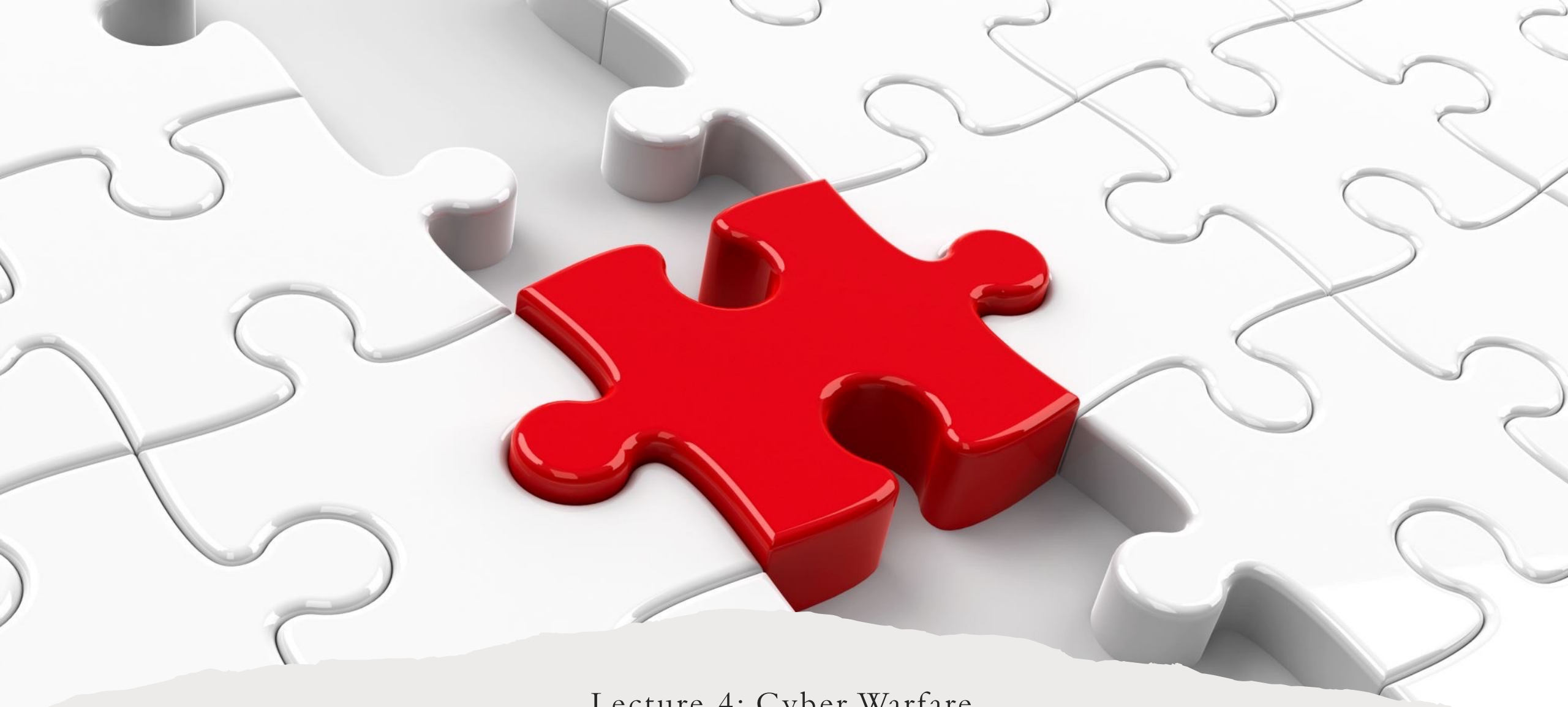


Lecture 4: Cyber Warfare.

SEC_RITY IS NOT COMPLETE WITHOUT U!

WEEK 4: CYBERWARFARE.

1. Principles of Cyberwarfare [3-20]
    a) Cyberwarfare and CyberSpace [3]
    b) United States Cyber Command [6]
    c) Information Warfare [11]
2. Cyber Security Incidents [24-25]
3. Ransomware [26-41]
4. Zero Day [43]
5. Solar Winds, HAFNium, Colonial Pipeline, LOg4J [50-53]
6. Cyberwarfare - Russia[54]
7. Discussion (20 minutes)
8. Extra Material [55-76]
9. Authentication

1) DEFINITIONS

- ***Cyberwarfare*** is the use of digital attacks against an enemy state, causing comparable harm to actual warfare and/or disrupting the vital computer systems.

  Singer, P. W.; Friedman, Allan (March 2014). *Cybersecurity and cyberwar : what everyone needs to know*. Oxford. ISBN 9780199918096. OCLC 802324804

  ISSUE: no offensive cyber actions to date could be described as war (violent, instrumental, and political) versus a label for cyber attacks which cause physical damage to people and objects in the real world.

  cyberwar, also called ***cyberwarfare*** or ***cyber warfare***, is war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states. Cyberwar is usually waged against government and military networks in order to disrupt, destroy, or deny their use. (Encyclopedia Britannica)

1B) CYBERSPACE DISTINGUISHES ATTACKS

- Cyberspace comprises of 3 layered components: computers+networks; software;humans
- A Nations Critical infrastructure now depends on cyberspace
- Cyber attacks can be made against the *physical infrastructure*, *syntactic (software)*, and *semantic (human interaction)* layers of cyberspace; note the dependencies between layers.
- Physical examples: NATO attacks on Yugoslavia (1999) and US-led attack on Iraq (2003) destroying communication networks, computer facilities, telecommunications.
- Syntactic examples: attacks against Estonia (2207) and Georgia (2008) using hijacked computers acting as botnets to swamp government, financial, media, and commercial web sites with network traffic (denial of service)
- Semantic examples: social engineering, phishing to acquire ids and names of intelligence agents, ransomeware attacks on medical facilities

CAUSE AND EFFECT OF WARFARE

- The argument against the definition of cyberwarfare is that it is usually associated with other typical acts of war as opposed to being an act of war in itself.
- In the Israeli-Hezbollah conflict in Lebanon in 2006 and the Russian invasion of Georgia in 2008, cyberattacks were launched before the armed conflicts began and afterwards too --- but they didn't create the conflicts.

