Presentation

Cyberwar

Topics

-What does cyberwar mean?

-Which methods and tools are used for attack?

-Who attacks and why?

-How can attackers be attributed?

-How can cyber systems be protected?

-What is the role of Smart Industry (Industry 4.0)?

Cyberwar definition

-Cyberwar (cyber warfare) is the military conflict with the means of the information technology

-Integrated and supportive element of coventional military activities

-Interaction between man and machine

-Computer / digital technology as a tool

-Offensive and defensive aspects: to protect the own systems and to ensure the freedom of action

-In case of military conflicts combined cyber and physical attacks

Cyberwar practice

-Misleading air defense systems (2007)

-Sabotage of uranium centrifuges (2010)

-Infiltration and spoofing of military drones (2011/2012)

-Attack on electricity infrastructre (Saglam Study 2014/Ukraine 2015)

-Cyberwar against Islamic State (2016)

-Expansion of Cyberwar capabilities (GB, F, Russian Science Squadrons, Germany CNO unit...)

-Deployment of Russian cyber soldiers in Venezuela (2019)

Espionage and Cyberwar

-Cyber attacks require intrusion into digital devices
Hacker > Intrusion > Malware >Action > bidirectional communication between infected device and attacker

-Aims are spionage, manipulation, sabotage, theft/ransom and misuse

-Espionage and cyberwar are closely related, because most attack types require prior intrusion

-As in warfare, cyber activities can support conventional espionage, but cannot replace the physical presence of agents

Cyber attacks

Cuurently leading methods:

- Emails with malignant attachments or links (Phishing) combined with Social Engineering
- Exploits (vulnerabilities, backdoors and bugdoors)
- Infected Apps and websites
- Insider threats most dangerous
- Botnets: use of infected digital devices as ‚bots‘, which can flood and paralyze computers or networks with inquiries and data (Distributed Denial of Service DDoS).

Cyber weapons

Codes for attack, intrusion, espionage and manipulation of target computers/devices which may have self-control of spreading and deactivation.

Conventional: Virus (implanted into computers),
Trojans (report information from target computer to attacker) und
Worms (which actively spread in networks)

Modern: beachheads, modular, variable, tailor-made, regular updates, ‚stealthy' = difficult to detect and to remove, obfuscation and false flags

Offensive Cyber weapons:
misleading signals (GPS, dummies, 20 kHz-commands), botnets, logic bombs, text bombs, Wiper Malware, Bricking, Ransomware, Fuzzing

Offensive Cyber weapons

What?	Used for…?
Misleading signals	GPS Spoofing: Misleading of drones, ships etc.
	Dummies for misdirection of autonomous systems, new form of camouflage painting with large low-contrast pixels
	>20 kHz-commands: Ultrasound commands for remote manipulation of home assistant systems
Botnets	Flooding with inquiries and data can paralyze computers or networks
Logic bombs	Malicious programs, which become active only after a certain time or specific action
Text bombs	Difficult-to-interpret symbols overloading the chip and causing a crash
Wiper Malware	Deletion programs that delete files from the infected computer
Bricking	Programs that overwrite important control files with zeros on smart devices, rendering the device unusable
Ransomware	Lock screens for which ransom money has to be paid to get an unlock code: increasing use of destructive ransomware, i.e. the screen can not be unlocked anymore
Fuzzing	Random commands to chips, which cause via design gaps a data access/release or even turn off the chips permanently (halt and catch fire)
	=> digital 'rescue shot' is technically possible, potential danger of 'shutdown' by opponents in combat

Expansion of attack targets

Past	Presence
Computer	Equipment: Mouse, Printer, Router, USB-Sticks Smartphones/iPhones Smart home: Internet of Things Infrastructure: Access to national servers, tapping of Internet nodes, redirection and copying of traffic, tapping deep-sea cables, attacks on clouds, 5G towers
Software	Hardware (Fuzzing), Firmware, Add-on Chips
Hacking/Virus	Interdiction, theft, ‚pre-installed viruses‘
User	Data collection in stock („everything from everybody“)
	Higher levels: account holders > bank > interbanking system
	Attacks on third vendors, suppliers and maintenance systems, help desks and contract staff

Attackers (I)

Hackers are (still) mostly male, young, mostly working in organizations and not (anymore) as stand-alone actors

Sectors:

- State with civil authorities, military and intelligence services
- Private sector with cybersecurity companies and cyberweapons producers
- Science (research, universities)
- Cybercriminals (Darknet, hacker forums, black market)
- Politically active hacktivists

Attackers (II)

Advanced Persistent Threat (APT)

Classic definition:

long-term attacking groups with defined techniques, tactics and programs (TTPs)

Modern definition:

A project group within an intelligence service that develops and applies its techniques, tactics, and programs (TTPs) as well as the targets of attack along the operational goals

Leading APTs

Country	Attributions by leading cyber security organizations
Russia	APT28/FancyBears/Sofacy/Strontium/Sednit (GRU)
	APT 29/Cozy Bears/Dukes (FSB oder SWR)
	Waterbug/Turla/Ouroburos/Venomous Bear/Krypton Gruppe (FSB)
	Sandworm/Quedagh (GRU)
	Energetic Bear/Dragonfly (to be clarified)
	Trisis/Triton/Temp Veles (Central Scientific Research Institute of Chemistry and Mechanics)
China (ca. 20 APTs)	APT 1/Comment Group (PLA)
	APT 10/Cloud Hopper (MSS)
USA	Equation Group (NSA)
	Longhorn/The Lamberts (CIA)
North Korea	Lazarus-Group and affiliations
Israel	Unit 8200 (IDF)

The above mentioned states do not comment or deny these attributions.

