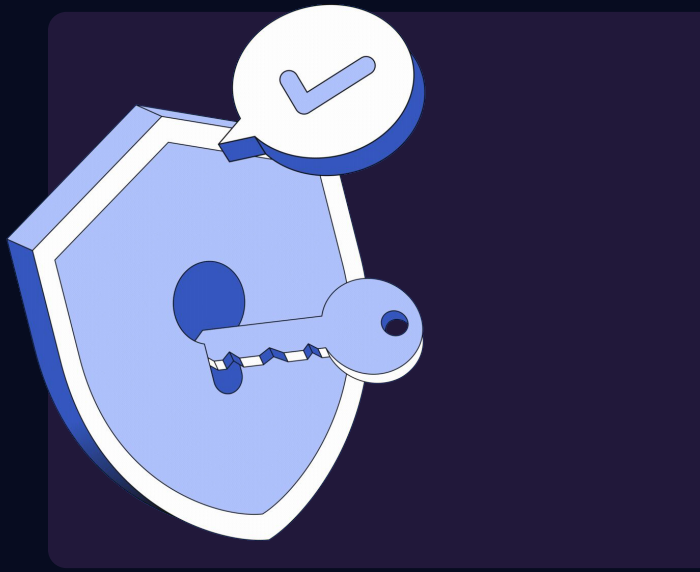
The Hidden Battlefield:

Cyberwarfare and its impact on the Digital World

Presented by: Hassan Al Achek



Who am i?

Hassan Al Achek

- Red Teamer
- CyberSecurity Researcher
- Offensive Cyber Security Engineer, Passionate about the inner workings of computers ;)
- Focused on web security, network security, reverse engineering, and malware analysis
- Attracted by state-sponsored threat actors 😉
- Moderator of Lebanon's largest cybersecurity community
- Instructor and penetration tester at Semicolon Academy
- Former Red Teamer at Covéa
- Ingénieur Civil des Mines (ICM) - École des Mines de Saint-Étienne
- Electrical and Telecommunications Engineer - Lebanese University

Agenda

01 Digital World

02 Lebanon's Position in the Digital World

03 Major Revolutions

04 Where are we know in the digital era?

05 What is Cyber Warfare?

06 How We Can Be Hacked?

Agenda

Digital World

- We all have at least one digital device in our homes!
- We interact with these devices and the digital network multiple times a day.
- Accessing information takes only seconds, making it incredibly easy to stay connected.

Digital World

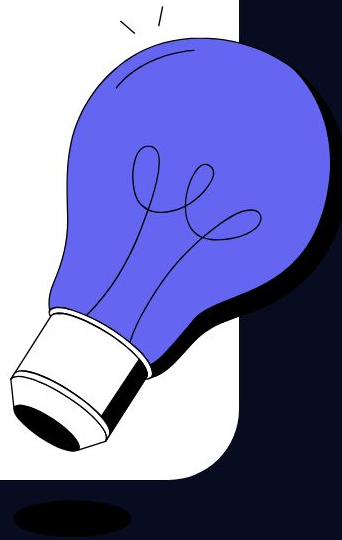
- We even have digital hardware on us without needing any surgery! 😉
- The use of IoT (Internet of Things) devices is increasing significantly worldwide.

02

Lebanon's Position in the Digital World

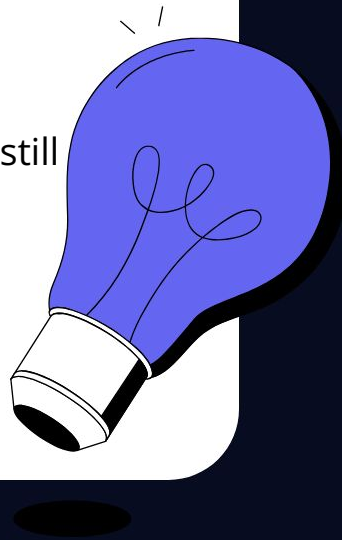
Lebanon's Position in the Digital World

- Not everyone has the luxury of owning a smart home or even using IoT devices in their homes.
- However, we have skilled, forward-thinking individuals who can make a significant impact in the digital world.



Lebanon's Position in the Digital World

- Unfortunately, government support for digital advancements is lacking, and our educational system falls short of preparing us adequately for these demands.
- Additionally, the economic crisis widens the gap between our digital development and that of other countries.
- Although we may not live in the most technologically advanced country, we still have a substantial attack surface.