However, it is believed that the increasing importance and consequences of cyberattacks will soon be considered an act of war by themselves.

1B) UNITED STATES CYBER COMMAND

USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[5][6]

"Cyber Command Fact Sheet". U.S. Department of Defense. 21 May 2010. Archived from the original on 16 April 2014.

US CYBER COMMAND

https://en.wikipedia.org/wiki/United_States_Cyber_Command#Mission_statement

Current Commander

General
Paul M. Nakasone
(born 1963)

U.S. Army

Paul Nakasone serves concurrently as the Director of the National Security Agency[3][4] and as Chief of the Central Security Service.

GENERAL NAKASONE TESTIFIES ON DOD CYBERSPACE OPERATIONS.

May 14, 2021

https://youtu.be/tMqcJKM0j7I?t=940

Time code 15:51 to 17:06

https://www.youtube.com/watch?v=TsMcE1clxTI

PRINCIPALS OF CYBERWARFARE

(*INFORMATION WARFARE AND SECURITY, DOROTHY DENNING, 1998*)

1. Information Resources
2. Players
   a) Offense
   b) Defence
   c) A Dual Role
3. Offensive Information Warfare
   a) Increased availability and integrity to Offensive Player
   b) Decreased availability and integrity to Defensive Player
4. Defensive Information Warfare
   a) Types of Defense: Passive & Active
   b) Information Security and Assurance (CIA Model and Authorization)
5. Can be viewed as a Game

COMMAND CYCLE IS BECOMING SHORTER

Adapted from Sullivan and Dubik, War In the Information Age. SSI US Army War College, 1994

- Speedy reactions to changing circumstances and data in warfare is creating a strong dependency on cyberspace.
- Attacks on cyberspace can quickly lead to considerable damage
- This makes cybersecurity very important in warfare
- In turn, this makes cyberwarfare extremely important.

1C) WHAT IS INFORMATION WARFARE ?

Information warfare is a coherent and synchronized blending of physical and virtual actions to have countries, organizations, and individuals perform, or not perform, actions so that your goals and objectives are attained and maintained, while simultaneously preventing your competitors from doing the same to you

(Global; Information Warfare: How Businesses, Governments and Others Achieve Objectives and Attain Competitive Advantages, Gerald Kovacich, Perry Luzwick, and Andy Jones.)

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

INFORMATION WARFARE

- Objective of Information Warfare
- Exploitation
- Deception
- Disruption
- Destruction
- To achieve the objective of Information Warfare
- Natural hazard and unintended threats
- Tactical attack
- Strategic attack

INFORMATION WARFARE

Advantages

- Less human causalities
- Less cost
- Information Technology

Disadvantages

- Trust
- Unexpected result
- Terrorism
- Undeclared war

WHO ARE THE PLAYERS?

- Military info-warriors
- Intelligent agents
- Economic espionage agents
- Technology terrorists
- Terrorists
- Activists
- Revolutionaries
- Freedom Fighters

THE NEW BATTLEFIELD

Prevalent revolutions in military affairs come in the form of:

1. cyberattacks,
2. autonomous robots and
3. communication management.

Two primary weapons:

1. network-centric warfare and
2. C4ISR, (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)

Cyberspace attacks initiated by one nation against another nation have an underlying goal of gaining information superiority over the attacked party, which includes disrupting or denying the victimized party's ability to gather and distribute information.

EXAMPLES FROM REAL LIFE

- Israel performed a cyberattack on Syria's defenses, which left them blind to an Israeli attack on an alleged nuclear reactor in Syria (New York Times 2014)
- Distributed Denial of Service attacks on Ukraine government and banking web sites as part of a psychological campaign against the people of Ukraine (CNN 2022) https://www.cnn.com/2022/02/16/europe/ukraine-cyber-attack-denial-service-intl/index.html
- Potential attacks on power grid servers in a specific area to disrupt communications, civilians and businesses in that area would also have to deal with power outages (BBC 2016-17). https://www.bbc.com/news/technology-38573074

TYPE OF ATTACKS IN CYBERWARFARE

1) Passive Attack

a) The attacker simply monitors the traffic being sent to try to learn secrets.

b) Passive attacks are the most difficult to detect.

c) Assume that someone is eavesdropping on the system.

