



APPLIED CYBERSECURITY

*Open Source Technologies for Real-Time Data
Analytics*

Imre Lendák, PhD, Associate Professor

Cybersecurity intro outline



- Cybersecurity incidents
- Key definitions
- Threat types & sources
- Challenges
- Vulnerabilities
- Security monitoring data





Positions in Cybersecurity

- Chief Information Security Officer (CISO)
 - Cybersecurity Manager
 - **Cybersecurity Architect**
 - Security Auditor
 - **Security Analyst – often data-intensive!**
 - **Penetration tester**
 - Incident response manager
 - **Digital forensic expert**
-
- Positions marked with bold font require thorough understanding of the topics and tools discussed!

CYBER INCIDENTS

High profile incidents...



Stuxnet (2010)



Ukraine (2015)



Technology

Hackers caused power cut in western Ukraine - US

12 January 2016 | Technology

Share



Ukraine has been forced to turn to back-up power sources in recent months following a spate of power cuts

Stuxnet sources



- Alex Gibney, “Zero Days”, documentary, 2016
- Kim Zetter, “Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon”, Broadway Books, September 2015
- David Kushner, “The Real Story of Stuxnet”, IEEE Spectrum, February 2013,
<http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>

Ukraine 2015 & 2016 literature



- SANS, “Analysis of the Cyber Attack on the Ukrainian Power Grid”, Report, March 2016
- ICS-CERT, “Cyber-Attack Against Ukrainian Critical Infrastructure”,
- National Cybersecurity and Communications Integration Center (NCCIC), “Seven Strategies to Defend ICSs”, December 2015
- Wikipedia, “December 2015 Ukraine power grid cyber attack”,
- Kim Zetter (2016). "Everything We Know About Ukraine's Power Plant Hack". Wired. January 20th, 2016.
- Kim Zetter (2016). "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid". Wired. March 3rd, 2016.
- Hackernews (2016), “Hackers Suspected of Causing Second Power Outage in Ukraine”, <http://thehackernews.com/2016/12/power-outage-ukraine.html>

...more high profile incidents...



▼ Mirai's trail of disruption in 2016



Mirai botnet (2016) sources

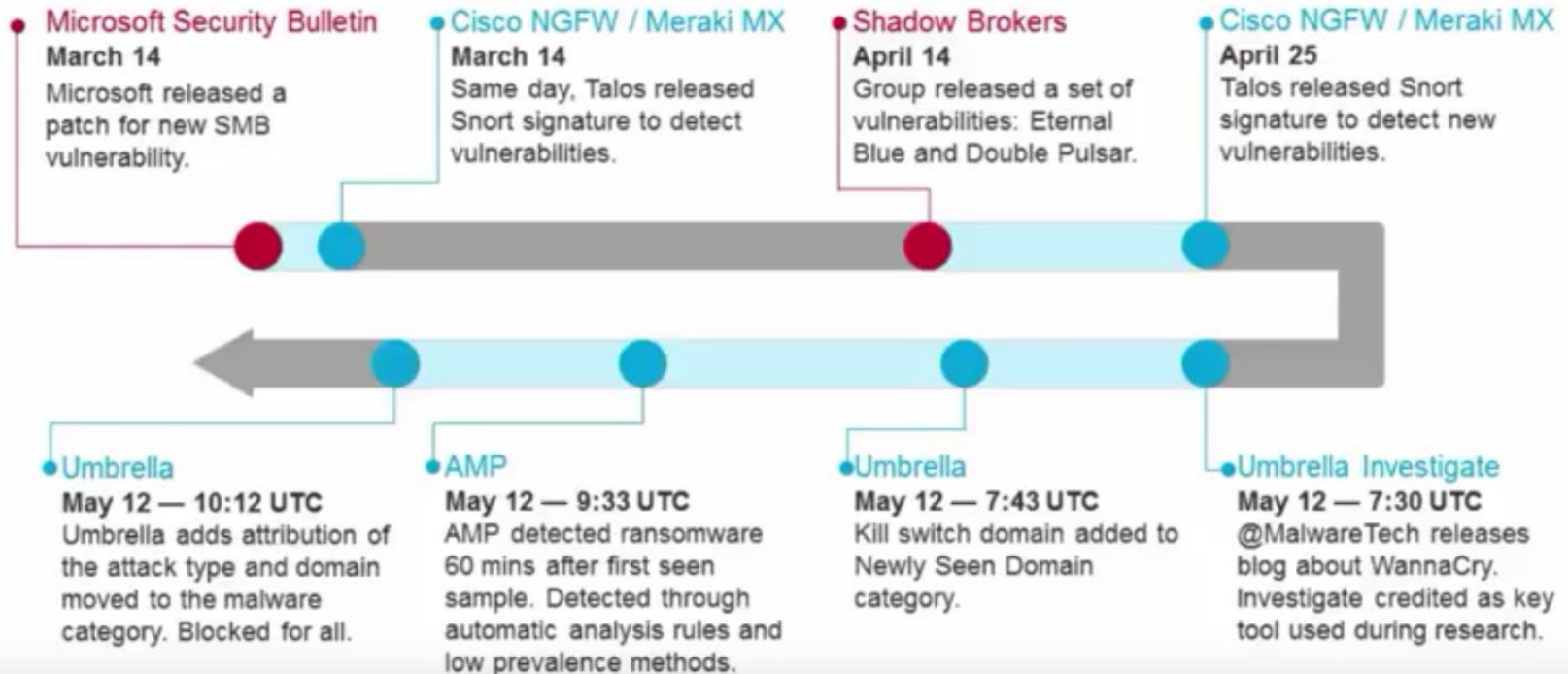
- Lily Hay Newman, "What We Know About Friday's Massive East Coast Internet Outage". Wired.
- Nate Lanxon, Jeremy Kahn & Joshua Brustein, "The Possible Vendetta Behind the East Coast Web Slowdown", Bloomberg.com
- Darrell Etherington & Kate Conger, "Many sites including Twitter, Shopify and Spotify suffering outage". TechCrunch.
- Wikipedia, "2016 Dyn cyberattack"
- Wikipedia, "Mirai (malware)"