03 Major Revolutions

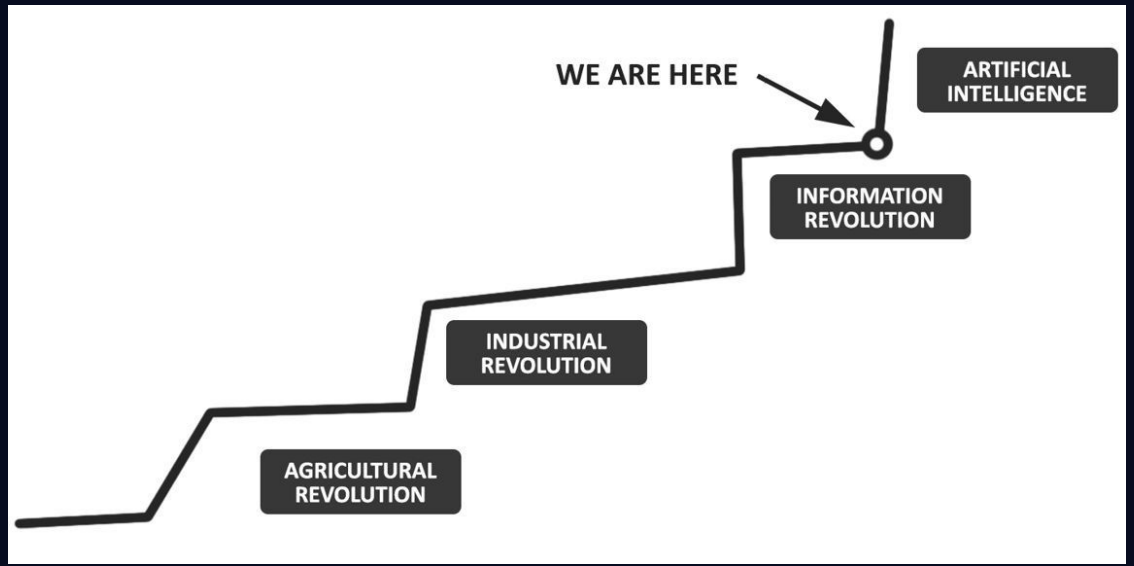
3) Major Revolutions

- Agricultural revolution
- Industrial revolution
- Information revolution
- Artificial intelligence

04 Where are we know in the digital era?

4) Where are we know in the digital era?

Chatbots, Tesla Optimus, Self driving cars, Image recognition and image processing, A large amount of information, Big data, Quantum computers, Nuclear facilities, Drones, War robots, Unmanned aerial vehicle



05 What is Cyber Warfare?

What is Cyber Warfare? | Public Perspectives

- Anything with an IP address will burst into flame
- Hackers could potentially disrupt the entire internet with just a few targeted actions.
- Adversaries seek to disable our communication systems to advance their agendas without resistance.
- They possess systems capable of launching automated cyberattacks against us.
- These attacks primarily target networks and essential facilities.
- We require advanced exploits to effectively engage in cyber warfare.
- ....

Strategy and Tactics

- A strategy is a plan of action designed to achieve a specific end goal in the future.
- Tactics are the specific steps and actions taken to reach your goal.

What is Cyber Warfare? | Public Perspectives

- Cyberwarfare is a series of strategic cyber attacks against a nation-state, causing it significant harm.

- This can range from disabling crucial computer systems to causing potential loss of life.

- It generally refers to actions taken by a nation or organization to infiltrate and attack the computer networks of countries or institutions, aiming to disrupt, damage, or dismantle critical infrastructure.

06

How We Can Be Hacked?

How We Can Be Hacked?

- Social Engineering (e.g., vishing, smishing, phishing, physical attacks, etc.)
- Past Data Breaches exposing sensitive information
- Malware Risks (especially from using cracked software)
- Weak Passwords (and absence of two-factor authentication)
- Excessive Sharing of personal or sensitive information
- Unpatched Systems (N-day vulnerabilities)
- Zero-Day Vulnerabilities exploited by attackers
- Supply Chain Attacks targeting external partners and vendors

Social Engineering

- Social Engineering (e.g., vishing, smishing, phishing, physical attacks, etc.)

