

Chapter 2: Labs

Activity 2.1: Explore the ATT&CK Framework

<https://attack.mitre.org/>

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2) Gather Victim Host Information (0/4) Gather Victim Identity Information (0/3) Gather Victim Network Information (0/6) Gather Victim Org Information (0/4) Phishing for Information (0/3) Search Closed Sources (0/2) Search Open Technical Databases (0/5) Search Open Websites/Domains (0/2) Search Victim-Owned Websites	Acquire Infrastructure (0/6) Compromise Accounts (0/2) Compromise Infrastructure (0/6) Develop Capabilities (0/4) Establish Accounts (0/2) Obtain Capabilities (0/6)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (0/3) Replication Through Removable Media Supply Chain Compromise (0/3) Trusted Relationship Valid Accounts (0/4)	Command and Scripting Interpreter (0/8) Exploitation for Client Execution Inter-Process Communication (0/2) Native API Scheduled Task/Job (0/6) Shared Modules Software Deployment Tools System Services (0/2) User Execution (0/2) Windows Management Instrumentation	Account Manipulation (0/4) BITS Jobs Boot or Logon Autostart Execution (0/12) Boot or Logon Initialization Scripts (0/5) Browser Extensions Compromise Client Software Binary Create Account (0/3) Create or Modify System Process (0/4) Event Triggered Execution (0/15) Event Triggered Execution (0/15) External Remote Services Hijack Execution Flow (0/11) Hijack Execution Flow (0/11) Implant Container Image Office Application Startup (0/6) Pre-OS Boot (0/5) Scheduled Task/Job (0/6) Server Software Component (0/3)	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) Boot or Logon Autostart Execution (0/12) Boot or Logon Initialization Scripts (0/5) Create or Modify System Process (0/4) Event Triggered Execution (0/15) Exploitation for Privilege Escalation Group Policy Modification Hijack Execution Flow (0/11) Process Injection (0/11) Scheduled Task/Job (0/6) Valid Accounts (0/4)	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) BITS Jobs Deobfuscate/Decode Files or Information Direct Volume Access Execution Guardrails (0/1) Exploitation for Defense Evasion File and Directory Permissions Modification (0/2) Group Policy Modification Hide Artifacts (0/7) Hijack Execution Flow (0/11) Impair Defenses (0/7) Indicator Removal on Host (0/6) Indirect Command Execution Masquerading (0/6) Modify Authentication Process (0/4) Modify Cloud Infrastructure (0/4)	Brute Force (0/4) Credentials from Password Stores (0/3) Exploitation for Credential Access Forced Authentication Input Capture (0/4) Man-in-the-Middle (0/2) Modify Authentication Process (0/4) Network Sniffing OS Credential Dumping (0/8) Steal Application Access Token Steal or Forge Kerberos Tickets (0/4) Steal Web Session Cookie Two-Factor Authentication Interception Unsecured Credentials (0/6) Modify Cloud Infrastructure (0/4)	Account Discovery (0/4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (0/3) Process Discovery Query Registry Remote System Discovery Software Discovery (0/1)	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (0/2) Remote Services (0/6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (0/4)	Archive Collected Data (0/3) Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (0/2) Data from Information Repositories (0/2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (0/2) Email Collection (0/3) Input Capture (0/4) Man in the Browser Man-in-the-Middle (0/2) Screen Capture Video Capture	Application Layer Protocol (0/4) Communication Through Removable Media Data Encoding (0/2) Data Obfuscation (0/3) Dynamic Resolution (0/3) Encrypted Channel (0/2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (0/4) Remote Access Software Traffic Signaling (0/1) Web Service (0/3)	Automated Exfiltration (0/1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (0/3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (0/1) Exfiltration Over Physical Medium (0/1) Exfiltration Over Web Service (0/2) Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (0/3) Defacement (0/2) Disk Wipe (0/2) Endpoint Denial of Service (0/4) Firmware Corruption Inhibit System Recovery Network Denial of Service (0/2) Resource Hijacking Service Stop System Shutdown/Reboot