...more high profile incidents...



Anatomy of the attacks: WannaCry ransomware & Google OAuth phishing

Timeline of WannaCry Ransomware



Cisco Umbrella

43:26 / 52:46

CC YouTube

WannaCry (2017) sources

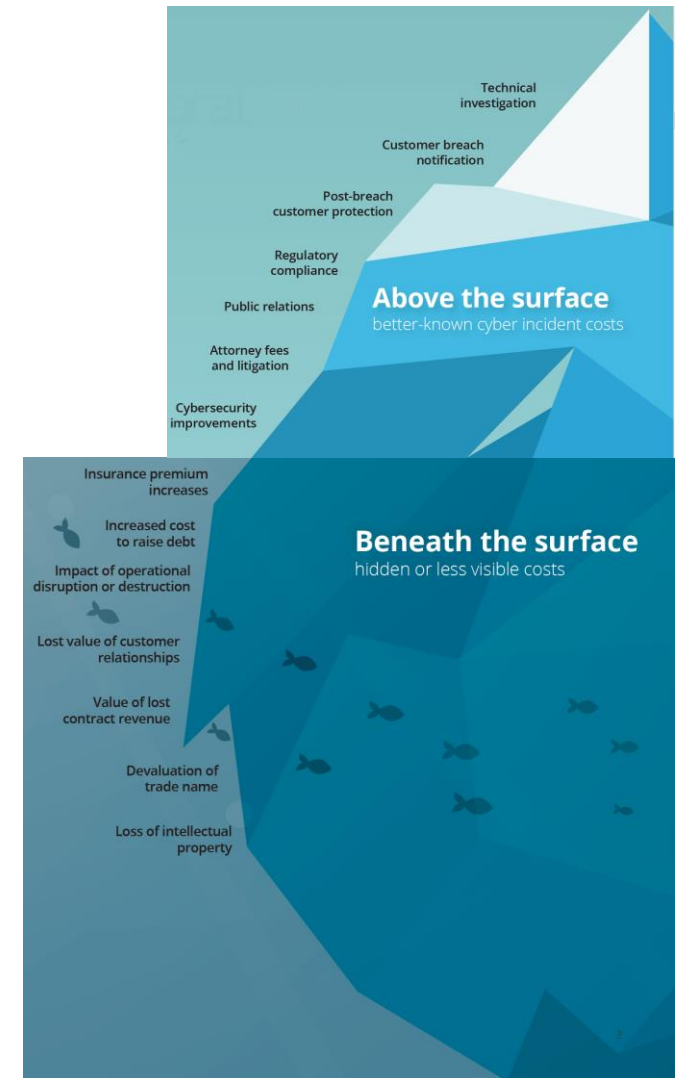


- Thomas P. Bossert, "It's Official: North Korea Is Behind WannaCry", The Wall Street Journal.
- Thomas Fox-Brewster, "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak". Forbes.
- Victoria Woollaston, "Wanna Decryptor: what is the 'atom bomb of ransomware' behind the NHS attack?". Wired UK.
- Wikipedia, "WannaCry ransomware attack"