2) Active Attack

a) The attacker is trying to break through your defenses

b) Cryptographic attacks

c) Spoofing

d) System access attempts

COMMON TYPES OF CYBER ATTACKS:

- Denial of Service
- Web Defacement
- System Modification
- Theft (Information)
- Radio Frequency
- TEMPEST
- Social Engineering
- Viruses and Warms
- Bugs

CYBER WARFARE TACTICS:

- Covertly probe and document the results
- Once inside, check for other systems
- Once inside, find and transmit sensitive information
- Once inside, set Logic Bombs, Trojan Horses and Trap Doors
- Erase evidence of intrusion
- Search for additional and systems of the nation-state

CONFLICTS BETWEEN NATION-STATES:

- Intelligence gathering
- Protection, Exploitation, and hacker war
- Diplomatic pressure
- Psychological Operation
- Economic pressure
- Economic Warfare
- Military posturing
- Deception
- Combat
- Precision and Information Weapons Electronic Warfare
- Reconstruction

2) EXAMPLES OF RECENT MAJOR CYBER INCIDENTS.

- Kaseya. Revil, Sodinokibi, pipeline attacks, SolarWinds…

CYBER INCIDENT HISTORY

- https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

3) THE RANSOMWARE STORY

- Kaseya attack on July 2, 2021 supply-chain ransomware
- Kayesa is an IT endpoint management, automation, and protection service company
- ransomware criminal group called Revil used Kaseya to distribute ransomware to its on-premises customers.
- The REvil payload (Ransomware Evil or also known as Sodinokibi) is ransomware as a service criminal enterprise.
- REvil is said to be related to the criminal group known as GandCrab.
- In a Ransomware as a service scheme, malicious actors partner with affiliates to extend their botnets and reap profits from new additions and attacks brought to them by affiliates. The profit is shared with affiliates which encourages them to infect more victims.

WHO IS REVIL

- ***REvil*** (***Ransomware Evil***; also known as ***Sodinokibi***) was a Russia-based[1] or Russian-speaking[2] private ransomware-as-a-service (RaaS) operation.[3]
- After an attack, REvil would threaten to publish the information on their page *Happy Blog* unless the ransom was received.
- In a high profile case, REvil attacked a supplier of the tech giant Apple and stole confidential schematics of their upcoming products.
- Russia's top domestic intelligence agency says REvil – the Russia-based ransomware gang tied to the Colonial Pipeline attack – ***has "ceased to exist"*** after the agency arrested 14 alleged members of the criminal organization last week 19 Jan 2022
- Cybersecurity experts believe REvil is an offshoot from a previous notorious, but now-defunct hacker gang, ***GandCrab***. This is suspected due to the fact that REvil first became active directly after GandCrab shutdown, and that the ransomware both share a significant amount of code.

HISTORY MAY 2020

- Stole nearly one terabyte of information from the law firm Grubman Shire Meiselas & Sacks and demanding a ransom to not publish it.
- They demanded $42 million from US president Donald Trump
- Released legal documents totaling a size of 2.4 GB related to the singer Lady Gaga.

HISTORY MARCH 2021

- On 27 March 2021, REvil attacked Harris Federation and published multiple financial documents of the federation to its blog. As a result, the IT systems of the federation were shut down for some weeks, affecting up to 37,000 students.
- an REvil affiliate claimed on their data leak site that they had downloaded data from multinational hardware and electronics corporation Acer, as well as installing ransomware, which has been linked to the 2021 Microsoft Exchange Server data breach by cybersecurity firm Advanced Intel, which found first signs of Acer servers being targeted from 5 March 2021.

HISTORY APRIL 2021

- In April 2021, REvil stole plans for upcoming Apple products from Quanta Computer, which is said to include plans for a pair of Apple laptops, a new Apple Watch and a new Lenovo ThinkPad. REvil threatened to release the plans publicly unless they receive $50 million.

HISTORY MAY 2021

- JBS S.A. (Brazil) was attacked by ransomware which forced the temporary shutdown of all the company's U.S. beef plants and disrupted operations at poultry and pork plants.

HISTORY JULY 2021

- On 2 July 2021, hundreds of managed service providers had REvil ransomware dropped on their systems through Kaseya desktop management software.[26] REvil demanded $70 million to restore encrypted data.[27] As a consequence the Swedish Coop grocery store chain was forced to close 800 stores during several days.
- On 7 July 2021, REvil hacked the computers of Florida-based space and weapon-launch technology contractor HX5, which counts the Army, Navy, Air Force, and NASA among its clients, publicly releasing stolen documents on its Happy Blog. The New York Times judged the documents to not be of "vital consequence".
- After a July 9 phone call between United States president Joe Biden and Russian president Vladimir Putin, Biden told the press, "I made it very clear to him that the United States expects when a ransomware operation is coming from his soil even though it's not sponsored by the state, we expect them to act if we give them enough information to act on who that is." Biden later added that the United States would take the group's servers down if Putin did not.

HISTORY JULY 2021 CONTINUED

- On 13 July 2021, REvil websites and other infrastructure vanished from the internet.[33] Politico cited an unnamed senior administration official as stating that "we don't know exactly why they've [REvil] stood down;" the official also did not discount the possibility that Russia shut down the group or forced it to shut down.
- On 23 July 2021, Kaseya announced it had received the decryption key for the files encrypted in the July 2 Kaseya VSA ransomware attack from an unnamed "trusted third party", later discovered to be the FBI who had withheld the key for three weeks, and was helping victims restore their files.[35] The key was withheld to avoid tipping off REvil of an FBI effort to take down their servers, which ultimately proved unnecessary after the hackers went offline without intervention.

