Data Breaches, Analysis Frameworks & Threat Modelling

•••

Sonika Verma
CSCD27

Threat Modeling

Advanced Persistent Threats

- A: Advanced - targeted, coordinated, purposeful
  P: Persistent - repeated, over a period of time
  T: Threat - person(s) with intent, opportunity, and capability

- A stealthy actor which gains unauthorized access to a system/network and is able to remain undetected for an extended period of time

What is Threat Modeling

- identify, communicate, and understand threats and mitigations within the context of protecting something of value
- threat model is a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the lens of security

Threat modeling is a process for capturing, organizing, and analyzing all of this information

- enables informed decision-making about application security risks
- produce a prioritized list of security improvements to the concept, requirements, design, or implementation of an application

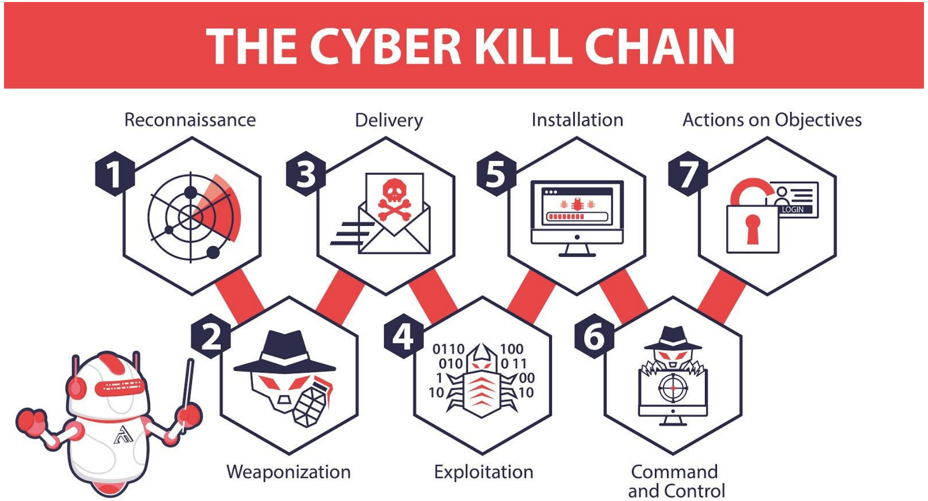
Case Studies, Analysis & Response Frameworks

Cyber Kill Chain
Supply Chain Attack

Case Study: Target

Cyber Kill Chain

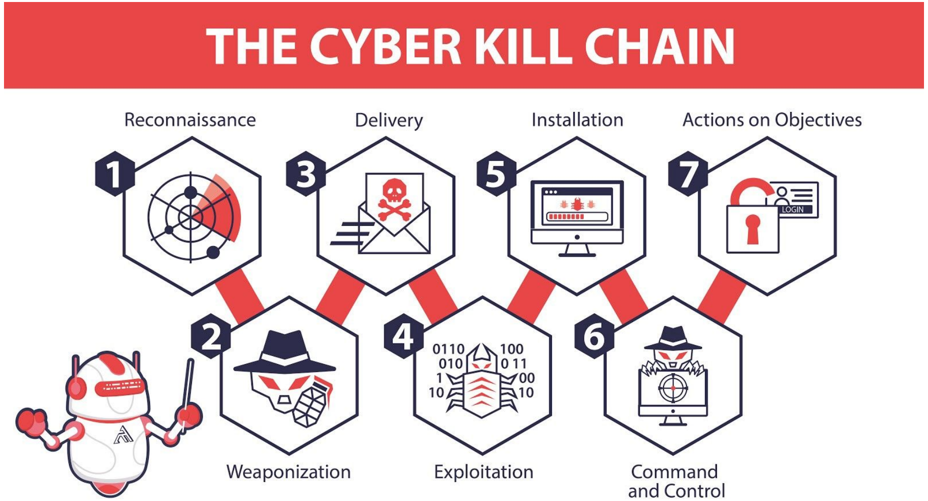
Framework



- **Reconnaissance**: research, identification, selection of targets, assess situation
- **Weaponization**: pairing remote access malware with exploit into a deliverable payload, leverage tools

Cyber Kill Chain

Framework



- **Delivery**: transmission of weapon to target
- **Exploitation**: once delivered, the weapon's code is triggered to exploit vulnerable system/applications

Cyber Kill Chain

Framework

- **Installation**: weapon installs backdoor on a target's system allowing persistent access
- **Command & Control**: outside server communicates with the weapons providing remote access inside target network
- **Actions on Objectives**: attacker works to achieve the objective of the intrusion (exfiltration, destruction, intrusion...)