Cyberattack impact

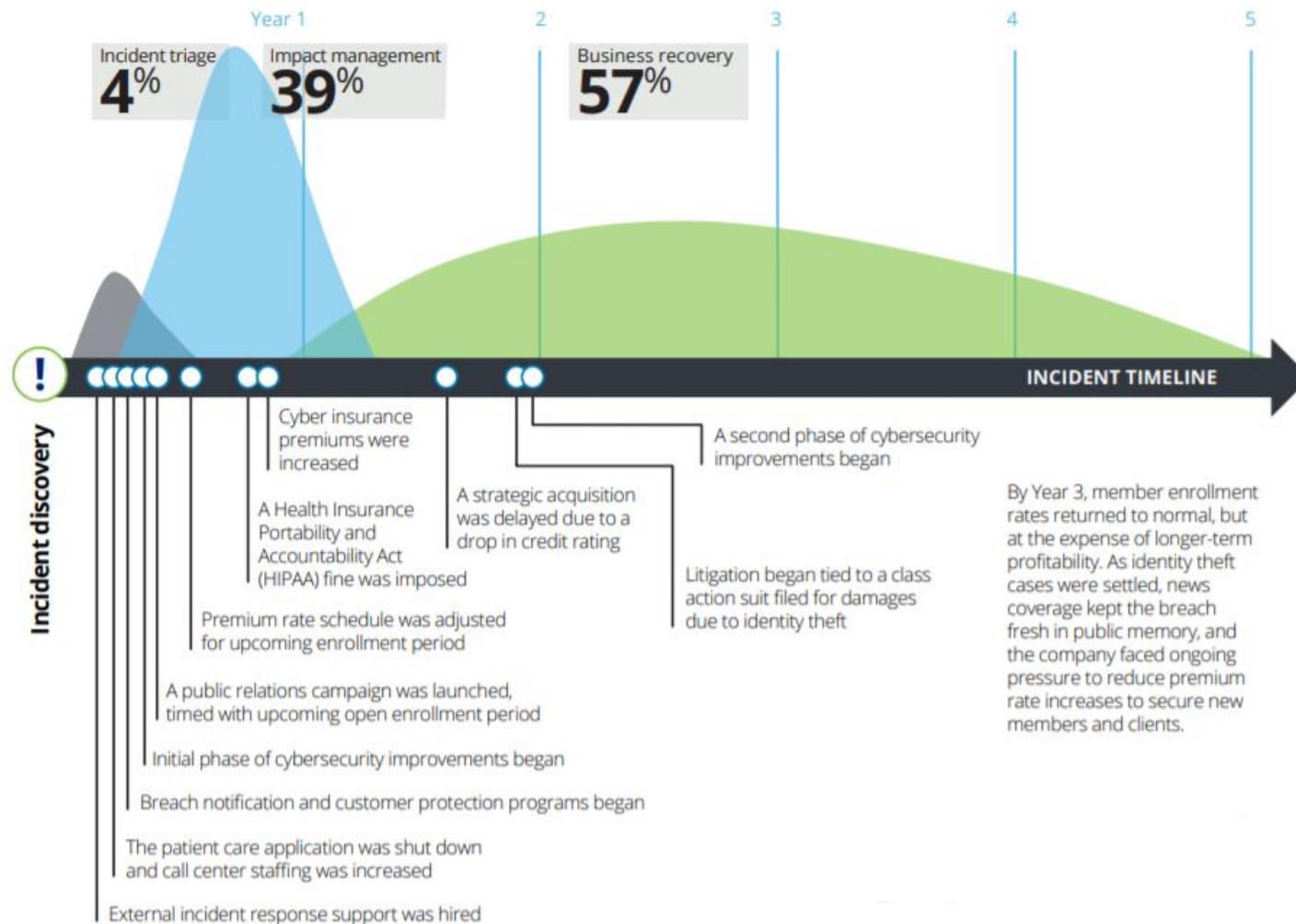


- Above the surface 7/14
 - Technical investigation
 - Customer breach notification
 - Post-breach customer protection
 - Regulatory compliance
 - Public relations
 - Attorney fees and litigation
 - Cyber Security improvements
- Underneath the surface 7/14
 - Service price increase
 - Increased cost to raise debt, i.e. borrow money
 - Impact of operational disruption or destruction
 - Lost value of customer relationships
 - Value of lost contract revenue
 - Devaluation of trade name
 - Loss of intellectual property