HISTORY SEPTEMBER 2021

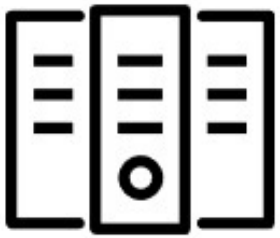
- In September 2021, Romanian cybersecurity firm Bitdefender published a free universal decryptor utility to help victims of the REvil/Sodinokibi ransomware recover their encrypted files, if they were encrypted before July 13, 2021.[37] From September until early November, the decryptor was used by more than 1,400 companies to avoid paying over $550 million in ransom and allow them to recover their files.[38]
- On 22 September 2021, malware researchers identified a backdoor built into REvil malware that allowed the original gang members to conduct double-chats and cheat their affiliates out of any ransomware payments.[39] Ransomware affiliates who were cheated reportedly posted their claims on a "Hacker's Court", undermining trust in REvil by affiliates. Newer versions of REvil malware reportedly had the backdoor removed.

HISTORY NOVEMBER 2021

- On 8 November 2021, the United States Department of Justice unsealed indictments against Ukrainian national Yaroslav Vasinskyi and Russian national Yevgeniy Polyanin. Vasinskyi was charged with conducting ransomware attacks against multiple victims including Kaseya, and was arrested in Poland on 8 October. Polyanin was charged with conducting ransomware attacks against multiple victims including Texas businesses and government entities. The Department worked with the National Police of Ukraine for the charges, and also announced the seizure of $6.1 million tied to ransomware payments. If convicted on all charges, Vasinskyi faces a maximum penalty of 115 years in prison, and Polyanin 145 years in prison.[43]
- In January 2022, the Russian Federal Security Service said they had dismantled REvil and charged several of its members after being provided information by the US

RANSOMWARE--- THE ATTACK

- In order to be successful, ransomware needs to gain access to a target system, encrypt the files there, and demand a ransom from the victim.
- phishing emails. A malicious email may contain a link to a website hosting a malicious download or an attachment that has downloader functionality built in. If the email recipient falls for the phish, then the ransomware is downloaded and executed on their computer.
- Remote Desktop Protocol (RDP). With RDP, an attacker who has stolen or guessed an employee's login credentials can use them to authenticate to and remotely access a computer within the enterprise network. With this access, the attacker can directly download the malware and execute it on the machine under their control.
- Exploit the EternalBlue vulnerability. Most ransomware variants have multiple infection vectors.



Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **xotbj-Decryptor**

Follow the instructions below. But remember that you do not have much time

[redacted]j-Decryptor price

You have 5 days, 00:45:40

* If you do not pay on time, the price will be doubled
* Time ends on **Jul 9, 13:08:51**

Current price 200.6550409 XMR
≈ 44,999 USD

After time ends 401.3100818 XMR
≈ 89,998 USD

ETERNAL BLUE

- ***EternalBlue***[5] is a cyberattack exploit developed by the U.S. National Security Agency (NSA).[6] It was leaked by the Shadow Brokers hacker group on April 14, 2017, one month after Microsoft released patches for the vulnerability.

- Used by WannaCry and NotPetya

PETYA

Petya is a family of encrypting malware that was first discovered in 2016.[2] The malware targets Microsoft Windows–based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system. The Petya malware had infected millions of people during its first year of its release. The maker of the Petya malware was arrested and fined.

PETYA

Petya's payload infects the computer's master boot record (MBR), overwrites the Windows bootloader, and triggers a restart. Upon startup, the payload encrypts the Master File Table of the NTFS file system, and then displays the ransom message demanding a payment made in Bitcoin.[6][25][26] Meanwhile, the computer's screen displays text purportedly output by chkdsk, Windows' file system scanner, suggesting that the hard drive's sectors are being repaired.[1]

The earlier versions of Petya disguised their payload as a PDF file, attached to an e-mail.

NOTPETYA

The "NotPetya" variant used in the 2017 attack uses EternalBlue, an exploit that takes advantage of a vulnerability in Windows' Server Message Block (SMB) protocol. The malware harvests passwords (using tweaked build of open-source Mimikatz[29]) and uses other techniques to spread to other computers on the same network, and uses those passwords in conjunction with PSExec to run code on other local computers. Additionally, although it still purports to be ransomware, the encryption routine was modified so that the malware could not technically revert its changes.

4) ZERO DAY ATTACKS

- A ***zero-day*** is a computer-software vulnerability either unknown to those who should be interested in its mitigation (including the vendor of the target software) or known and without a patch to correct it.

- https://en.wikipedia.org/wiki/Zero-day_(computing)

PREVENTION OF ZERO DAY ATTACKS

- Border Protection
- System Hardening
- Antivirus Software
- Patch Management
- Vulnerability Management
- Application Hardening
- Blocking Attachments
- Honeypots

DETECTING A ZERO-DAY ATTACK

- Behavior-based systems (IDS and IPS) alerts
- Antivirus software alerts as a result of heuristic scanning
- Unusual events in the system log files (i.e. failed logons)
- Poor system performance
- Unexplained system reboots
- Network traffic on unexpected ports, especially on ports known to be backdoor ports for known blended threats (i.e. MyDoom: TCP ports 3127 through 3198)
- Increased network traffic on a legitimate port
- Increased scanning activity
- Unusual SMTP traffic, especially originating from systems that should not be using SMTP

EXAMPLES OF ZERO-DAY ATTACKS

2021: Chrome zero-day vulnerability

Google's Chrome suffered a series of zero-day threats, causing Chrome to issue updates. The vulnerability stemmed from a bug in the V8 JavaScript engine used in the web browser.