Supply Chain Attack

Case Study: Target

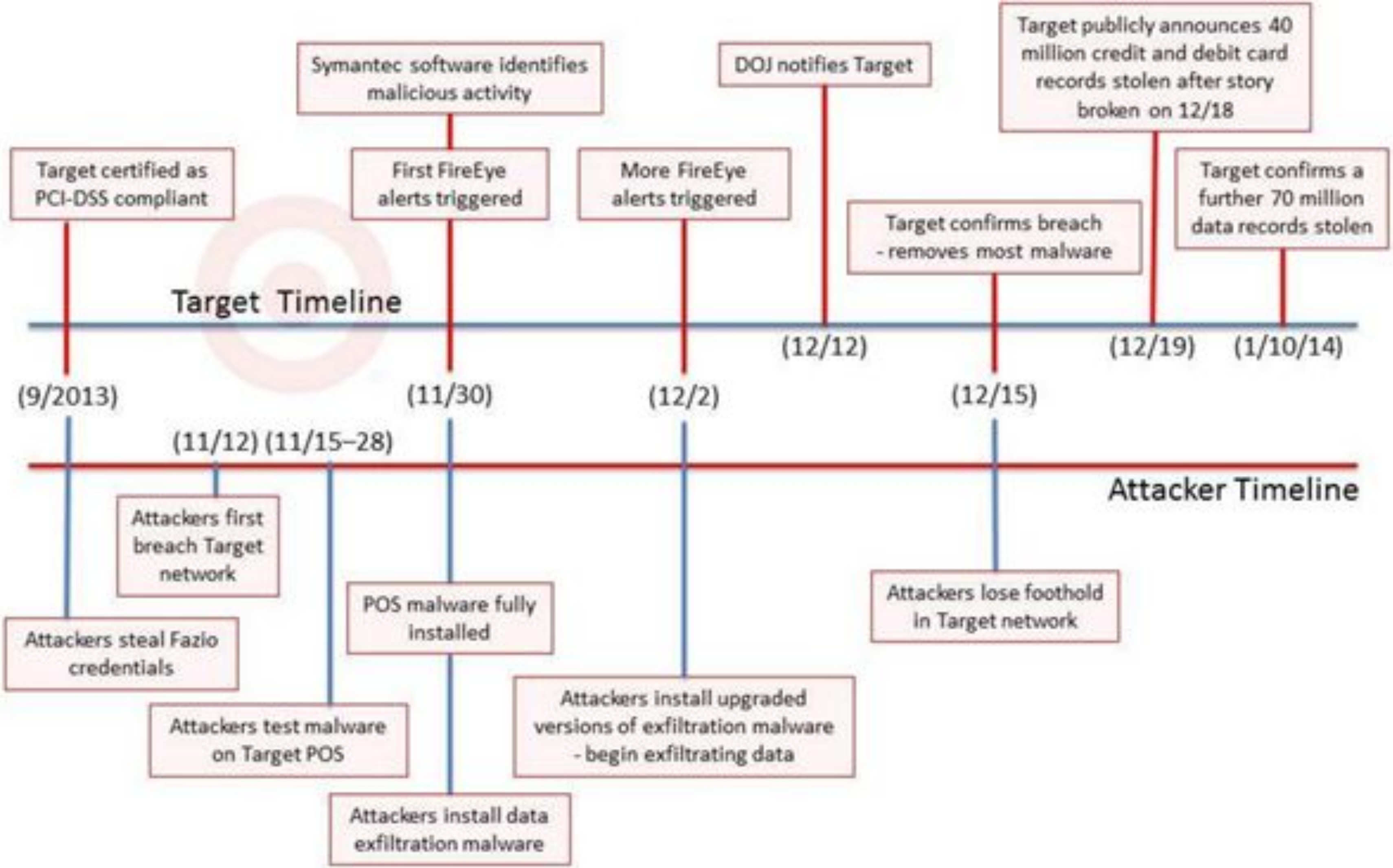
- Cyber attack that seeks to damage an organization by targeting less-secure elements or entities that have access to the system(s)
- Typically within the manufacturing process of a product by installing a rootkit or hardware based spying malware