<https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf>

Cyber incident timeline



<https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf>

Open source tools & technologies

CYBERSECURITY DEFINED

Common information security goals

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation
- Privacy



<https://www.comtact.co.uk/blog/what-is-the-cia-triad>

Cybersecurity elements



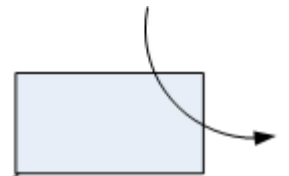
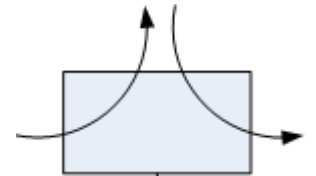
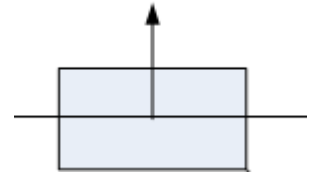
- **Threat** – anything that has the potential to cause serious harm to an information system
- **Vulnerability** – a flaw (often unintentional) in a system that can leave it open to attack
- **Attack** – attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset – usually by exploiting a vulnerability
- **Risk** – a combination of the likelihood and impact of a security incident, e.g. attack or vulnerability-related outage
- **Security controls** – safeguards or countermeasures to avoid, detect, counteract, or minimize risks to physical property, information, computer systems, or other assets
- **Trust** – degree of trust end users have in/about a system

- Information systems have physical and electronic **access points** (PAP & EAP)
 - Physical: gates, doors, windows, human resources, mobile devices (e.g. laptops, mobiles, USB drives), switches, routers
 - Electronic: website, remote access, software running on physical access points
- Potential **locations** of vulnerabilities: all access points
- Most **frequent locations** of vulnerabilities (2019):
 - Human resources, e.g. employees, subcontractors, visitors
 - Publicly available electronic access points, e.g. websites
 - Mobile devices, e.g. USB drives, laptops

THREAT TYPES & SOURCES

Threat types

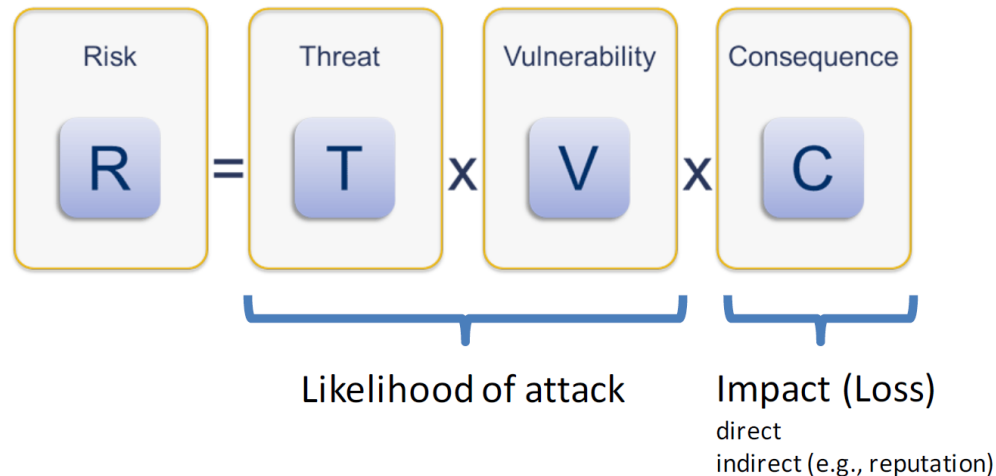
- **Interception** – an unauthorized entity gains access to services and/or data, e.g. spyware
- **Interruption** – service or data becomes unavailable due to corruption or cyber attack, e.g. Distributed Denial of Service (DDoS)
- **Modification** – unauthorized change in data and/or services → deviation from specification, e.g. unwanted change of middleware
- **Fabrication** – generate unwanted data, services or requests which would not exist during normal operation, e.g. add entries to a shadow (password) file