2020: Zoom

This zero-day attack on video conferencing platform involved hackers accessing a user's PC remotely if they were running an older version of Windows. If the target was an administrator, the hacker could completely take over their machine and access all their files.

2020: Apple iOS

Apple's iOS is often described as the most secure of the major smartphone platforms. However, in 2020, it fell victim to at least two sets of iOS zero-day vulnerabilities, including a zero-day bug that allowed attackers to compromise iPhones remotely.

2019: Microsoft Windows, Eastern Europe

This attack focused on local escalation privileges, a vulnerable part of Microsoft Windows, and targeted government institutions in Eastern Europe. The zero-day exploit abused a local privilege vulnerability in Microsoft Windows to run arbitrary code and install applications and view and change the data on compromised applications. Once the attack was identified and reported to the Microsoft Security Response Center, a patch was developed and rolled out

EXAMPLES OF ZERO-DAY ATTACKS

2017: Microsoft Word

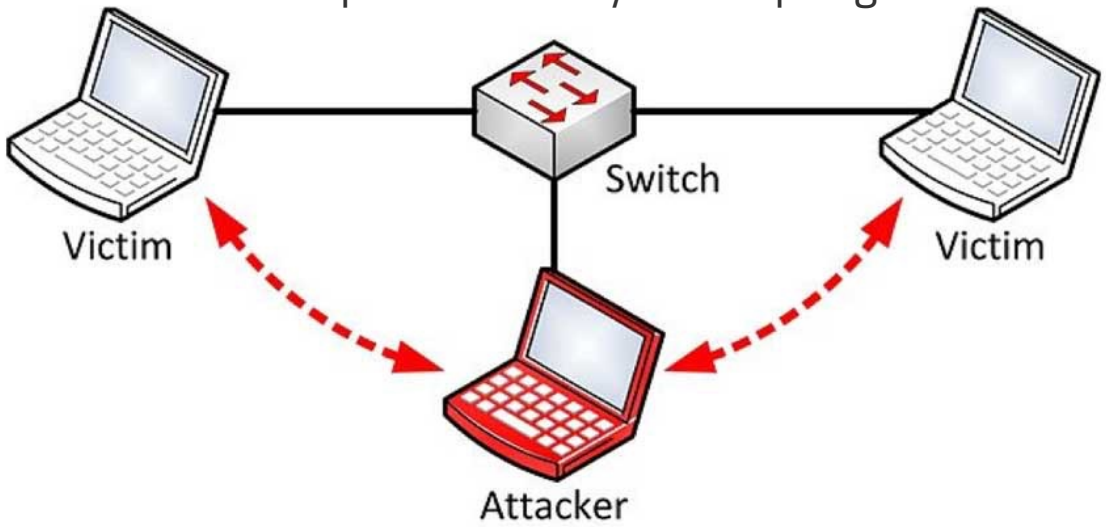
Compromised personal bank accounts. Victims were people who unwittingly opened a malicious Word document. The document displayed a "load remote content" prompt, showing users a pop-up window that requested external access from another program. When victims clicked "yes," the document installed malware on their device, which was able to capture banking log-in credentials.

Stuxnet

Famous example Stuxnet. First discovered in 2010 but with roots that spread back to 2005, this malicious computer worm affected manufacturing computers running programmable logic controller (PLC) software. The primary target was Iran's uranium enrichment plants to disrupt the country's nuclear program. The worm infected the PLCs through vulnerabilities in Siemens Step7 software, causing the PLCs to carry out unexpected commands on assembly-line machinery. The story of Stuxnet was subsequently made into a documentary called Zero Days.

Man-in-the-Middle (MitM) Attacks

Occurs when an attacker intercepts a two-party transaction, inserting themselves in the middle. From there, cyber attackers can steal and manipulate data by interrupting traffic.



This type of attack usually exploits security vulnerabilities in a network, such as an unsecured public WiFi, to insert themselves between a visitor's device and the network. The problem with this kind of attack is that it is very difficult to detect, as the victim thinks the information is going to a legitimate destination. Phishing or malware attacks are often leveraged to carry out a MitM attack.

.

Denial-of-Service (DOS) Attack

DOS attacks work by flooding systems, servers, and/or networks with traffic to overload resources and bandwidth. This result is rendering the system unable to process and fulfill legitimate requests. In addition to denial-of-service (DoS) attacks, there are also distributed denial-of-service (DDoS) attacks.
DoS attacks saturate a system's resources with the goal of impeding response to service requests. On the other hand, a DDoS attack is launched from several infected host machines with the goal of achieving service denial and taking a system offline, thus paving the way for another attack to enter the network/environment.
The most common types of DoS and DDoS attacks are the TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack,and botnets.

4) SOLAR WINDS CYBER-ATTACK

December 13, 2020

FireEye announced the discovery of a highly sophisticated cyber intrusion that leveraged a commercial software application made by SolarWinds.

It was determined that the advanced persistent threat (APT) actors infiltrated the supply chain of SolarWinds, inserting a backdoor into the product.

As customers downloaded the Trojan Horse installation packages from SolarWinds, attackers were able to access the systems running the SolarWinds product(s).

33,000 public and private sector customers were impacted

HAFNIUM MICROSOFT HACK

March 2021

Four previously undiscovered weaknesses in Microsoft's Exchange software, known as "zero days" because of the amount of time the company had had to fix the flaws before they were exploited, lay behind the mass hack.

Tens of thousands of organizations around the world discovered their private internal discussions had been cracked open and lain bare by a group of Chinese hackers.