Target 2013 Data Breach

Case Study

- Dec 2013
- Data breach affecting up to 110 million customers (name, address, contact, financial account)
- Stole financial data, personally identifiable information (PII)
- Removed sensitive information from from network to own
- Stolen data found on black-market forms, card shops
- ~$252 million in losses

PCI-DSS: Payment Card Industry Data Security Standards



Target Timeline

(9/2013) Target certified as PCI-DSS compliant

(11/30) Symantec software identifies malicious activity

(11/30) First FireEye alerts triggered

(12/2) More FireEye alerts triggered

(12/12) DOJ notifies Target

(12/15) Target confirms breach - removes most malware

(12/19) Target publicly announces 40 million credit and debit card records stolen after story broken on 12/18

(1/10/14) Target confirms a further 70 million data records stolen

Attacker Timeline

(9/2013) Attackers steal Fazio credentials

(11/12) Attackers first breach Target network

(11/15–28) Attackers test malware on Target POS

(11/30) POS malware fully installed

(11/30) Attackers install data exfiltration malware

(12/2) Attackers install upgraded versions of exfiltration malware - begin exfiltrating data

(12/15) Attackers lose foothold in Target network

Analysis

Cyber Kill Chain	Target
Reconnaissance	Found information about Fazio via publicly available Internet searches; found information about Target's HVAC facilities, analysis and metadata used to map network
Weaponization	Targeted Fazio, created malware stricken emails, sent malware emails to vendor in spear-phishing attempt, deployed, record passwords
Delivery	Shift focus to Target, weak perimeter security around network and storage that held customer/cardholder data, used stolen credentials, upload RAM scraping malware
Exploitation	Memory scraping and exfiltration malware records financial data through millions of cards used on POS terminals, stored information for later exfiltration
Installation	Attempted to further breach during installation by exploiting default/reused credentials, successful in some privilege escalation and gain additional internal access
Command & Control	Maintained communication with systems for over a month, maintain remote access in network to read, store, transfer data, or even remove data
Actions on Objectives	Transmitted stolen data to external servers, deleted customer information, stolen data offered on Russian dark website for sale

Target 2013 Data Breach

Case Study

Technical Tools

- Open Source Intelligence
- Citadel malware
- Trojan.POSRAM

Lessons Learned

➢ How do we respond to security incidents?