Risk in cyberspace

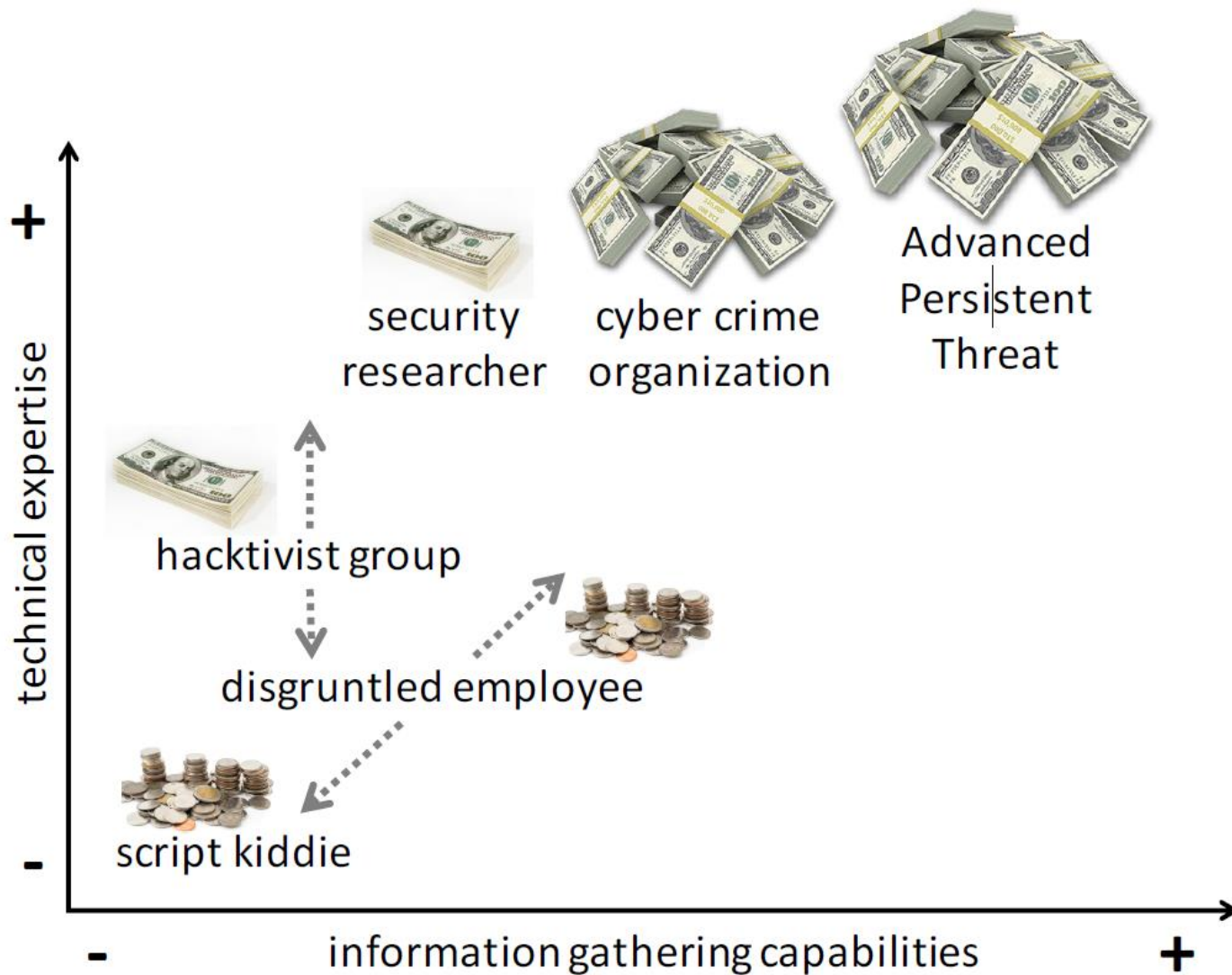


- Risk in cyberspace is a composition of:
 - **Threat** - a product of both intention and capability
 - **Vulnerability** - depends on the characteristics of the target and the probability that an attempted attack will be successful
 - **Consequences** - political, social, economic or environmental damages or costs caused by a successful attack



* Computer Security course content, CrySyS Lab, BME, Budapest, Hungary

Threat sources



* Computer Security course content, CrySyS Lab, BME, Budapest, Hungary

Cyber Kill Chain model (steps)



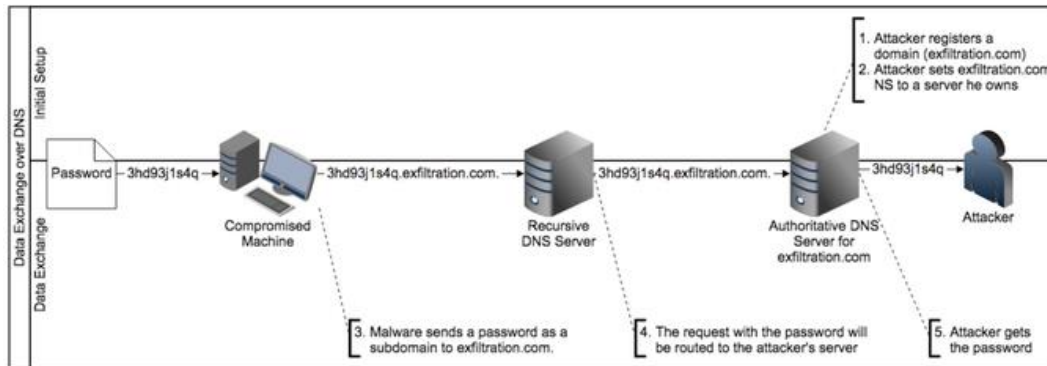
- **Reconnaissance** – analyze all access points and find vulnerability of the target, e.g. company, person
- **Weaponization** – create an attack tool/process to exploit the vulnerability
- **Delivery** – deliver the ‘weapon’
- **Exploitation** – initiate the attack
- **Installation** – install tools necessary to reach objectives
- **Command-and-Control** – maintain persistence in the breached system
- **Actions on Objectives** – perform the planned actions, e.g. exfiltrate data, interrupt normal business activities

