THREAT INTELLIGENCE

DigiSuraksha

Parhari Foundation

Exploration and Proof of concept (POC)

Prathamesh Arun Kamble

07.08.2025

Intern Id-195

🔍 MITRE ATT&CK Enterprise: 14 Tactics + 3 Techniques Each + Procedures

No	Tactics	Techniques	Procedures
1	Initial Access	Phishing (T1566)	Craft a spear-phishing email with a malicious link or attachment targeting a user. When clicked or opened, it delivers malware payload to the victim's machine.
		Drive-by Compromise (T1189)	Compromise a website frequently visited by the target, inject malicious code that exploits browser vulnerabilities to silently deliver malware when the user visits the site.
		Exploit Public-Facing Application (T1190)	Scan target web servers for known vulnerabilities, exploit a SQL injection flaw to gain unauthorized access and execute commands on the server.
2	Execution	Command and Scripting Interpreter: PowerShell (T1059.001)	Execute PowerShell commands remotely to download and execute malicious scripts on Windows hosts.
		User Execution (T1204)	Trick the user into running a malicious file disguised as a legitimate document or installer.
		Scheduled Task/Job (T1053)	Create a scheduled task to run a malicious script every hour to maintain persistence and execute

			payloads.
3	Persistence	Registry Run Keys / Startup Folder (T1547.001)	Add malicious executable path to registry run keys so it launches on system startup.
		Create Account (T1136)	Create a new user account with administrative privileges to retain access after initial compromise.
		Scheduled Task/Job (T1053)	Set up a recurring scheduled task that executes malware to maintain persistence.
4	Privilege Escalation	Exploitation for Privilege Escalation (T1068)	Exploit a Windows kernel vulnerability to gain SYSTEM-level privileges from a user-level context.
		Process Injection (T1055)	Inject malicious code into a legitimate process (like explorer.exe) to evade detection and elevate privileges.
		Bypass User Account Control (T1548.002)	Use UAC bypass techniques to run a payload with elevated privileges without prompting the user.
5	Defense Evasion	Obfuscated Files or Information (T1027)	Use base64 encoding or encryption on malware payloads to evade signature-based detection.
		Disable Security Tools (T1562.001)	Terminate or disable antivirus and endpoint detection tools to avoid detection.
		File Deletion (T1107)	Delete logs or malware dropper files after execution to remove forensic evidence.

6	Credential Access	Credential Dumping (T1003)	Extract hashed credentials from the Windows LSASS process memory using mimikatz or similar tool.
		Brute Force (T1110)	Attempt multiple password guesses against remote services like RDP or SSH using automated tools.
		Input Capture (T1056)	Use keyloggers or credential sniffers to capture user credentials as they type.
7	Discovery	System Network Connections Discovery (T1049)	Run commands like netstat or Get-NetTCPConnection to map active network connections and identify targets.
		System Information Discovery (T1082)	Collect detailed system information using commands like systeminfo or PowerShell's Get-ComputerInfo.
		File and Directory Discovery (T1083)	Enumerate directories and files to find sensitive data or configuration files.
8	Lateral Movement	Remote Services: SMB/Windows Admin Shares (T1021.002)	Use SMB to connect to administrative shares (C$, ADMIN$) on remote machines and execute commands.
		Windows Remote Management (WinRM) (T1028)	Use WinRM to execute commands remotely on Windows hosts in the domain.
		Pass the Ticket (T1550.003)	Capture and reuse Kerberos tickets to impersonate users and access resources on other systems.

9	Collection	Screen Capture (T1113)	Take screenshots periodically to gather information displayed on the victim's desktop.
		Input Capture: Keylogging (T1056.001)	Capture keystrokes to obtain passwords, messages, and other sensitive input.
		Data from Local System (T1005)	Search and exfiltrate sensitive files and documents stored on the compromised host.
10	Command and Control (C2)	Standard Application Layer Protocol: HTTP/S (T1071.001)	Use HTTPS for encrypted communication with the C2 server, sending commands and receiving data stealthily.
		Domain Generation Algorithms (DGA) (T1483)	Generate domain names algorithmically to periodically connect with C2 infrastructure, evading static detection.
		Custom Command and Control Protocol (T1095)	Implement a proprietary C2 communication protocol over uncommon ports to evade firewall and IDS rules.
11	Exfiltration	Exfiltration Over C2 Channel (T1041)	Send collected data through the existing C2 channel, hiding exfiltration within normal command traffic.
		Automated Exfiltration (T1020)	Automate the transfer of sensitive files to attacker-controlled servers using scheduled scripts.
		Exfiltration Over Alternative Protocol (T1048)	Use protocols like FTP or DNS tunneling to send data out of the network unnoticed.

12	Impact	Data Destruction (T1485)	Delete critical files or overwrite disks to cause permanent data loss.
		Data Encrypted for Impact (Ransomware) (T1486)	Encrypt user files and demand ransom for decryption keys.
		Resource Hijacking (T1496)	Use victim systems' CPU/GPU resources to mine cryptocurrency without authorization.
13	Reconnaissance	Gather Victim Identity Information (T1589)	Collect information such as usernames, emails, and organizational details from public sources.
		Search Open Websites/Domains (T1590)	Scan and harvest data from open websites, DNS records, or social media to profile the target.
		Phishing for Information (T1598)	Send phishing emails designed to trick users into revealing credentials or internal information.
14	Resource Development	Acquire Infrastructure (T1583)	Rent or purchase cloud servers or domain names to host malware and C2 infrastructure.
		Develop Malware (T1587)	Create custom malware or modify open-source tools tailored to the target environment.
		Compromise Accounts (T1586)	Use stolen credentials to establish footholds on cloud services or third-party platforms.