about

Printnightmare Attack Map 1 by Joas

domain

Enterprise ATT&CK v9

platforms

Windows, PRE, Network

Reconnaissance

- **Active Scanning**
- **Gather Victim Host Information**
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

Resource Development

- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
  - Social Media Accounts
  - Email Accounts
- Obtain Capabilities
- **Stage Capabilities**

Initial Access

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

Execution

- **Command and Scripting Interpreter**
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- **Scheduled Task/Job**
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation

Persistence

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- **Create Account**
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- **Hijack Execution Flow**
- Modify Authentication Process
- Office Application Startup
- Pre-OS Boot
- **Scheduled Task/Job**
- Server Software Component
- Traffic Signaling
- **Valid Accounts**

Privilege Escalation

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

Defense Evasion

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- **Hijack Execution Flow**
- Impair Defenses
- Indicator Removal on Host
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- Obfuscated Files or Information
- Pre-OS Boot
- **Process Injection**
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Subvert Trust Controls
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Use Alternate Authentication Material
- **Valid Accounts**
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

Credential Access

- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Man-in-the-Middle
- Modify Authentication Process
- **Network Sniffing**
- OS Credential Dumping
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials

Discovery

- **Account Discovery**
- Application Window Discovery
- Browser Bookmark 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
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

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

Collection

- Archive Collected Data
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Man-in-the-Middle
- Screen Capture
- Video Capture

Command and Control

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

Exfiltration

- **Automated Exfiltration**
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- **Exfiltration Over C2 Channel**
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer

Impact

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