CYBERSECURITY THREAT SOURCES

- A **criminal organization** or an **adversarial nation state** executes a zero day attack against a financial institution's public web server
 - www.examplebank.hu is accessed by the attackers
- The attackers pivot (i.e. move laterally inside the bank's information system) into the internal network
- The attackers gain access to the database server without getting noticed
- The attackers want to exfiltrate data about the bank's customers through DNS by installing appropriate custom scripts

Internal threats

- Mick is a malicious insider within a hedge fund investing large amounts for investors, i.e. bank employee with bad intentions
- Mick wants to exfiltrate the fund's investment strategies to a competitor and get paid for that
- Mick receives malware on a USB drive, inserts it in his workstations and the malware infects the system
- The malware exfiltrates trade secrets and receives commands via DNS queries/responses



<https://blogs.akamai.com/2017/09/introduction-to-dns-data-exfiltration.html>

VULNERABILITIES

Cybersecurity vulnerabilities



- Social engineering
- Software bugs
- Malware
- Misused DNS
- Misused BGP
- ...
- The above is not a definite list!

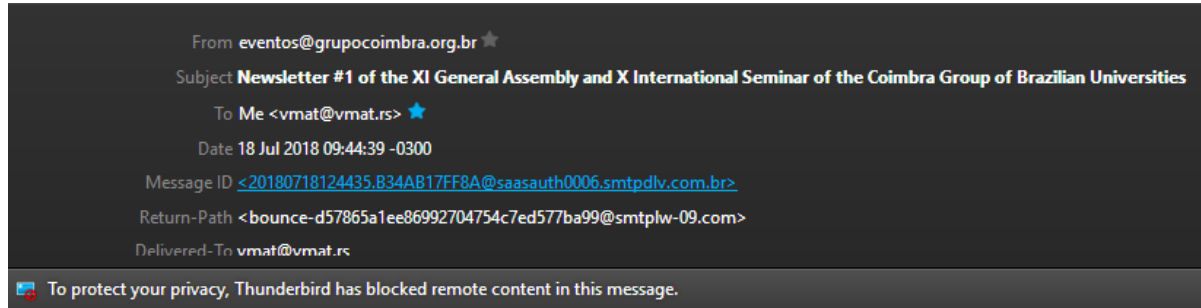


Social engineering



- **DEF:** Social engineering is psychological manipulation of human resources into performing actions or revealing confidential information
 - **Interception:** either at the physical or electronic access points, e.g. voice or video recording devices, installed keyloggers or other spyware
 - **Shoulder surfing:** often seen in films, involves the attacker coming near the victim and visually capturing sensitive information
 - **Impersonation:** pose as a colleague, system administrator or top manager and convince the victim to perform the desired actions.
 - **Phishing:** a subtype of impersonation, involves the attacker impersonating a trusted service and asking for secrets

Social engineering – CEO fraud



GCUB Logo

Brasilia, July 18, 2018

Your Magnificence
Imre Lendák
President
Hungarian Academic Council of Vojvodina

Dear Sir/Madam,

Please receive the best compliments from the Coimbra Group of Brazilian Universities (CGBU) and the Hungarian Rectors' Conference (HRC).

In this email, you will find attached the **Newsletter #1 of the XI General Assembly and X International Seminar of the Coimbra Group of Brazilian Universities (CGBU)**.

Please note that the deadline for hotel reservations without penalty for cancellation or change of date is **July 23, 2018**. Check below some suggestions of hotels with special rates:

Mercure Budapest Korona (<https://bit.ly/2KURJhl>)****

Software bugs & backdoors



- **DEF:** Software bugs are unintentional mistakes in source code which cause services to produce incorrect or unexpected results, or to behave in unintended ways
 - Might cause system crashes, i.e. interruption
 - Might allow attackers remote code execution (RCE), command injection (CI) or other unauthorized actions
- **DEF:** Backdoors are physical or electronic access points allowing system administrators or attackers to gain access to a system
 - E.g. hard-coded sysadmin password for accessing systems during remote maintenance

Simple

- Self-replication
 - Virus
 - Worm – zero human interaction!
- (Usually) no self-replication
 - Trojan
 - Backdoor
 - Spyware
 - Logical bomb