Past Data Breaches

- Past Data Breaches exposing sensitive information

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

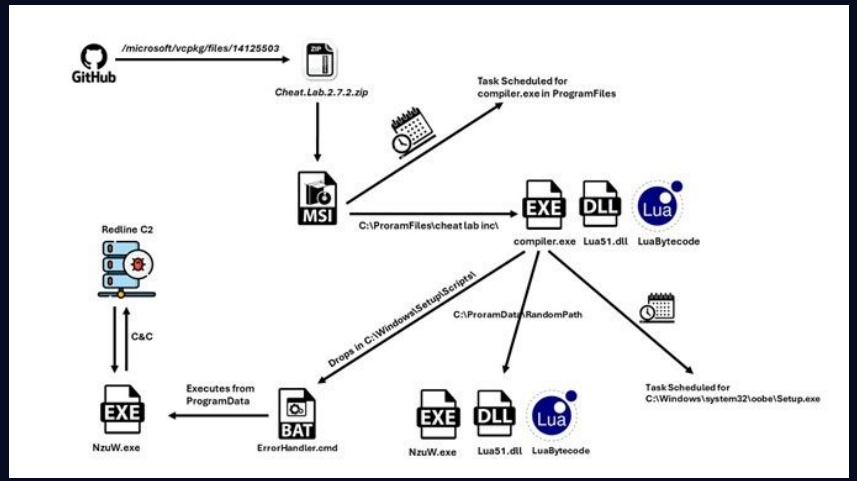
_IntelligenceX

Targeted Attacks

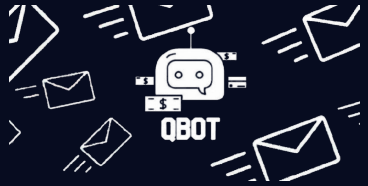
Dark Web Forums

Malware

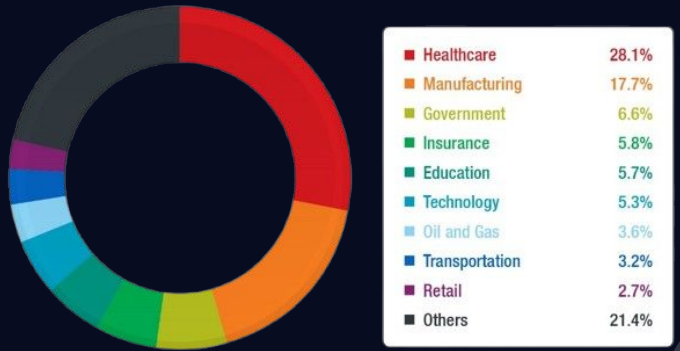
- Malware Risks (especially from using cracked software)



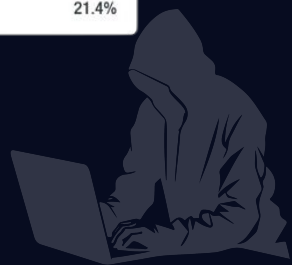
RedLine Infostealer



Qbot Infostealer



Trend Micro



Weak Passwords

- Weak Passwords (and absence of two-factor authentication)

Something You Know	Something You Have	Something You Are
Password	Smartphone (Authenticator App)	Fingerprint/Retina pattern
Pin	Hardware Device (Yubikey)	Face recognition

How We Can Be Hacked?

- Excessive Sharing of personal or sensitive information

“The United States Department of Justice has announced that a Ukrainian programmer has been charged, among other things, with computer and bank fraud in the United States.”

Raccoon Stealer Developer: Mark Sokolovsky

Vulnerabilities

- Unpatched Systems (N-day vulnerabilities)
- Zero-Day Vulnerabilities exploited by attackers

ETERNALBLUE

NATION-STATE

North Korean Hackers Exploited Chrome Zero-Day for Cryptocurrency Theft

The Lazarus APT created a deceptive website that exploited a Chrome zero-day to install malware and steal cryptocurrency.

Vulnerabilities

- Unpatched Systems (N-day vulnerabilities)
- Zero-Day Vulnerabilities exploited by attackers