Recon | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 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	Acquire Infrastructure (6) Compromise Accounts (2) Compromise Infrastructure (6) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (6) Stage Capabilities (5)	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)	PowerShell AppleScript Windows Command Shell Unix Shell Visual Basic Python JavaScript Network Device CLI Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (2) Native API At (Windows) Scheduled Task At (Linux) Cron Systemd Timers Container Orchestration Job Shared Modules Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation
Scanning IP Blocks Vulnerability Scanning Hardware Software Firmware Client Configurations Credentials Email Addresses Employee Names Domain Properties DNS Network Trust Dependencies Network Topology IP Addresses Network Security Appliances Business Relationships Determine Physical Locations Identify Business Tempo Identify Roles Spearphishing Service Spearphishing Attachment Spearphishing Link Threat Intel Vendors Purchase Technical Data WHOIS DNS/Passive DNS Digital Certificates CDNs Scan Databases Social Media Search Engines	Domains DNS Server Virtual Private Server Server Botnet Web Services Social Media Accounts Email Accounts Domains DNS Server Virtual Private Server Server Botnet Web Services Malware Code Signing Certificates Digital Certificates Exploits Social Media Accounts Email Accounts Malware Tool Code Signing Certificates Digital Certificates Exploits Vulnerabilities Upload Malware Upload Tool Install Digital Certificate Drive-by Target Link Target	Spearphishing Attachment Spearphishing Link Spearphishing via Service Compromise Software Dependencies and Development Tools Compromise Software Supply Chain Compromise Hardware Supply Chain Default Accounts Domain Accounts Local Accounts Cloud Accounts	Additional Cloud Credentials Exchange Email Delegate Permissions

	Add Office 365 Global Administrator Role		
	SSH Authorized Keys		
BITS Jobs			
	Registry Run Keys / Startup Folder	Create Account (3)	Local Account
	Authentication Package		Domain Account
	Time Providers		Cloud Account
	Winlogon Helper DLL	Create or Modify System Process (4)	Launch Agent
	Security Support Provider		Systemd Service
	Kernel Modules and Extensions		Windows Service
	Re-opened Applications		Launch Daemon
Boot or Logon Autostart Execution (15)	LSASS Driver		Change Default File Association
	Shortcut Modification		Screensaver
	Port Monitors		Windows Management Instrumentation Event Subscription
	Plist Modification		Unix Shell Configuration Modification
	Print Processors		Trap
	XDG Autostart Entries		LC_LOAD_DYLIB Addition
	Active Setup	Event Triggered Execution (15)	Netsh Helper DLL
	Login Items		Accessibility Features
	Logon Script (Windows)		AppCert DLLs
	Logon Script (Mac)		Applnit DLLs
Boot or Logon Initialization Scripts (5)	Network Logon Script		Application Shimming
	RC Scripts		Image File Execution Options Injection
	Startup Items		PowerShell Profile
Browser Extensions			Emond
Compromise Client Software Binary		External Remote Services	Component Object Model Hijacking

	Services File Permissions Weakness
	Executable Installer File Permissions Weakness
	Services Registry Permissions Weakness
	Path Interception by Unquoted Path
Hijack Execution Flow (11)	Path Interception by PATH Environment Variable
	Path Interception by Search Order Hijacking
	DLL Search Order Hijacking
	DLL Side-Loading
	Dynamic Linker Hijacking
	Dylib Hijacking
	COR_PROFILER

Implant Internal

Privilege Escalation 13 techniques	
Abuse Elevation Control Mechanism (4)	Setuid and Setgid
	Bypass User Account Control
	Sudo and Sudo Caching
	Elevated Execution with Prompt
Access Token Manipulation (5)	Token Impersonation/Theft
	Create Process with Token
	Make and Impersonate Token
	Parent PID Spoofing
	SID-History Injection
Boot or Logon Autostart Execution (15)	Registry Run Keys / Startup Folder
	Authentication Package
	Time Providers
	Winlogon Helper DLL
	Security Support Provider
	Kernel Modules and Extensions
	Re-opened Applications
	LSASS Driver
	Shortcut Modification
	Port Monitors
	Plist Modification
	Print Processors
	XDG Autostart Entries
	Active Setup
	Login Items
	Logon Script (Windows)

Change Default File Association
Screensaver
Windows Management Instrumentation Event Subsc
Unix Shell Configuration Modification
Trap
LC_LOAD_DYLIB Addition