Details and sources in: Cyberwar-methods and practice 2019

Attribution: Who did it?

- Infrastructure: IP addresses, domain names and providers are registered (search with WHOIS etc.), infrastructures and names are often recycled
- Hackers: act in forums, limited number of aliases
- Malware: typically embedded in other activities, copying therefore risky
- Conventional espionage / counterintelligence: e.g. buy IP addresses, infiltrate surveillance cameras, hack into the adversary system, and so on...

Cyber defense

Level	Approach
User	Regular updates, careful file handling, virus protection, spam filters, secure passwords, 2-factor authentication with password and a physical device, data encryption, firewalls (control of network access) Research: Key pressing duration and strength and mouse movement patterns as unique individual identifiers
Organisations	Whitelisting, segmented networks, Need to know principle, four-eyes-principle for admins
Security firms	Threat Intelligence, Intrusion Detection, Penetration Testing, Honeypots, Sandbox Analysis, Data/Knowledge combination
Cooperations	Intelligence (e.g. 5-/9-/14-eyes), Police (Europol/FBI), European Cybersecurity (ENISA), Cooperations for Critical Infrastructures, Charter of Trust and so on…
Legal	Criminal and liability regulations, safety standards
Technology	e.g. DDoS-defense: redirect data traffic, involve provider, switching off own IP, blocking foreign IP (geoblocking), slowing down (tarpitting) One-way street technologies: campus networks (data out, but not in), data diodes (in, but not out)

Smart Industry

- Smart Industry (Industry 4.0): digital (networked, computerized, intelligent), with remote maintenance and control systems (Industrial Control Systems ICS/Supervisory Control and Data Acquisition SCADA)
- Subarea of smart technologies (smart home, smart cities, smart grid/smart meter, smart cars usw.) and of the Internet of Things IoT
- A key element will be the 5G technology
- Exponential growth of devices, interfaces, updates, variants
- Networked = Open Systems: Monitoring, Wartung, Updates, Backdoors
- Low password protection / Unnecessary network connections: Shodan

Smart Industry Attacks

Basics:

- Infiltration > lateral movement > escalation > manipulation
- Development of the attack takes years (including tests) and requires the cooperation of computer scientists and engineers
- Hacking alone is not enough, you also have to know the system (otherwise discovery, accidental sabotage)
- Usually only spying, not sabotaging (in cybercrime, however, ransomware and botnets)
- The primary goal is the (industry) espionage, the cyberwar an option

Important Attacks I

Stuxnet (2005-2010): originally valves, then frequence modulation of uranium centrifuges by targeted attack on Simatic S7-SPS and prozessvisualisation WinCC

Still unclear: Shamon attack on Aramco (2012), wiper attack on Iran (2012)

Cloud Hopper (2006-2016): attack on Managed Service Providers MSPs (Clouds, IT Services, Help Desks etc.), in addition on technology firms and the US Navy

Lazarus-Gruppe (2012-heute): since years use of wipers as logic bombs or to eliminate traces, use of desctructive ransomware (WannaCry) 2017

Triton/Trisis/Temp.Veles (2017): Malware Triton/Trisis against Schneider Electrics Triconex Safety Instrumented System (SIS) in Saudi-Arabia, manipulation of emergency shutdowns

Dragonfly/Energetic Bear: infected ICS Provider with Malware Havex for surveillance and manipulation of ICS/SCADA-Systems (ca. 2000 cases)/
Wolf Creek-incident 2017 with spearphishing using fake CVs

Important Attacks II

Sandworm/Quedagh (since 2011): Modified multi-function Malware BlackEnergy3 against Human-Machine-Interfaces HMI

2015 Power failures in the Ukraine by disconnecting power connections and Telephone Denial of Service (TDoS)-attacks to block alert hotlines and Wipers (Killdisk)

2016 Industroyer-Attack Wrong IEC-104 protocol orders to a single infiltrated transmission substation led to a power outage in Kiev

2017 Petya/Not-Petya/Moonraker-Petya Use of NSA exploits for destructive ransomware

2018 VPN-Filter reboot-resistant IoT-Malware for network devices for surveillance of SCADA protocols with bricking option

Conclusions

Collaboration between organizations is critical to detection, attribution and defense of cyber attacks.

The cybersecurity trend has shifted from the sole analysis of attacks and malicious software to an active counterintelligence, so that the leading APTs were identified.

After a long-term dominance of the perspective of the cyberspace as a virtual world, security experts are gaining a more and more physical understanding: who controls the devices and the cables, also controls the data in them.

The fear of retaliation explains the huge gap between espionage activities and damaging attacks on the smart industry, even though the technical possibilities for far-reaching attacks are constantly increasing.

Literature

2010-2019 Online-Paper Cyberwar-methods and practice (English Version)

http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-methods-and-practice.pdf