NIST/SANS Incident Response Point-of-Sale

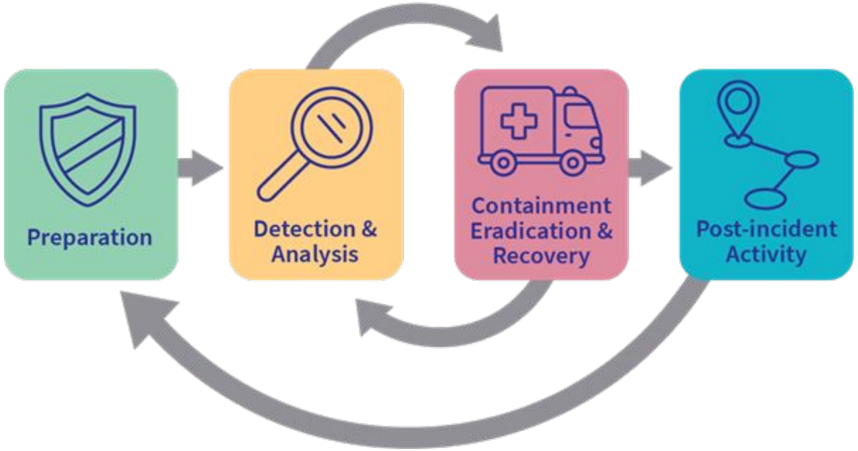
Case Study: Home Depot

NIST/SANS: Incident Response

Framework

NIST: National Institute of Standards and Technology

SANS: SysAdmin, Audit, Network and Security



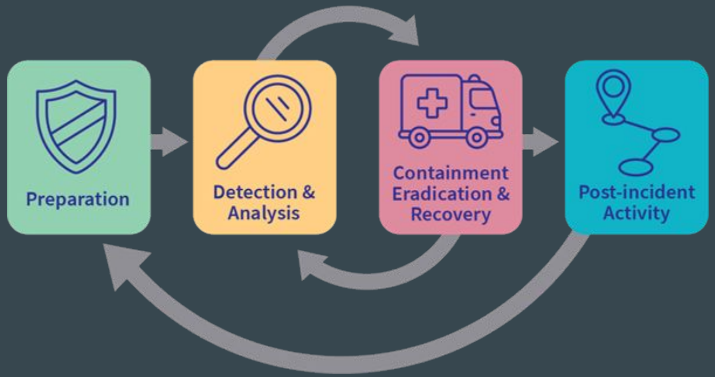
NIST/SANS Incident Response

Framework

- **Preparation**: well-designed policies to address events, define approach, responsibilities, evaluation, technical processes and tools, training
- **Detection**: detecting first signs of a kill chain, network/communication security, minimize false-positives, threat landscape

NIST/SANS Incident Response

Framework



- **Analysis**: event correlation, log configuration and management, synchronizing time, standardizing inputs, determining risk, prioritization, event notification, tracking until resolution
- **Response**: containment, eradication, recovery, isolate damage, restore affected systems
- **Review & Improvement**: proper documentation, lessons learned, evidence handling, sequence of events, areas of improvement, timing, suggestions, document future changes

Point-of-Sale Attack

Case Study: Home Depot

- ➢ Malicious software (malware) to target POS and payment terminals with intent to obtain financial information
- ➢ RAM scraping malware (encrypted end-to-end, decrypted in memory)
- ➢ RAT(s!) - Remote Access Trojans
- ➢ Scans active processes, searches for recognizable (pattern) data

Analysis

Case Study: Home Depot

- Sept 2014 retail data breach
- ~50 million payment cards stolen
  ~53 million email addresses mapped to customer info
- ~$200 million in losses
- 57 class action lawsuits

- Criticized for falling victim to the same kill chain as Target -- loss of reputation (business)

Analysis

Incident Response	Home Depot
Preparation	Did not take advantage of known threat landscape, no defined policies for evaluating security practices, lack of secure configuration in POS terminals, lack of network segregation, improper management of identity access and credentials
Detection	No solutions to detect malware installation, did not have regularly scans for vulnerability management, exploited zero-day, lack of security controls around intrusion detection/prevention, were not able to track actors that maintained elevated privileges
Analysis	Implemented anti-virus missing Network Threat Protection feature, systems/staff were not able to correlate information on host-intrusion, running outdated Windows software with known vulnerabilities
Response	Response to attack was largely delayed as it was not detected for about 5 months and continued to run in internal systems under disguise
Review & Improvement	Conducted post-incident

Home Depot 2014 Data Breach

Case Study

Technical Tools

- Custom malware with similarities to that used in Target breach
- BlackPOS
- Alina
- Rescator[dot]cc

Lessons Learned

➢ Many!
➢ Payment card security standards

STRIDE
Third-Party

Case Study: Marriott Hotels

STRIDE

Framework

Created by Microsoft engineers to guide discovery of threats in a system

- **S -** spoofing
- **T -** tampering
- **R -** repudiation
- **I -** information disclosure
- **D -** denial of service
- **E -** privilege escalation

Third-Party Breach

Case Study: Marriott Hotels

- ➢ Sensitive data is stolen from a third-party vendor
- ➢ Third-parties are compromised and used to breach/access/steal sensitive information from privileged systems