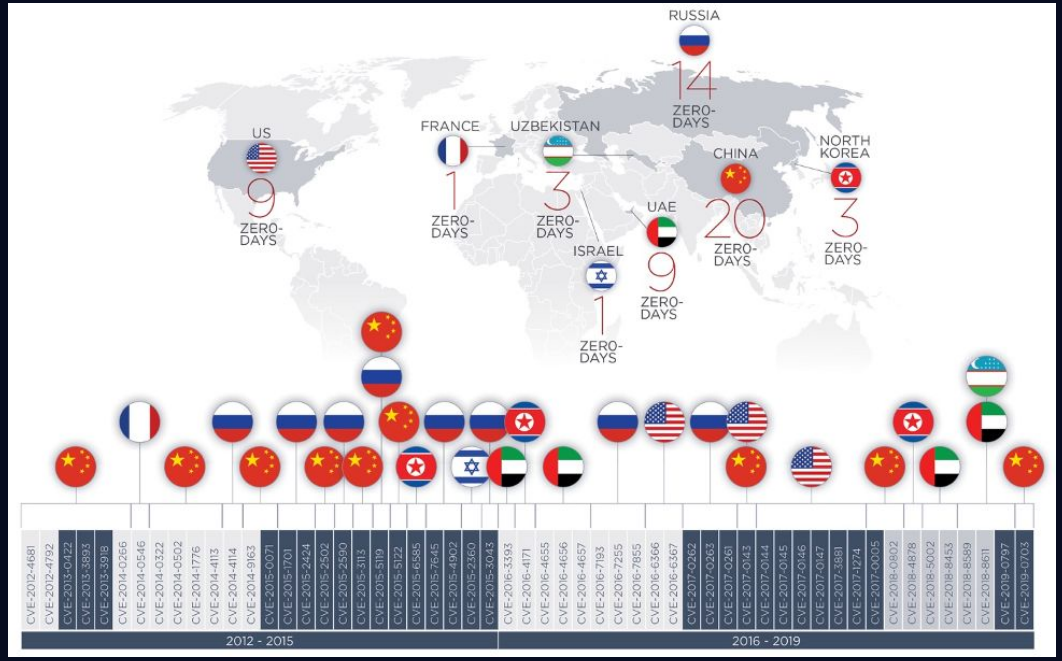
BLASTPASS

NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild

September 7, 2023

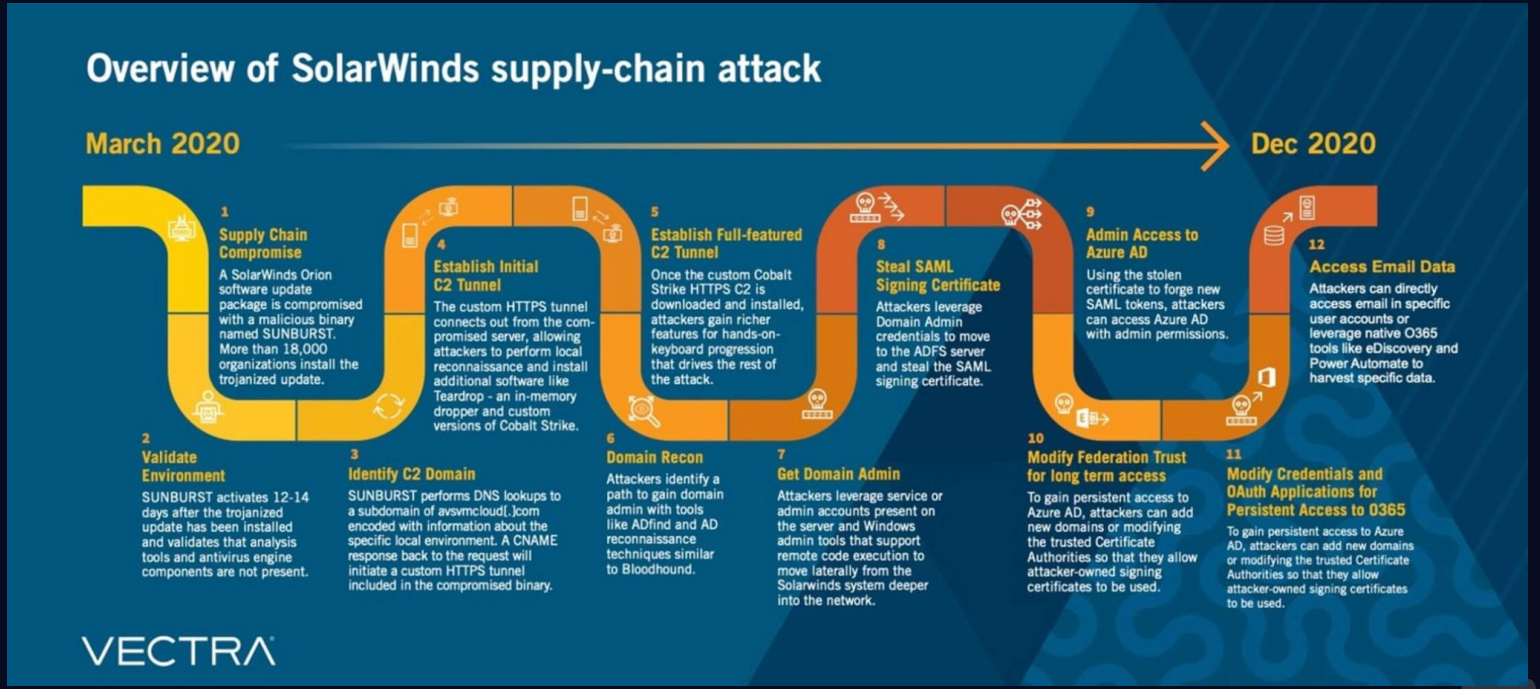
Vulnerabilities

- Unpatched Systems (N-day vulnerabilities)
- Zero-Day Vulnerabilities exploited by attackers