US and Britain blame China. Hafnium is the name of the Chinese state-sponsored hacking group.

PIPELINES ATTACKED

- ***Hackers Breached Colonial Pipeline Using Compromised Password***
- Hackers gained entry into the networks of Colonial Pipeline Co. on April 29, 2021 through a virtual private network account using a single compromised password.

Colonial paid the hackers, who were an affiliate of a Russia-linked cybercrime group known as DarkSide, a $4.4 million ransom shortly after the hack.

LOG4J ZERO-DAY VULNERABILITY

December 9, 2021

Vulnerability in the code of a software library used for logging. The software library, Log4j, is built on a popular coding language, Java, that has widespread use in other software and applications used worldwide. This flaw in Log4j is estimated to be present in over 100 million instances globally. This vulnerability and associated attacks against it are being characterized as *Log4Shell* in the cybersecurity community.

6) CYBERWARFARE BY RUSSIA

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

ATTACKS

Estonia, France, Georgia, Germany, Kyrgyzstan, Poland

South Korea, Ukraine, Ukrainian presidential election

United Kingdom "Brexit" referendum

United States, Venezuela

Senate minority report: Putin's Asymmetric Assault on Democracy in Russia and Europe (2018):

https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

Images of military near Ukraine

https://www.reuters.com/world/europe/new-russian-deployments-armored-equipment-troops-near-ukraine-maxar-2022-02-20/

IF WE HAVE TIME

CYBERSECURITY ISSUES I HAVENT COVERED YET

- TEMPEST; wireless, thermal, acoustic emissions including cables, screens, PCs, keypress https://en.wikipedia.org/wiki/Tempest_(codename)
- Dopplar https://www.celeno.com/wifi-doppler-imaging
- Backdoors for government https://en.wikipedia.org/wiki/Backdoor_(computing)
- Fake images etc https://www.boredpanda.com/fake-news-photos-viral-photoshop/?utm_source=google&utm_medium=organic&utm_campaign=organic
- Sidechannel and Rowhammer Rowhammer is an attack technique involving accessing — that's "hammering" — rows of bits in memory, millions of times per second, with the intent of causing bits in neighboring rows to flip. This is a side-channel attack, and the result can be all sorts of mayhem.
- Airtags https://www.hackread.com/apple-airtags-exploited-credential-hacking/
- SMS phishing, Netflix: [Name], please update your membership with us to continue watching. [very sketchy URL]. pop-up ads that drove smart phone users to "security" applications on both app stores, using fake alert pages resembling mobile operating system alerts that warned of virus infections on devices. https://cybersecurity.att.com/blogs/security-essentials/sms-phishing-explained-what-is-smishing

SEEING THROUGH WALLS – DOPPLAR IMAGING USING WIFI

- https://www.celeno.com/wifi-doppler-imaging

AUTHENTICATION

- Authentication is the act of verifying a claim of identity.
- Something you know:
  PIN, password, or your mother's maiden name
- Something you have:
  driver's license, magnetic swipe card, token
- Something you are:
  biometrics, including fingerprints, voice prints

https://en.wikipedia.org/wiki/Multi-factor_authentication

MULTIFACTOR AUTHENTICATION

- 2 or more Factors

  Something you know: e.g. PIN or password

  Something you have: security token, USB stick, bank card, key…

  Something you are: biometric: fingerprint, eye iris, face, voice,…

  Somewhere the user is: network connection, GPS

  Early authenticators used a SMS Text to send a code

SMART PHONE, SMS BASED AUTHENTICATION

THIRD PARTY AUTHENTICATOR DEVICE

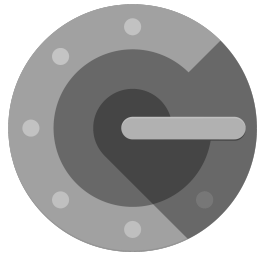
Provides a user with a randomly generated and constantly refreshing code which the user:

1) types the code in as a second authentication or
2) connects the device to a cell phone or laptop in some way- operates on click of button- better than sending an SMS or using another method.

These devices continue to work even without an internet connection.

THIRD PARTY AUTHENTICATOR APP

- Third-party authenticator apps include
- Google Authenticator
- Authy
- Microsoft Authenticator
- password managers: e.g. LastPass



Can be installed on cell phone or laptop

SOFTWARE AUTHENTICATOR (SOFT TOKEN)

- Software tokens are stored on a general-purpose electronic device such as a desktop computer, laptop, PDA, or mobile phone and can be duplicated.
- Typically an X.509v3 certificate is used as the token. Not interactive.
- Good for accessing websites and files from laptop

IN ORDER OF SECURITY STRENGTH

- Software Token
- SMS
- Authenticator app
- Authenticator device like YubiKey

DIFFERENT KINDS OF DEVICE AUTHENTICATOR

- THETIS FIDO U2F SECURITY KEY
- GOOGLE TITAN KEY
- KENSINGTON VERIMARK FINGERPRINT KEY

- USB-A connector and wireless NFC — is the best key for logging into your online accounts, services, macOS computers, Android devices, and the iPhone 7 and up. Few issues using it in a USB-A port, or with a mobile device using the NFC feature. The YubiKey 5 NFC supports a plethora of security standards, including OTP, Smart Card, OpenPGP, FIDO U2F, and FIDO2.