Tutorial: typical attack scenario is gain initial access, elevate privilege

Analysis

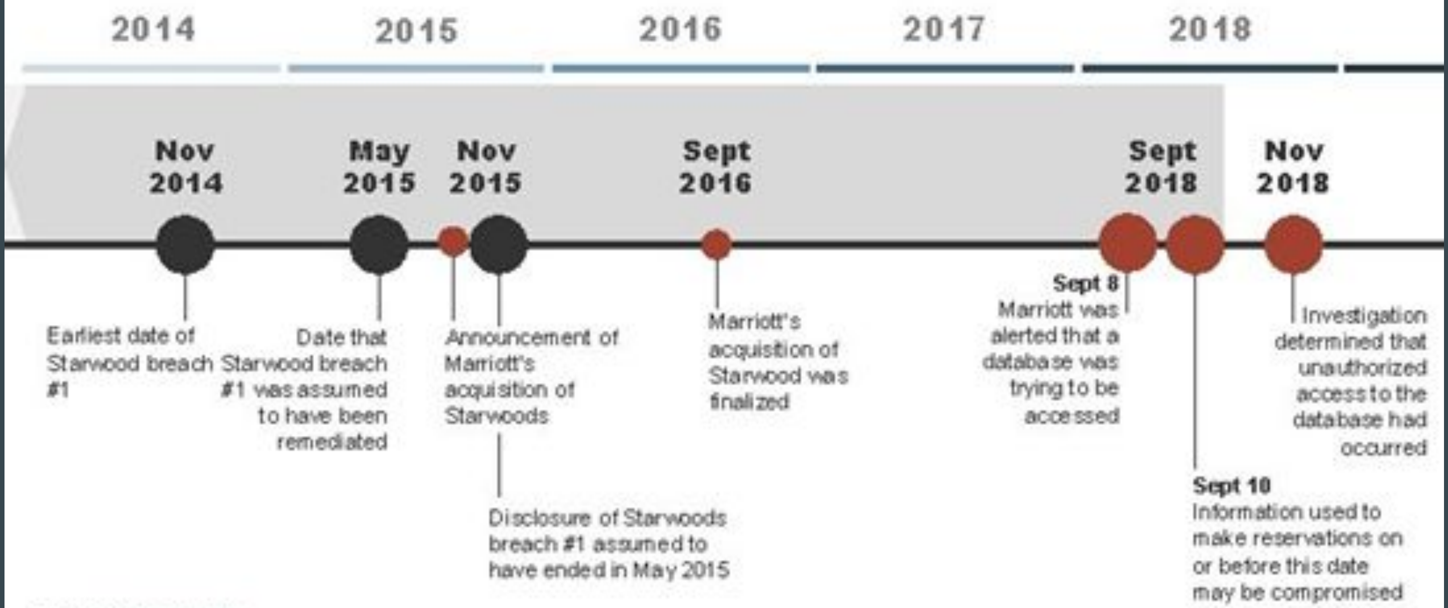
Case Study: Marriott Hotels

- September 2018
- Affecting up to 339 million people who stayed at any of their 6700 Starwoods hotel location
- ~7 million hotel guest records (arrival and departure, VIP status, loyalty program numbers)
- Tool flagged a suspicious access request of the guest reservations database
- Copied and encrypted sensitive information, attempted to remove
- €18.4 million fine (originally around €99 million) for violating privacy rights as described under GDPR

GDPR: General Data Protection Regulation

Timeline of Marriott/Starwood breach(s)

The 2018 Marriott breach may be linked to a 2014 vulnerability in Starwood's environment, disclosed shortly after acquisition was announced.



2014 2015 2016 2017 2018

Nov 2014 Earliest date of Starwood breach #1

May 2015 Date that Starwood breach #1 was assumed to have been remediated

Nov 2015 Announcement of Marriott's acquisition of Starwoods

Disclosure of Starwoods breach #1 assumed to have ended in May 2015

Sept 2016 Marriott's acquisition of Starwood was finalized

Sept 2018

Sept 8 Marriott was alerted that a database was trying to be accessed

Sept 10 Information used to make reservations on or before this date may be compromised

Nov 2018 Investigation determined that unauthorized access to the database had occurred