Boot or Logon Initialization Scripts ⁽⁵⁾	Logon Script (Mac)	Event Triggered Execution ⁽¹⁵⁾	Netsh Helper DLL
	Network Logon Script		Accessibility Features
	RC Scripts		AppCert DLLs
	Startup Items		Applnit DLLs
	Launch Agent		Application Shimming
Create or Modify System Process ⁽⁴⁾	Systemd Service		Image File Execution Options Injection
	Windows Service		PowerShell Profile
	Launch Daemon		Emond
Domain Policy Modification ⁽²⁾	Group Policy Modification		Component Object Model Hijacking
	Domain Trust Modification	Exploitation for Privilege Escalation	
Escape to Host			

	Services File Permissions Weakness
	Executable Installer File Permissions Weakness
	Services Registry Permissions Weakness
	Path Interception by Unquoted Path
	Path Interception by PATH Environment Variable
Hijack Execution Flow ⁽¹¹⁾	Path Interception by Search Order Hijacking
	DLL Search Order Hijacking
	DLL Side-Loading
	Dynamic Linker Hijacking
	Dylib Hijacking
	COR_PROFILER
	Dynamic-link Library Injection
	Portable Executable Injection
	Thread Execution Hijacking
	Asynchronous Procedure Call
	Thread Local Storage
Process Injection ⁽¹¹⁾	Ptrace System Calls
	Proc Memory
	Extra Window Memory Injection
	Process Doppelg�nging
	Process Hollowing
	VDSO Hijacking
	At (Windows)
	Scheduled Task
Scheduled Task/Job ⁽⁶⁾	At (Linux)
	Cron
	Systemd Timers
	Container Orchestration Job
	Default Accounts
Valid Accounts ⁽⁴⁾	Domain Accounts
	Local Accounts
	Cloud Accounts

<https://edition.cnn.com/2021/06/11/cars/vw-audi-hack-customer-information/index.html>

1.
- What was stolen?

hit by a data breach that exposed the contact information and, in some cases, personal details, like driver license numbers, of customers in the United States and Canada.
- Who is affected?

More than 3 million customers or shoppers had at least basic contact information stolen from an outside company that worked with the automakers, according VW. That data included phone numbers, email addresses, postal mailing addresses and, in some cases, vehicle identification numbers.
- What is the company doing to "make it better?"

The company is offering free credit protection to those who had very sensitive information taken.
- How was the data stolen?

The data, which was stolen from an outside vendor that VW and Audi and some of their dealers use, had been gathered between 2014 and 2019. The information had been collected and saved for marketing purposes, according to VW(VLKPE), and had been left in an unsecured file. VW did not name the vendor.

Part 1: Build a threat profile/Part 2: Analysis

1. List what you know about the compromise or exploit, including details about the threat actor, what occurred, what tools were used, and as many other details as you can find.

2. Review your list against the headings for the appropriate ATT&CK matrix. Do you have items that match the headings?
3. If you still lack data, you should continue your search or find another example to work through!

Insider Threat (unintentional): VW did not protect the data securely, and exposed the file to a 3rd party. The file was unsecured.

ATT&CK: Enterprise/Trusted Relationship

Mitigation: Properly manage accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if the party is compromised by an adversary.

OR

ATT&CK: Collection/Archived Collected Data

Mitigation: Systems scans to identify unauthorized archival utilities

Activity 2.2: Set Up a STIX/TAXII Feed

user: anomali
default password: anomolistaxx
changed pw: biddion4212

Anomali's STAXX community version provides an easy way to consume STIX feeds. In this exercise, you will download and install the STAXX client, and then review the data from one of the included feeds.

1. Visit www.anomali.com/community/staxx and download the STAXX Community edition software. STAXX is a 1 GB download and requires an email to get the download link.
2. Install the STAXX client. You will need a virtualization environment like VirtualBox or VMWare to open the OVA file. Follow the Anomali setup and installation guide at update.anomali.com/staxx/docs/Anomali_STAXX_Installation_&Administration_Guide.pdf.
3. This guide will help you get Anomali set up. When you connect to the web interface, you will need to accept the insecure connection on most major browsers.
4. When asked, use the Anomali Limo service to gather data for your first feeds.
5. Once you are in and Anomali has ingested its feeds, explore the dashboards. What is the most common indicator type? Does it match what you would expect?
6. Advanced: Identify a STIX feed that isn't part of the STAXX default feed list and add it to STAXX.



