Darstellung eines Angriffsablaufs mittels des sog. MITRE ATT&CK-Frameworks - eine Wissensbasis über das Verhalten des Gegners

Angriffe erkennen und abschwächen bzw. abwehren (https://attack.mitre.org/)

Techniques / Techniken: how the goals are achieved / wie die Ziele erreicht werden

Tactics / Taktiken: the adversary's technical goals / technisches Ziel des Gegners

1 Reconnaissance Aufklärung	2 Resource Development Ressourcen entwickeln	3 Initial Access Erstzugang	4 Execution Ausführung	5 Persistence Persistenz	6 Privilege Escalation Erweiterung von Berechtigungen	7 Defense Evasion Umgehung von Abwehrtechniken	8 Credential Access Zugang zu Berechtigungen	9 Discovery Entdeckung	10 Lateral Movement laterale Bewegung	11 Collection Sammlung	12 Command and Control Steuerung und Kontrolle	13 Exfiltration Exfiltration	14 Impact "Anschlag"
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information — Informationen über das Opfer sammeln	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Daten verschlüsseln — Data Encrypted for Impact
Credentials	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration über einen Command & Control Kanal — Exfiltration Over C2 Channel	Data Manipulation
E-Mail-Adressen — Email Addresses	Fähigkeiten entwickeln — Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Fernbedienungs-Dienste — Remote Services	Browser Session Hijacking	Datenverschleierung — Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Namen von Arbeitnehmern — Employee Names	Code Signing Certificates	Phishing	Inter-Process Communication	Compromise Client Software Binary	Kreieren oder Verändern von System-Prozessen — Create or Modify System Process	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Cloud Services	Clipboard Data	Junk Data	Exfiltration Over Physical Medium	Disk Wipe
Gather Victim Network Information	Digital Certificates	Spearphishing Attachment	Native API	Create Account	Launch Agent	Deploy Container	Input Capture	Cloud Storage Object Discovery	Direct Cloud VM Connections	Data from Cloud Storage	Protocol Impersonation	Exfiltration Over Web Service	Endpoint Denial of Service
Gather Victim Org Information	Exploits	Spearphishing Link	Scheduled Task/Job	Kreieren oder Verändern von System-Prozessen — Create or Modify System Process	Launch Daemon	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Distributed Component Object Model	Data from Configuration Repository	Steganografie — Steganography	Scheduled Transfer	Financial Theft
Phishing for Information	Schadsoftware — Malware	Spearphishing via Service	Service Execution	Launch Agent	Systemd Service	Domain Policy Modification	Multi-Factor Authentication Interception	Debugger Evasion	Remote Desktop Protocol	Data from Information Repositories	Dynamic Resolution	Transfer Data to Cloud Account	Firmware Corruption
Search Closed Sources	Establish Accounts	Spearphishing Voice	Shared Modules	Launch Daemon	Windows Dienst — Windows Service	Execution Guardrails	Multi-Factor Authentication Request Generation	Device Driver Discovery	administrative Freigaben in Windows — SMB/Windows Admin Shares	Data from Local System	Encrypted Channel		Inhibit System Recovery
Search Open Technical Databases	Obtain Capabilities	Replication Through Removable Media	Software Deployment Tools	Systemd Service	Domain Policy Modification	Exploitation for Defense Evasion	Mitschneiden von Netzwerkverkehr — Network Sniffing	Domain Trust Discovery	SSH	Daten eines geteilten Netzwerklaufwerks — Data from Network Shared Drive	Fallback Channels		Network Denial of Service
Durchsuchen offener Webseiten/Domains — Search Open Websites/Domains	Stage Capabilities	Supply Chain Compromise	System Services	Windows Dienst — Windows Service	Escape to Host	File and Directory Permissions Modification — Veränderung von Datei- und Ordner-berechtigungen	Herunterladen von OS-Anmeldeinformationen — OS Credential Dumping	File and Discovery					
Code Repositories		Trusted Relationship	Benutzer-Ausführung — User Execution	Event Triggered Execution	Event Triggered Execution	Linux and Mac File and Directory Permissions Modification	/etc/passwd and /etc/shadow	Group Policy					
Suchmaschinen — Search Engines		Valid Accounts	schadhafte Datei — Malicious File	External Remote Services	Exploitation for Privilege Escalation	Windows File and Directory Permissions Modification — Veränderung von Windows-Datei- und Ordner-berechtigungen	Cached Domain Credentials	Log Er					
Social Media			Malicious Image	Hijack Execution Flow	Hijack Execution Flow	Hide Artifacts	DCSync	Netwo Servic					
Search Victim-Owned Websites			Malicious Link	Implant Internal Image	Process Injection	Hijack Execution Flow	LSA Secrets	Netwo Share					
			Windows Management Instrumentation	Modify Authentication Process	Scheduled Task/Job	Impair Defenses	LSASS Speicher — LSASS Memory	Mitschneiden von Netzwerkverkehr — Network Sniffing	Use Alternate Authentication Material	Video Capture	Proxy		
				Office Application Startup	Valid Accounts	Impersonation	NTDS	Password Policy Discovery			Remote Access Software		
				Power Settings		Indicator Removal	Proc Filesystem	Peripheral Device Discovery			Traffic Signaling		
				Pre-OS Boot		Indirect Command Execution	Security Account Manager	Permission Groups Discovery			Web Service		

Procedures / Verfahren: specific technique implementation / spezifische Umsetzung der Technik

Phishing: Spearphishing Link

Procedure Examples

ID	Name	Description
S0677	AADInternals	AADInternals can send "consent phishing" emails containing malicious links designed to steal users' access tokens.[5]
S0584	AppleJeus	AppleJeus has been distributed via spearphishing link.[6]
G0006	APT1	APT1 has sent spearphishing emails containing hyperlinks to malicious files.[7]