4A) BIOMETRIC AUTHENTICATION

- Multifactor biometric authentication is one of the most effective forms of logical security available to organizations. By requiring users to verify their identity with biometric credentials
- Fingerprints
- Facial Recognition
- IRIS
- Retina
- DNA
- Voice
- Behavior
- You can ensure that the people accessing and handling data and documents are who they claim to be.

GOOGLE ESTIMATES OF BIOMETRICS

	Verify	*ID*	*Accuracy*	*Reliability*	*Error Rate%*	*False Pos*	*False Neg*	*Errors*
Fingerprint	yes	yes	5	4	0.2	6	6	dryness, dirt, age
Facial Recognition	yes	no	4	3	?	4	1	lighting, age, glasses, hair
Speaker Recognition	yes	no	4	2	2	3	1	noise, weather, colds
Iris Scan	yes	yes	5	4	7.10^{-5}	5	5	poor lighting
Signature	yes	no	3	2	2	3	1	changing signatures
Keystroke	yes	no	2	2		4	1	hand injury, tiredness
DNA	yes	yes	5	5		6	6	none

GOOGLE ESTIMATES OF BIOMETRICS

	Security Level	Long-term Stability	User Acceptance	Intrusive	Ease of Use	Low Cost	Hardware	***Standards***
Fingerprint	High	High	Medium	Somewhat	High	Yes	Special, cheap	Yes
Facial Recognition	Medium	Medium	Medium	Non	Medium	Yes	Common, cheap	?
Speaker Recognition	Medium	Medium	High	Non	High	Yes	Common, cheap	?
Iris Scan	High	High	Medium	Non	Medium	No	Special, expensive	?
Signature	Medium	Medium	Medium	Non	High	Yes	Special, mid-price	?
Keystroke	Medium	Low	High	Non	HIgh	Yes	Common, cheap	?
DNA	High	High	Low	Extremely	Low	No	Special, expensive	Yes

LOOP FINGERPRINTS

Radial Loops: Named after the radius bone, these loops join the hand on the same side as the thumb, flowing in a downward slope from the little finger toward the thumb.

Ulnar Loops: This name refers to the ulna bone. The loop has a circular pattern, running from the thumb toward the pinky.

Double Loops: As the name suggests, these loops have two separate loop formations and at least one recurving ridge within the inner pattern.

WHORL FINGERPRINTS

Plain Whorl: These include concentric circles, with one complete circle and two deltas.

Central Pocket Loop Whorl: This is a loop with a whorl at the end of it, which can be oval, spiral, or circular.

Accidental Whorl: As the name implies, this type is irregularly shaped.