Supply Chain Attacks

- Supply Chain Attacks targeting external partners and vendors

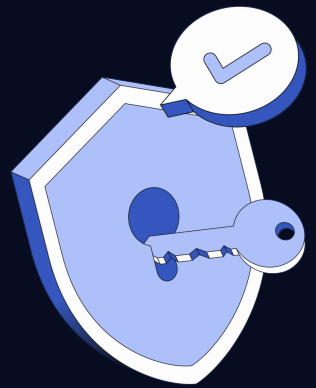


07

Key Players

Key Players: State-Sponsored Actors

- State-sponsored actors are government-supported groups engaged in cyber operations, often involving espionage, sabotage, and cyber attacks on other nations or entities to further national interests.



Key Players: State-Sponsored Actors | China

- China's goal is to overtake the United States as the world's foremost superpower by 2049.

- In 2003, a cyber operation known as "Titan Rain," conducted by the People's Liberation Army Unit 61398, targeted major U.S. defense and engineering entities, including Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, and NASA.

Key Players: State-Sponsored Actors | China

- Through these attacks, China acquired crucial research and development data for advanced fighter jets, dramatically cutting down the time and resources needed for independent research. This effort significantly reduced the technological gap between Chinese and U.S. military capabilities.

- From 2011 to 2012, the cyber group **Hidden Lynx** focused on targeting organizations linked to the U.S. Department of Defense and various sectors including information technology, aerospace, energy, and defense.

Key Players: State-Sponsored Actors | China

- Their goal was to infiltrate Bit9's (VMware Carbon Black) infrastructure to gather intelligence on its methods and steal private digital certificates.

- In the summer of 2013, Hidden Lynx initiated a multi-step operation called VOHO, which involved watering hole attacks. This operation compromised websites commonly visited by political activists, educators, and defense professionals, particularly in the Washington D.C. and Boston regions.

Key Players: State-Sponsored Actors | China

- Their goal was to infiltrate Bit9's infrastructure to gather intelligence on its methods and steal private digital certificates.

- In the summer of 2013, Hidden Lynx initiated a multi-step operation called VOHO, which involved watering hole attacks. This operation compromised websites commonly visited by political activists, educators, and defense professionals, particularly in the Washington D.C. and Boston regions.