Source: Krebs Security

Analysis

STRIDE	**Marriott Hotels**
Spoofing	Attackers were able to misuse stolen/phished credentials to make database queries from authenticated but non-authorized user accounts
Tampering	Attackers were able to access database information, encrypt files, take some steps towards deleting some of those tables
Repudiation	Acting as users in the acquired systems, attackers were able to better disguise themselves and have activities go unnoticed for a long period of time
Information Disclosure	Attackers were able to access and exfiltrate customer information and data
Denial of Service	Had the deletion attempt been successful, hotel operations would have been compromised by lacking the information they need for regular procedures Resources needed to recover from attack would slow down or hinder standard operations
Elevation of Privileges	Attackers were able to made database queries on authenticated accounts despite not being the rightful owner

Marriott 2018 Data Breach

Case Study

Technical Tools

- MimiKatz RAT

Lessons Learned

- ➢ Security important!
- ➢ Security awareness

OWASP TOP 10 Watering Hole

Case Study: VOHO Campaign

OWASP Top 10

Framework

Open Web Application Security Project (open-community model)

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities
5. Broken Access Control
6. Security Misconfigurations
7. Cross-Site Scripting
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

Watering Hole Attack

Case Study: VOHO Campaign

- ➢ Computer attack strategy in which an attacker guesses or observes which websites an organization often uses and infects them with malware
- ➢ Infecting portable devices outside of organization network
- ➢ Could be targeted towards a specific predator
- ➢ Infect and compromise user to then be led to larger organization

Analysis

Case Study: VOHO Campaign

- June 2012
- First published by RSA
- Targeted USA operating organizations in the business-political sector (industry-specific attack)
- More than 32,000 hosts from over 700 organizations were redirected to exploit site
- ~4000 machines downloaded a malicious payload delivered to unsuspecting users from legitimate websites

VOHO Campaign 2012 Data Breach

Case Study

Technical Tools

- Gh0st RAT by malicious JavaScript delivery

Lessons Learned

➢ UBEA

PASTA
Insider Threats

Case Study: WireCard Inc.

PASTA

Framework

Process for Attack Simulation and Threat Analysis

1. Define business objectives
2. Define technical scope of assets and components
3. Application decomposition and identify application controls
4. Vulnerability detection
5. Attract enumeration and modeling
6. Risk analysis and development of countermeasures

Insider Threats

Case Study: WireCard Inc.

- ➢ Security risk that originates within the targeted organization
- ➢ Internal trusted actors

- ➢ Turncloack: insider who is maliciously stealing data
  Pawns: regular employee’s that make a mistake which is exploited by a bad actor

- ➢ Social Engineering

Analysis

Case Study: WireCard Inc.

German financial-tech company

- 2016 - 2021
- Several audits alleging fraudulent activity
- WireCard continuously denied claims and forged reports
- Money laundering, insider trading, defrauding external contracted companies, forging audit and financial record reports
- Hiring external actors

WireCard Inc.