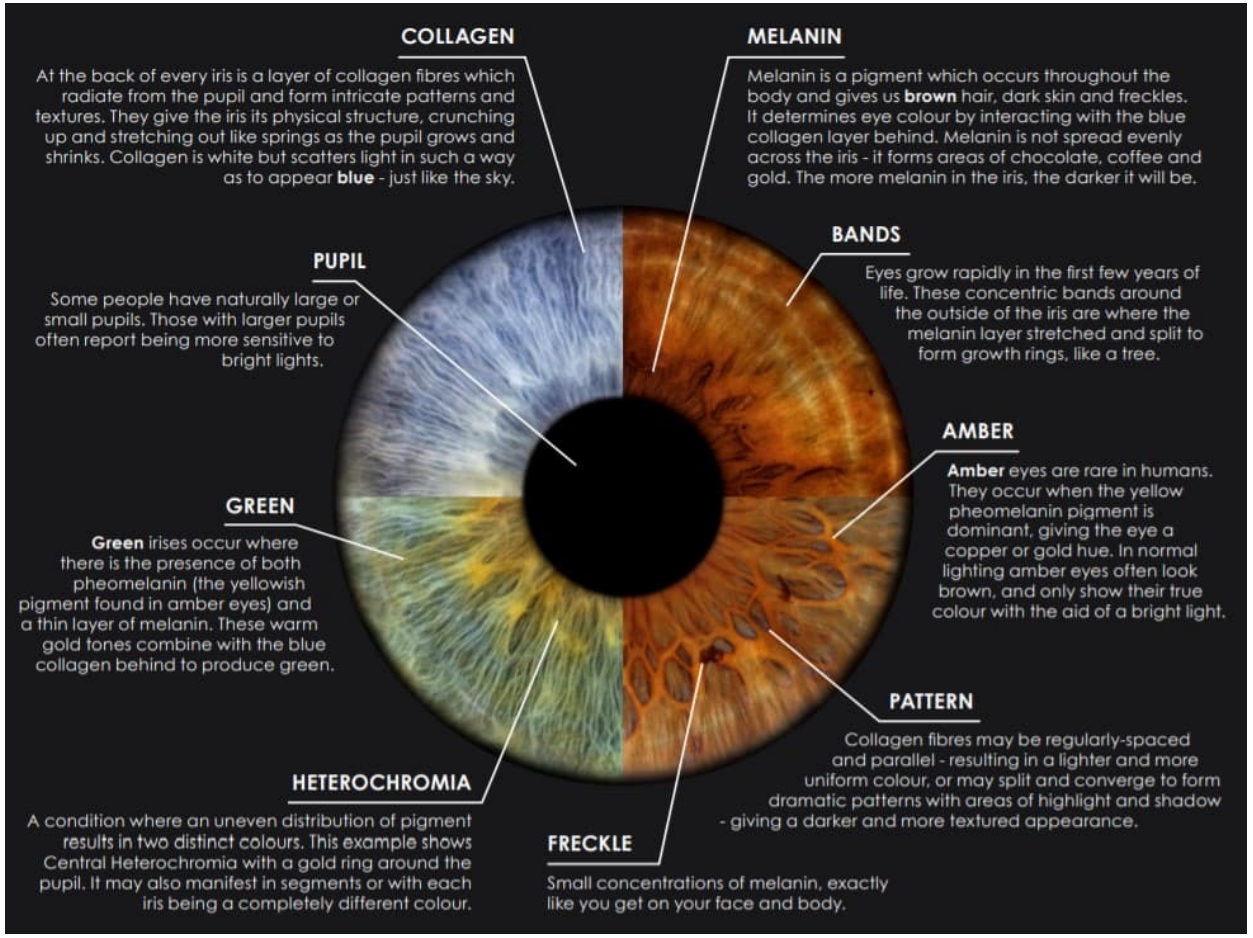
PLAIN ARCH

Plain Arch: The pattern starts on one side and slightly cascades in an upward direction.
Tented Arch: The arch lies in the center ridges and does not show a continuous arch.

IRIS PATTERNS

2,000 genes impact the development of each person's iris

Pigmented rings: Colored bands that are wide and wrapped around the pupil.
Crypts: Diamond shaped holes that vary in size, located throughout the iris.
Furrows: Pale lines that curve around the iris.



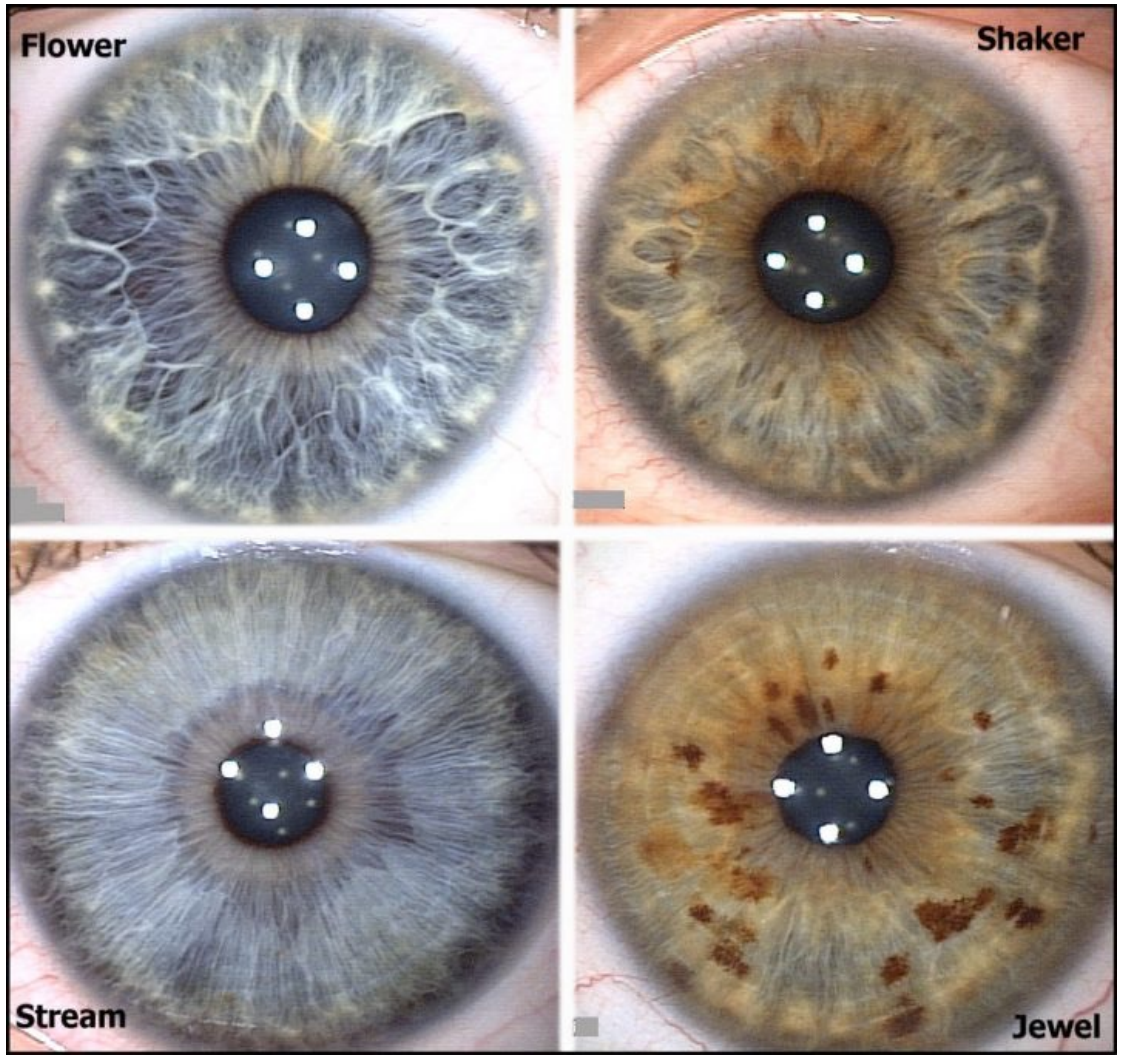
TYPES OF IRIS PATTERNS

Two primary structures are:

1. Jewel
2. Flower

Two secondary patterns that modify the first are:

1. Stream
2. Shaker.



"We forgot to back up our files, so we're asking everyone to remember everything they've typed during the past 10 days."


Thank
you!!