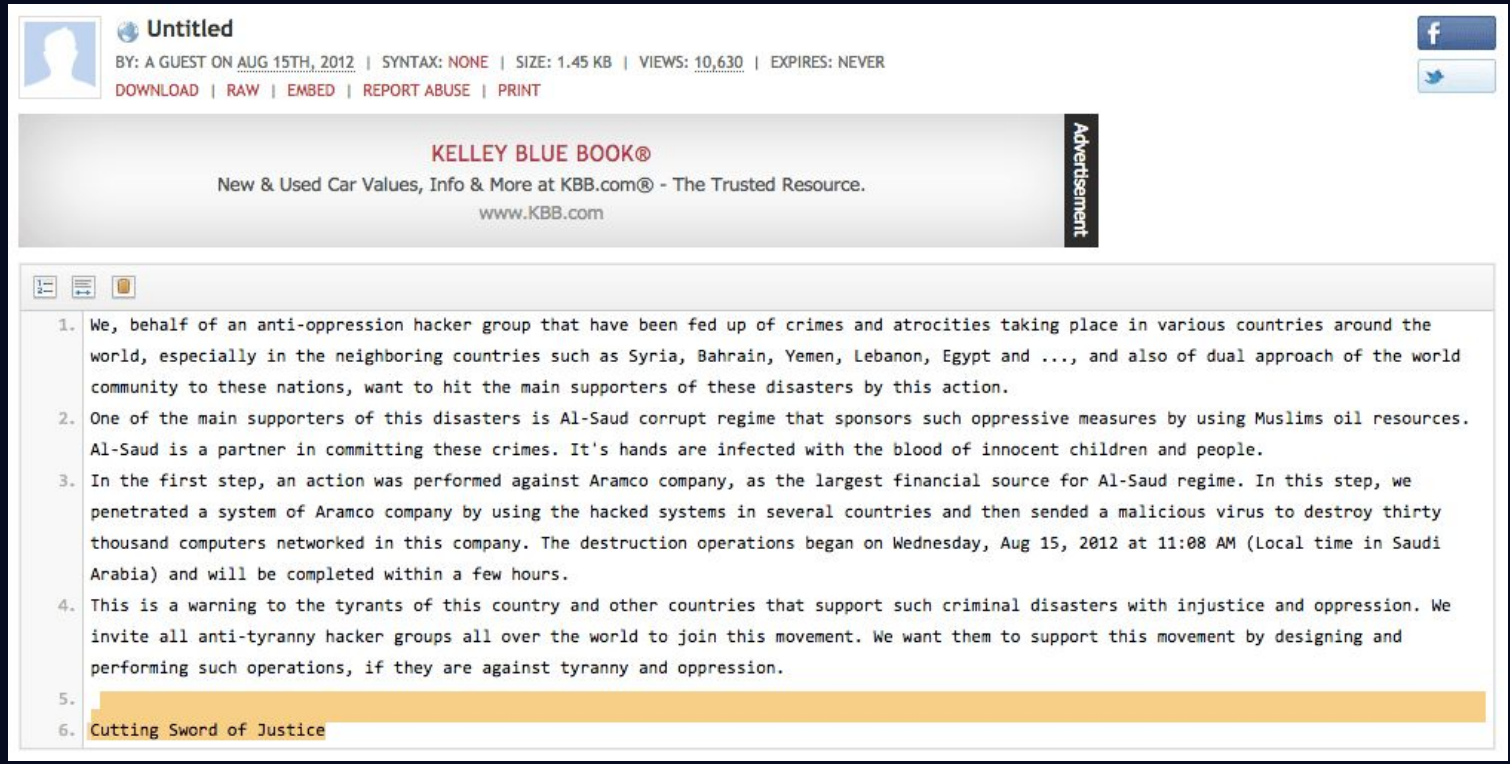
- APT1 and Mandiant LINK

Key Players: State-Sponsored Actors | China

Key Players: State-Sponsored Actors | Iran

- One of the most significant cyber warfare incidents attributed to Iran is the 2012 attack on Saudi Aramco, using the Shamoon virus (also known as Wiper)
- The Shamoon malware targeted Saudi Aramco’s computer network, aiming to disrupt the company's operations.
- 30,000 systems had been wiped of their data and replaced with the image of a burning American flag
- Saudi Aramco is one of the largest oil producers globally.

Key Players: State-Sponsored Actors | Iran



Untitled

BY: A GUEST ON AUG 15TH, 2012 | SYNTAX: NONE | SIZE: 1.45 KB | VIEWS: 10,630 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

1. We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.
2. One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.
3. In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.
4. This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.
5.
6. Cutting Sword of Justice

Key Players: State-Sponsored Actors | USA/israel

- In 2010, the Fuel Enrichment Plant (FEP) in Natanz, Iran, experienced significant disturbances as concrete walls rumbled and shook.

- This event caused the nuclear centrifuges to spin uncontrollably, damaging systems and sensitive equipment vital for uranium enrichment.

Key Players: State-Sponsored Actors | USA/israel

- The developers of the Stuxnet malware possessed extensive knowledge of the uranium enrichment process and the specific systems used at the Natanz plant. Stuxnet was designed to disrupt or modify the speed of the centrifuges, ultimately leading to their failure.

Key Players: State-Sponsored Actors | USA/israel

4 zero-days!

Key Players: State-Sponsored Actors | North Korea

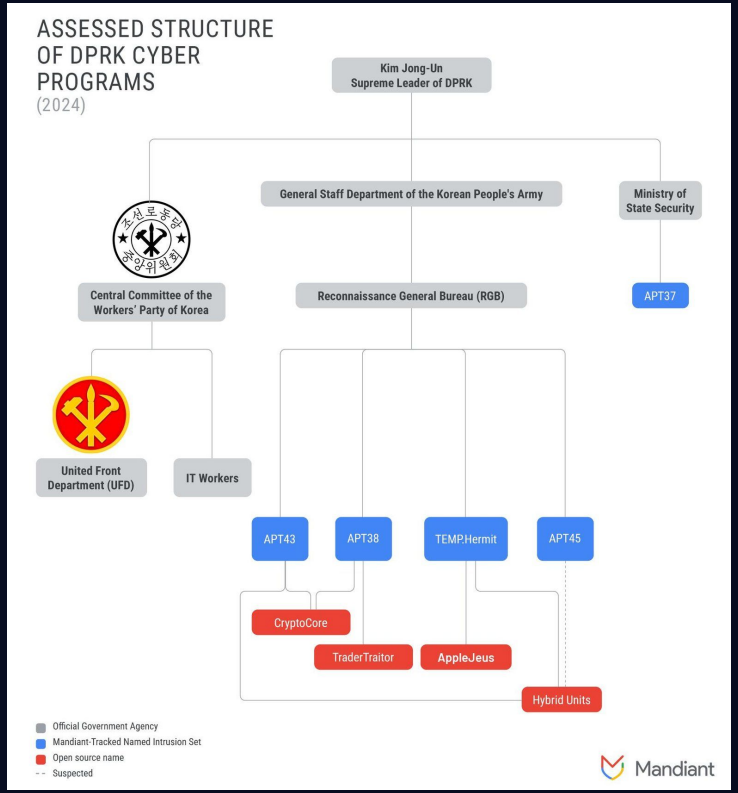
- **Operation Blockbuster (Lazarus Group):** One of the most significant and widely known cyber warfare incidents attributed to North Korea is the 2014 Sony Pictures hack, which demonstrated North Korea's willingness to use cyberattacks to achieve political and strategic objectives.

