Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

Title : MOVIES (Black hat and Live Free)

Lab : 14

Blackhat :
Overview
The film focuses on a dangerous cyber criminal threatening critical infrastructure systems. After attacks disable a Chinese nuclear power plant and disrupt Chicago stock trading, the FBI teams up with expert hacker Nicholas Hathaway (Chris Hemsworth) in pursuit.

Cybersecurity Concepts : (A lot is used in this movie than Die hard)
Infrastructure Protection - The attacker targets vulnerable systems managing power grids, transit networks, air control systems, military weapons, etc that enable public and economic functioning. Disrupting them risks safety, causes major financial impacts, and can be an act of cyberterrorism. Protecting them is crucial but they present diverse technological risks spanning access control, patch management, IoT devices embedded in machines, human-machine interfaces and more at enterprise IT and system control, especially in this movie the power grid is attacked using the pump which is exploited through the PLC(Programmable Logic Controllers).

Sponsored Cyber Threats - The attacks are attributed to North Korean state sponsorship but the true perpetrator turns out to be a hidden extremist Chinese hacktivist group financially backed by elite sources. Nation-state and state-adjacent actors can conduct the most dangerous cyber campaigns given their mix of substantial resources and capabilities coupled with ideological, economic or political motivations.

Malware Design and Deployment - Unique self-duplicating malware provides the attacker remote access to air-gapped critical systems, demonstrating sophisticated coding skills and an understanding of advanced operating system internals to bypass security mechanisms. Delivery relies on infected USB devices - a common and successful technique. Malware analysis and reverse engineering are key defenses. This malicious USB is used in multiple times in the movie, especially gaining access over the bank to transfer 74 million dollars from the Chinese extremist.

Network Intrusion and Lateral Movement - The malware allows secretly persisting within networks for reconnaissance and lateral traversal between nodes to reach protected classified data and control systems by pivoting through related organizations and supply chain partners. Detecting lateral adversary movement represents a challenge for defenders despite firewalls and network segmentation.

Insider Threat and Access Management - Social manipulation provides initial network footholds. The attacker clones an industry expert's RFID badge for

physical access and copies fingerprints from a manipulated female asset for biometric system access. Insider clearance enabled the most crucial system breaches. Personnel security and access deprovisioning are vital.

Operational Security - The hacking campaign relies on anti-forensics erasing logs and malware, proxy bouncing communications, burner devices, anonymizing tools, stealth malware variants and disciplined tradecraft - forcing the FBI and allies into difficult digital and physical manhunts. Adversaries conceal operations security better than ever before.

Hacking Power Systems - After territorial hacks between US and China, power grids are compromised to disable safety systems, crosstalk industrial controls, and manipulate indicators to hide sabotage before catastrophic failure. System integrity validation, manual overrides, redundancy and resilience address such scenarios.

Cybersecurity Tools Depicted
SCADA System Malware - Custom malware specifically targets power plant, transit system and other industrial control system networks by masquerading as a routine software update through infected USB insertion. This provides the initial foothold even within air-gapped critical networks.

Remote Access Trojans - Advanced malware allows secretly persisting within compromised networks and workstations for reconnaissance, credential theft and lateral traversal between nodes to reach protected classified data and control systems by pivoting through related organizations and supply chain partner networks.

Hypervisor Bootkits - Bootkit malware variants install a stealth virtual machine-based hypervisor below the base OS to gain deepest root privilege on infected systems while concealing the adversary OS from host detection. This permits total system monitoring and control.

Windows Exploit Development - Weaponized privilege escalation exploits are developed for initial network infiltration by reverse engineering patched Microsoft binaries to discover useful software vulnerabilities, then reliably exploiting these undisclosed flaws through code injection attacks.

Injected Manipulation Code - Malware injects falsified sensor readings and control commands directly into programmable logic controllers managing transit systems, aircraft flight engines, weapons platforms and nuclear reactors. This could trigger catastrophic failure when unsafe thresholds are crossed.

Backdoor & Rootkit Malware - Backdoors allow covert remote access to compromised machines for uploading additional malware. Rootkit components conceal these tools deep in the kernel and filesystem to prevent detection and removal. Combined they are very powerful.

Wiki Code Hosting - An anonymous, encrypted wiki allows decentralized collaboration between geographically dispersed criminal team members contributing code, tools, data, notes etc. This supports sophisticated hacking campaigns.

Supply Chain Poisoning - Compromising trusted software developers allows inserting malware that spreads via authentic updates even to air-gapped secure networks. Investigating third party trusts and updating code integrity checks provides some defense.

Domain Generation Algorithms - DGA pseudo-random domain generation hinders sinkholing all command and control domains at once, requiring ongoing botnet analysis and registry blacklisting to sever C2 infrastructure links used to control infected machines globally.

Active Directory Privilege Escalation - Pass-the-Hash and Pass-the-Ticket attacks leverage valid credentials extracted from memory or the authentication process to escalate privileges horizontally within Microsoft Active Directory domains.

Infrastructure Cyber Sabotage - After accessing critical system endpoints, timed firmware hacks manipulate PLCs to crosstalk systems and override safeties precisely when unsafe failure thresholds are crossed, causing catastrophic destruction.

Bitcoin Money Laundering - Stolen millions are laundered through Monero, Bitcoin tumblers, changers, gambling sites and other dark web financial tools to prevent tracking. But blockchain analysis of poorly anonymized transfers provides clues, as virtual asset exchanges still require real verified identities.
Wireless Sensor Hacking - Out-of-band wireless access via compromised radio communication firmware allows manipulating reading from critical measurement endpoints like reactor core sensors to hide emerging unsafe states.