Complex

- Botnet
- Ransomware
- Cryptomining malware

Malware – Ransomware

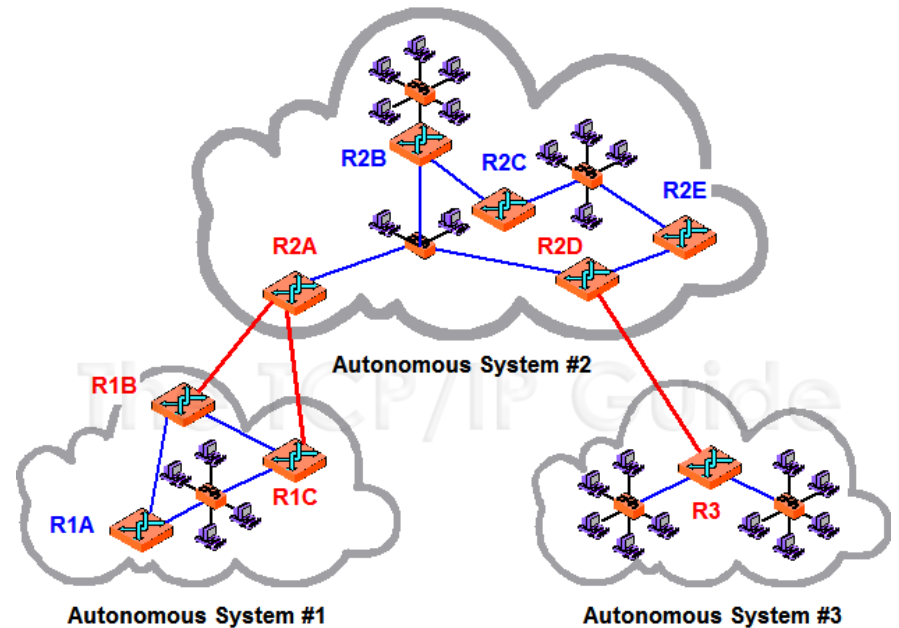


- Ransomware is a form of malware that encrypts a victim's files.
- Ransomware steps:
 1. Phishing emails with malicious attachments or links pointing to malicious web pages.
 2. Admin-level access is gained on the victim's computer.
 3. The ransomware encrypts the user's files, e.g. PDF, DOC, PNG, etc.
 4. The (decryption) key is uploaded to a remote command & control server (C&C) controlled by the attacker.
 5. The attacker then demands a ransom from the victim to restore access to the data upon payment.

- DNS is one of the basic protocols underpinning the Internet
 - It resolves domain names by finding Internet Protocol (IP) addresses based on symbolic domain names, e.g. finds the IP address corresponding to www.inf.elte.hu
 - Not strictly monitored by most organizations (!)
- DNS for **data exfiltration**
 - Resolve 2317540194857019487.attackerdomain.com – split & encode data in the least significant part of the domain name
- DNS **tunnelling** in botnets
 - Use of DNS response messages to send commands to bots (who first need to send DNS queries to the attacker's server(s))
- DNS **cache poisoning**
 - Redirect users to malicious websites
- DNS **amplification and reflection** attack
 - DNS request with spoofed IP address sent to (multiple) open DNS resolvers
→ Distributed Denial of Service (DDoS)

BGP hijacking

- **DEF:** An autonomous system (AS) is a collection of resources under the control of a single administrative entity with common, clearly defined routing policy to the internet.
 - Large Internet Service Providers
- **DEF:** Border Gateway Protocol (BGP) is an exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS).
 - Type: path-vector routing protocol
→ routers exchange path vectors between source & destination AS.
- **DEF:** BGP hijacking constitutes the takeover of IP address ranges by corrupting BGP routing tables, usually by advertising unauthorized routes.



http://www.tcpipguide.com/free/t_OverviewOfKeyRoutingProtocolConceptsArchitecturesP-2.htm

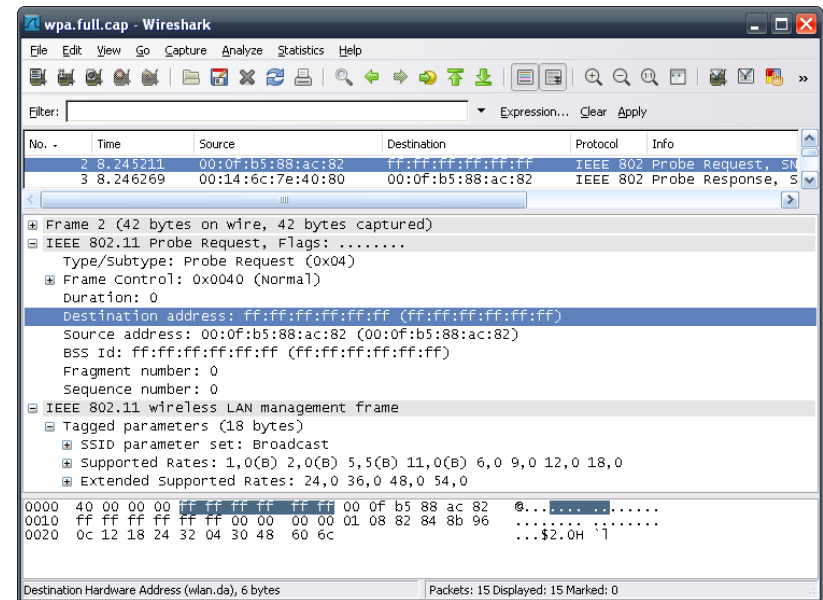
MONITORING DATA

- **Security data feeds** – published by cybersecurity organizations (e.g. national Computer Emergency Response Team – CERT), or companies, might be industry-specific
- **Transaction data** – any element of an information system records an event which can have security relevance
- **Session data** – capture aggregated data about the communication sessions occurring among entities in an information system
- **(Full) Packet Capture** – capture every piece of data exchanged between entities in an information system