- The goal was to prevent the release of the film, which North Korea found offensive.

- The malware not only exfiltrated data but also wiped hard drives and rendered computers unusable.

- The company spent months recovering, lost an estimated $15 million

Key Players: State-Sponsored Actors | North Korea



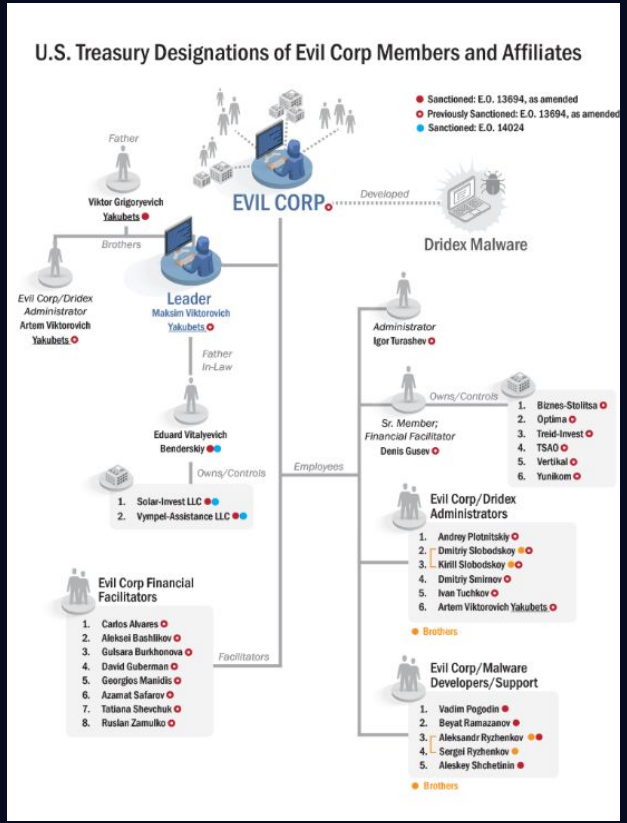
Key Players: Ransomware Gangs

- **REvil:** is infamous for its double extortion model, where they encrypt data and threaten to leak it publicly. They offer ransomware-as-a-service (RaaS).

- **LockBit:** LockBit specializes in highly automated attacks, making it one of the fastest-spreading ransomware strains.

- **Conti:** is known for aggressively targeting healthcare and critical infrastructure sectors, particularly during the COVID-19 pandemic. They also use a double-extortion model and have a dedicated data leak site.

Key Players: Ransomware Gangs



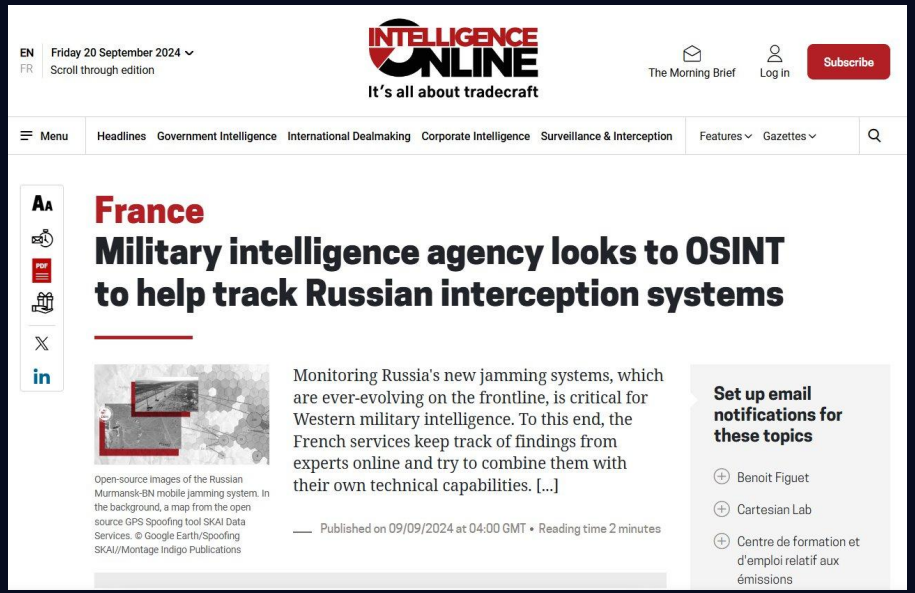
08 We are the Product!