Advanced Social Engineering - Highly personalized phishing messages convince targets to insert infected drives, enable remote access, or install mobile surveillanceware. Well executed human hacking breaks down technical controls.

Bootable Kali Linux - Portable bootable hacking focused Linux distro allows easy use of advanced penetration tools from any operation site using minimal hardware footprint. Variants are hardened against forensics and surveillance.

In the climax, Hathaway relies on his blackhat skills to infiltrate the extremist group through its dark web communications and ultimately track down the hidden Chinese hackers, averting their next high casualty attack by turning part of their malware against them. This underscores reformed criminal cooperators applying unorthodox skills can uniquely counter emerging threats. The film concludes by warning expanded national cyber readiness and resilience is crucial as threat tools and capabilities accelerate.

They showcase Blackwidow used by NSA and how Hathaway gets the credentials through social engineering attack is really cool. Especially he inject the malicious code to activate the keylogger to find the keys that were pressed.

I personally learnt a lot of tools and techniques and studied a lot of them and it was fun, especially in this movie they didn’t show any graphics to cover up, instead they tried to showcase the real life scenario of above tools as possible and some of them we discussed in our class.

Live free or die hard :

Overview
The film focuses on cyberterrorist Thomas Gabriel who conducts an advanced persistent threat campaign against US critical infrastructure and financial systems. His goal is to expose national vulnerabilities and undermine public confidence through an attack known as the "Fire Sale" which hacks key utilities, transports and data systems to cause mass disruption.
Veteran detective John McClane becomes embroiled in the plot when his daughter Lucy's boyfriend turns out to be one of Gabriel's hackers. McClane must team up with Lucy and use his old school physical resilience to take down Gabriel's technological capabilities threatening infrastructure and innocent lives.

Key Cybersecurity Concepts
Advanced Persistent Threat (APT) - Gabriel exhibits sophisticated capabilities matching an APT group, including funding, organization, technical skills, and intentional targeting of vulnerable systems for political ends over an extended period. His access allows slowly stealing and corrupting data over time.

Zero-Day Exploits - Gabriel uses undisclosed IT vulnerabilities and specialized code sequences allowing undetected system access and escalation of privileges. Exploiting these zero-days permits penetrating networks, stealing data, and inserting malware.

Malware Usage - Malicious software is central to Gabriel's attack, including remote access trojans, worms, spyware, viruses, and ransomware. Variants target industrial control and financial transfer systems. Methods include phishing emails, drive-by downloads, and compromising third-party suppliers.

Protecting Critical Infrastructure - Gabriel seeks to control utilities, communication networks, transportation systems, and core government data systems that operate infrastructure sectors vital for public health and economic functioning. Their disruption threatens life and can cripple response capabilities.

Cyber Deception - Deceptive techniques used include digital impersonation, data manipulation, surveillance, false identities, and sophisticated social engineering to manipulate perceptions and trick people into giving access, information, or carrying out desired actions.

Securing Connected Networks - Gabriel exploits interconnected IT systems controlling physical infrastructure, accessing through one network vulnerable segments controlling power grids, pipeline controls, airport systems etc. This demonstrates risks from linked managed services.

Insider Threats - Gabriel recruits an insider to help design custom malware, showing that not just external attackers but malicious insiders with approved access can present threats through abusing privileges and accessing sensitive data.

Key Tools and Techniques :
SCADA System Hacking - Gabriel uses specialized malware tailored to corrupt supervisory control and data acquisition (SCADA) systems managing critical infrastructure sectors. This demonstrates increased cyber physical risks.

Botnets and C2 Servers - Gabriel likely uses a botnet, a network of compromised machines with remote command and control servers, to distribute attacks and disguise his origin point by relaying through zombie machines. Botnets enable scalable automated threats.

VPN and Encryption - Gabriel masks location and activity through virtual private networks, cryptography, anonymizing tools, and dark web access to conceal his group's communications and cyber operations.

Social Engineering - Manipulation, impersonation, deception etc are used for surveillance, gaining insider access, and tricking targets into enabling breaches across digital and physical channels. Well orchestrated human hacking expands technical capabilities.

Wireless Penetration Tools - Gabriel’s team uses wireless spy cameras, network sniffers, rogue devices, and VLAN hopping to extract data from secure networks by intercepting insecure RF communications and gaining access to connected systems.

Custom Malware Variants - Tailored malware strains are created to extract data, manipulate industrial controls, disable security software, corrupt backups, erase logs, prevent system recovery etc. This shows advanced threat capabilities.

Data Destruction and Ransomware - Gabriel deploys programs to erase data, logs, and file backups to cover his tracks and prevent recovery. Other tools encrypt government databases to make information unusable. This technique destroys availability and integrity.

Phishing and Social Malware - Deceptive messages with infected attachments or embedded links to compromised sites trick users into inadvertently downloading malware, enabling infiltration of secure networks. This continues to be a simple but common infiltration vector.

Reverse Engineering - Gabriel's team likely reverse engineers acquired malware samples, available IT products, and device firmware to discover vulnerabilities that are secretly kept unpatched. These become secret zero-day exploits.

In addition to these cyber techniques, physical force including assassins, explosives, guns, and surveillance further Gabriel’s operation by eliminating opposition, distracting attention, stealing data, and forcing compliance.

Ultimately McClane and his daughter Lucy's combined operational security skills and mental toughness enable initially identifying, resisting, tracking, and finally overwhelming Gabriel's technological advantages to stop the fire sale. This underscores that competence, adaptability, and collaboration remain vital to overcome sophisticated, relentless threats. With national security and public safety increasingly cyber-physical risks, the film highlightsExpanded cyber resilience capabilities are crucial to match the persistence and complexity of modern cyber operations.