Full packet capture data

















- **DEF:** Packet capture is a technique in which data packets are captured and recorded at a specific point in a network.
 - Possible capture locations: routers, switches, servers, workstations
 - Captured packets can be retained and analyzed.
 - In **full packet capture** every data packet is captured and recorded
- Packet capture **challenges:**
 - Storage capacity
 - Realtime analytics capabilities
 - Encryption, i.e. what if the captured data is encrypted?
 - Filtering, i.e. how to filter data?



Session data



- In session data the exchanged data is aggregated for a time period or the entire duration of a communication session between two entities
 - Example: Cisco Netflow falls into this category

Src IP	Dst IP	Appln	Src Port	Dst Port	Protocol	DSCP	TCP FLAGS ?	Flow Rate	Traffic	Packets	NextHop	FNFB NbarApp
 192.168.10.1	192.168.13.1	compressnet	2	169	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	15.80.39.28	-
 192.168.10.1	192.168.13.1	compressnet	2	564	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	190.23.69.213	-
 192.168.10.1	192.168.13.1	compressnet	2	741	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	95.55.61.159	-
 192.168.10.1	192.168.13.1	compressnet	281	2	TCP	AF12	UAP SF	1.0 Kbps	1.0 KB	2	223.191.78.79	-
 192.168.10.1	192.168.13.1	compressnet	165	3	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	64.15.70.93	-
 192.168.10.1	192.168.13.1	compressnet	424	3	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	149.191.44.148	-
 192.168.10.1	192.168.13.1	compressnet	822	3	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	73.7.175.22	-
 192.168.10.1	192.168.13.1	rje	800	5	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	74.157.168.220	-
 192.168.10.1	192.168.13.1	discard	9	714	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	1.209.56.6	-
 192.168.10.1	192.168.13.1	daytime	13	252	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	232.237.195.100	-
 192.168.10.1	192.168.13.1	daytime	960	13	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	22.88.95.248	-
 192.168.10.1	192.168.13.1	msh	18	116	TCP	AF12	UAP SF	1.0 Kbps	1.0 KB	2	81.203.252.131	-
 192.168.10.1	192.168.13.1	msh	18	735	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	18.50.17.126	-
 192.168.10.1	192.168.13.1	ftp-data	20	513	TCP	AF12	UAP SF	0 Kbps	1.0 KB	2	240.7.195.4	-

Transaction data



- Physical access point (PAP) transaction logs
 - Security gate/door access
 - Physical access to a network router
 - Example: security card swiped to cross into a higher security zone
- Electronic access point (EAP) transaction logs
 - Operating system logs, e.g. system file changes
 - Application logs, e.g. data warehouse transactions, web server/proxy, DNS server, email server, authentication-authorization-accounting (AAA) server
 - Example: a syslog entry generated by an authentication service recording a user logging in via mobile banking app on Android 7 from at 02:17 CET from Malaysia



Security alerts



- **DEF:** Security alert data is generated by the security controls when anomalous, unwanted actions are detected in an information system
- Sources of security alerts at the **physical access points**:
 - Human guards or (regular) employees
 - Physical security controls, e.g. security doors, motion sensors
- Sources of security alerts at the **electronic access points**:
 - Endpoint security solutions: firewall, IDS/IPS, anti-malware
 - Network/system-level security solutions: edge firewall, edge IDS/IPS, security analytics solutions (e.g. packet capture analysis)
- Security data feeds (next slide!) might raise alerts as well

Security data feeds



- Advisories about the latest threats
- Provide valuable advance notification about the latest threats in near real-time
- Can be exchanged on the following levels:
 - Between nation states
 - Between cybersecurity companies
 - Between actors in a specific sector, e.g. electric power system operators
- Examples:
 - AlienVault OTX → provides an API
 - Secjuice, Feed Your SIEM With Free Threat Intelligence Feeds, <https://www.secjuice.com/threat-intelligence-siem-free/>

Summary



- Major cybersecurity incidents
- Definitions:
 - Threat types & sources
 - Challenges
 - Vulnerabilities
- Data types in security analytics
- What is next? → Security analytics, i.e. tools & technologies in cybersecurity





Thank you for your attention!