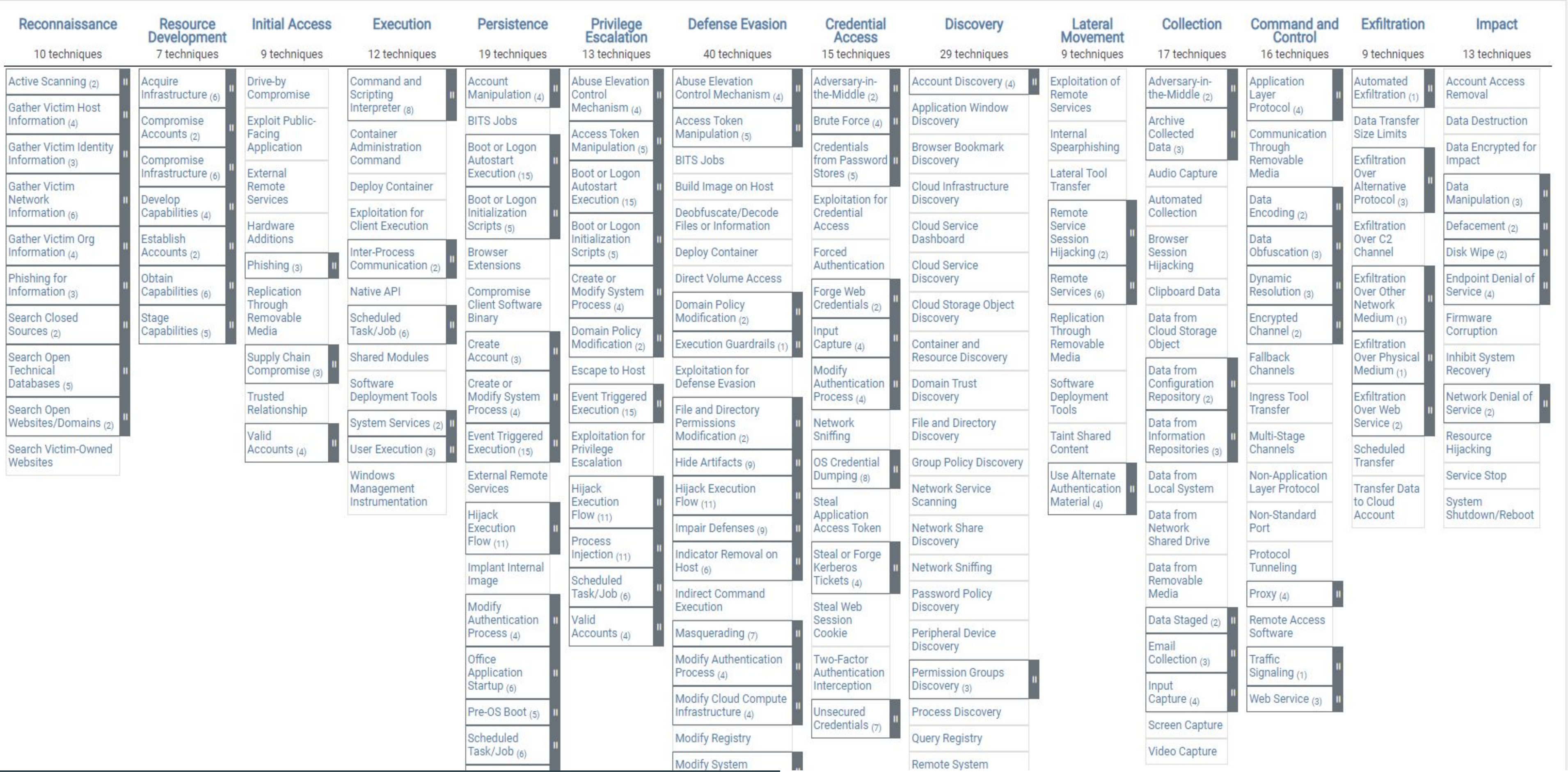
Case Study

- ➢ Security is meant to serve the business
- ➢ Business goals are a strong indication on assets of values, sensitive data, crucial operations and procedures

Lessons Learned

- ➢ Continuous monitoring
- ➢ Zero-trust
- ➢ Auditing
- ➢ Security awareness

MITRE ATT&CK



Reconnaissance

10 techniques

- Active Scanning (2)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development

7 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (5)

Initial Access

9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution

12 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (6)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence

19 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (15)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (11)
- Implant Internal Image
- Modify Authentication Process (4)
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (6)

Privilege Escalation

13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (15)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (11)
- Process Injection (11)
- Scheduled Task/Job (6)
- Valid Accounts (4)

Defense Evasion

40 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (9)
- Hijack Execution Flow (11)
- Impair Defenses (9)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (4)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System

Credential Access

15 techniques

- Adversary-in-the-Middle (2)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (4)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (7)

Discovery

29 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System

Lateral Movement

9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection

17 techniques

- Adversary-in-the-Middle (2)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Screen Capture
- Video Capture

Command and Control

16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

Exfiltration

9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact

13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Lessons Learned

Recent Data Breaches

1. 2018 TicketMaster (chatbot)
2. 2020 LinkedIn (leaked user data)
3. 2020 Audi-Volkswagen (publicly available data)
4. 2020 SolarWinds (supply-chain, backdoors, code-injection)
5. 2021 T-Mobile (cyber attack)
6. 2021 Twitch (data breach / leak)

The CSCD27 Framework

Case Study: You!

Security Learnings

1. Applied Cryptography
   a. Cryptography protocols
   b. Encrypted data
2. Network Security
   a. Communication protocols
   b. TCP/IP stack
   c. Security architecture
3. System Security
   a. Secure coding
   b. Web security
   c. Malware

Be aware, be secure!