terminal 3000 trucks per day

Well, patch

- Critical
- Patch Large Infrastructures
- Apps were written decades ago
- Pirated copies - not easily patched
- Perfect storm
- Today Zerologon VPN

- Feb 2018 WH & GCHQ public statement
- Sanctions & indictments
- Indictments require evidence
- Bad Rabbit smokescreen?
- Olympic Destroyer forged metadata
- ISIS
- IRA disabled for 2018 Mid-terms
- Iowa caucus
- Perception attack?

- US not calling out actions so those actions are available to US
- Geneva civilian protections in time of war

  civilian attacks in time of peace

Other Actors

- USA
- Syrian Electronic Army
- 5 Eyes
- North Korea
- China
- EVERY ONE

China

- Titan Rain 2003 –
- Sensitive
- Espionage unreported unknown unnerved
- 2011 Google
- 2011 RSA stepping stone F-35 cost overruns
- BYZANTINE HADES Mandiant APT persistent
- Nortel ↓ Huawei ↑
- Greatest transfer of wealth in history
- Government & Industry
- OPM data breach

Power Grid

- USA 3 grids
- Nov. , 2018 DARPA Plumb Island grid

Estonia revisit

- Statue relocated still
- Tactical & strategic defeat for attackers
- Estonian government not coerced
- Economy and reputation improved
- NATO Cooperative Cyber Centre of Excellence Tallinn, Estonia
- Estonia aware of impending attacks NATO and world leaders not
- Estonia control IXP (Internet Exchange Point)
- Georgia not Georgia transferred some sites to US

  International consequences?

Buckshot Yankee

- 2008 US Central Command classified network
- Agent.btz
- SIPRNET operational commands
- JWICS highest classification intelligence material
- It just takes 1 USB drive infection?

Hackers are cyber immune systems

- Cuckoo's Egg Morris Worm
- Encryption of military drone
- Hack a F-35 Hack the Pentagon Hack a satellite
- Cyber warfare is **very different**
- As each of us are safer we are ALL safer

Cyber Warfare

- Increased sophistication
- Increased magnitude
- Increased intensity
- Increased volume
- Increased velocity
- One hits 155 countries in ONE DAY It just takes one
- Perfect weapon Perfect storm Pandemic, riots, division, election + cyber
- Dis-informationdemic
- Hacking-as-a-service

China

- OPM 25 Million security clearance files
- F-35
- RSA
- Google
- Anthem
- Huawei
- Covid-19 research
- China government & Industry strongly linked
- Economic inroads

Voter registration

- You can see yours, mine, and others
- Those databases can be purchased
- Those databases have been left with no or little protections in cloud

Voter Lists | 50 State Political Voter Database

Why Voter Lists?

Gravis Marketing believes that **accurate voter lists** are essential to any campaign. As the new currency in politics, voter lists can make or break elections by determining whom your campaign is reaching.

Having access to a detailed voter database is the most effective way to streamline your campaign, sending your message to specific voters from any region, affiliation, or demographic.

Why Our Voter Database?

Gravis Marketing can adapt your voter lists to the changing trends of your voters, helping you with your specific goals in the specific ways you need.

We know that making the most of your budget is a priority. You need something flexible, customizable, and dependable. That's why our comprehensive database includes:

- **Voter files** from all states, kept up-to-date with 24-hour turnaround.
- **Phone numbers**, including updated landlines and cell phones.
- **Email addresses**, trimmed of inactive and unresponsive inboxes.
- **Detailed demographic information**, including age, race, ethnicity, religion, and income.
- **National changes of address**.
- **Party and interest group affiliations**, with voter histories.
- **Social memberships**.

Lessons Learned & Unlearned