We are the Product!

- Sharing is caring, but please don’t share too much!
- Open-source intelligence (OSINT)
- Signals intelligence (SIGINT)
- Psychological Operations (PSYOP)

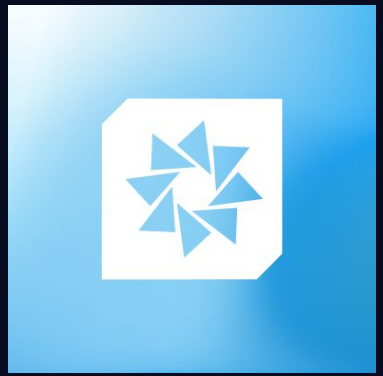
We are the Product!

- Sharing is caring, but please don’t share too much!
- Open-source intelligence (OSINT)



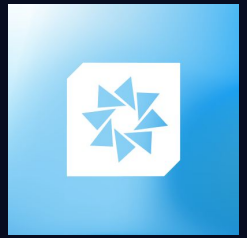
Zero-day Marketplace

- NSO Group
- Zerodium
- Operation Zero



Zero-day Marketplace

- NSO Group
- Zerodium
- Operation Zero



What about Lebanon?

What about Lebanon?

- Pagers Attack.
- Can I still be tracked if I turned off my GPS?
- If they destroy communication, they destroy their visibility.
- If we have skilled people, why don’t we carry out a cyber attack?
- AI?

Message for you

- We can’t escape the new world, but we can adapt and change!
- Please pay attention to your studies, study more, and don't rely solely on learning a specific technology.
- It all starts with you. Begin by protecting yourself, and you’ll be making a positive change

Message to Universities

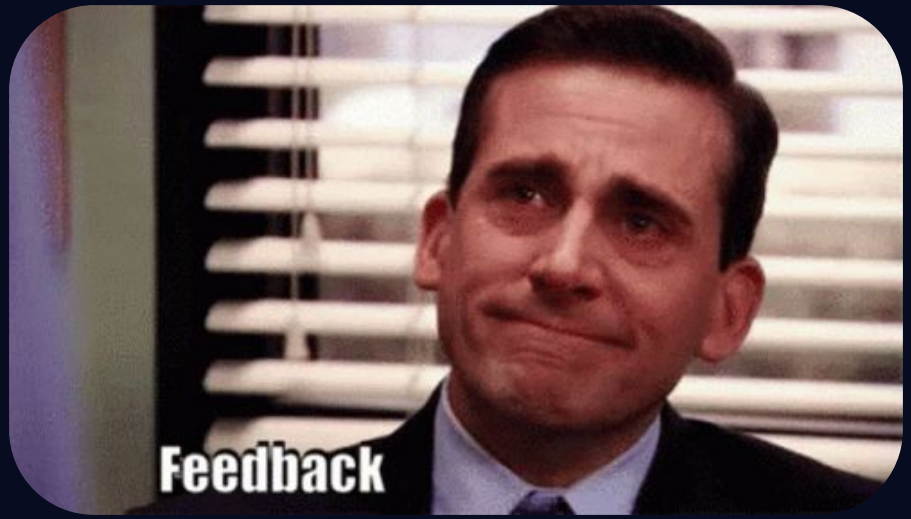
- Please keep the students motivated.
- Adapt to the modern world!
- Encourage research and try to benefit from our talents.

Message to organizations

- Security is not just about compliance
- Security is not unnecessary!
- Even if our countries don’t force you to protect our data, you should do it anyway!
- Hire talented people!

Questions?

Seeking Feedback



REACH ME!

Email: hassanalachek@hotmail.com

LinkedIn: in/hassan-al-achek

Social media: @hassanalachek

WTM Cyber Security Community