



# آموخته‌های حملات سایبری از تهدیدشناسی تا دفاع پیشگیرانه

شرکت نرم‌افزاری امن‌پرداز



تهدید شناسی فضای کشور

مدل سازی حملات سایبری

گروه های مهاجم فعال در کشور

تکنیک های نفوذ پر استفاده

مطالعه موردی حملات سایبری

پرونده ۱)

حمله در سطح مجازی ساز

پرونده ۲)

حمله زنجیره تأمین

پرونده ۳)

آلوده سازی سفت افزار

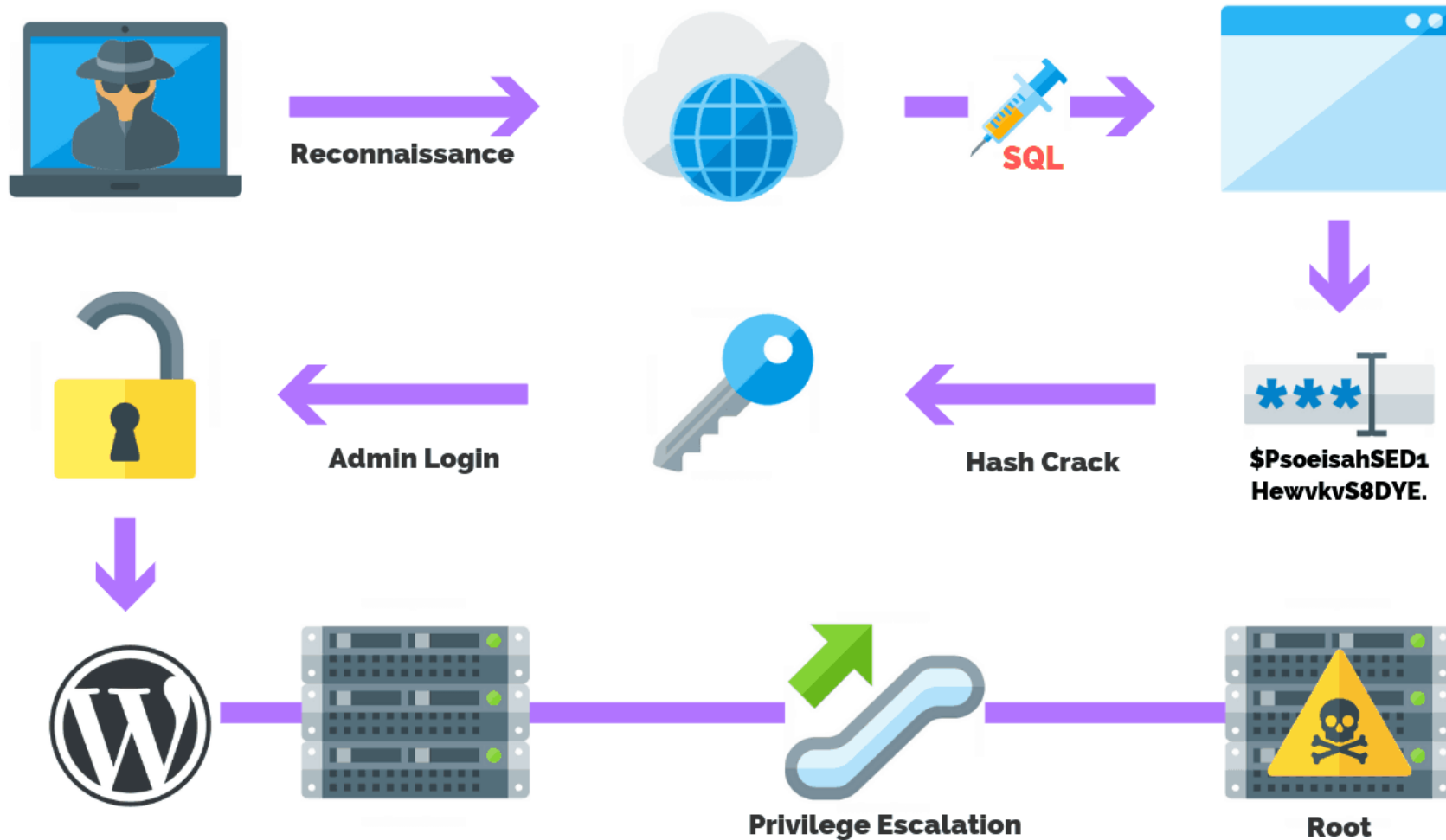
درس آموخته های  
حملات سایبری

و روش های مقابله

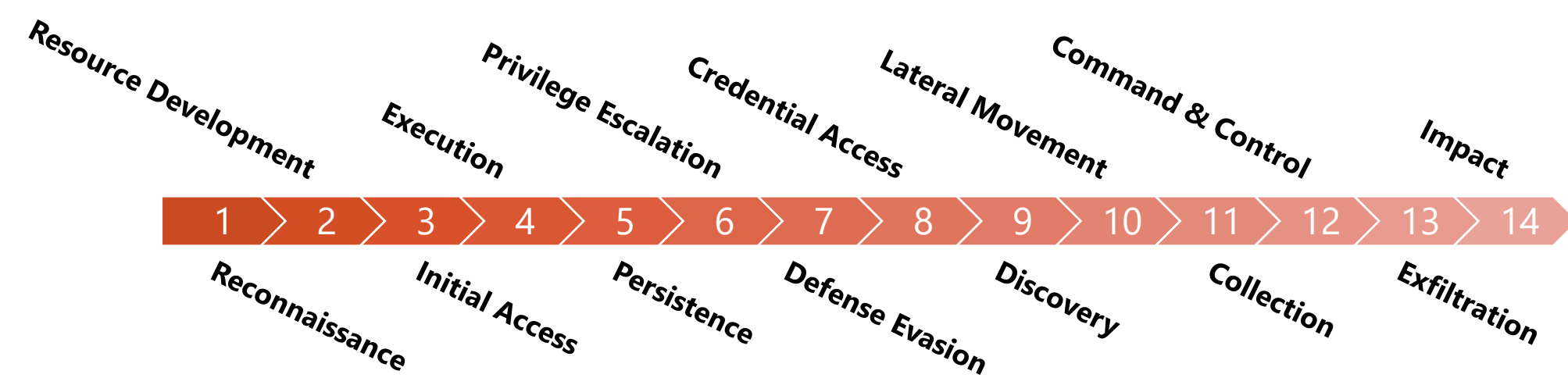


# مدل سازی حملات سایبری

# مثالی از یک حمله سایبری



# مدل سازی حمله سایبری بر اساس MITRE ATT&CK



# تقسیم کار گروه‌های فعال تهدید سایبری

مدل زنجیره تخریب سایبری (Cyber Kill Chain)

Lockheed Martin - 2011



# تقسیم کار گروه‌های فعال تهدید سایبری

پویشگرها و جستجوگرهای تجاری و غیرتجاری  
Shodan, Censys

گروه‌های کشف آسیب‌پذیری و ساخت اکسپلویت‌ها و بدافزارها  
Metasploit, Veil, Cobalt Strike

گروه‌های اخذ دسترسی  
ایمیل‌های آلوده، نصب درب‌های پشتی، اطلاعات اکانت‌ها، تروجان، بات‌نت

انجام اقدام نهایی حمله سایبری





# گروه‌های مهاجم فعال در کشور

# PIG.006-GhiyamTaSarneguni

| Reconnaissance<br>10 techniques          | Resource Development<br>8 techniques | Initial Access<br>10 techniques     | Execution<br>14 techniques              | Persistence<br>20 techniques               | Privilege Escalation<br>14 techniques      | Defense Evasion<br>43 techniques                  | Credential Access<br>17 techniques             | Discovery<br>32 techniques                        | Lateral Movement<br>9 techniques            | Collection<br>17 techniques              | Command and Control<br>17 techniques  | Exfiltration<br>9 techniques                 | Impact<br>14 techniques          |
|------------------------------------------|--------------------------------------|-------------------------------------|-----------------------------------------|--------------------------------------------|--------------------------------------------|---------------------------------------------------|------------------------------------------------|---------------------------------------------------|---------------------------------------------|------------------------------------------|---------------------------------------|----------------------------------------------|----------------------------------|
| Active Scanning (1/3)                    | Acquire Access                       | Content Injection                   | Cloud Administration Command            | Account Manipulation (0/6)                 | Abuse Elevation Control Mechanism (0/5)    | Abuse Elevation Control Mechanism (0/5)           | Adversary-in-the-Middle (0/3)                  | Account Discovery (0/4)                           | Exploitation of Remote Services             | Adversary-in-the-Middle (0/3)            | Application Layer Protocol (0/4)      | Automated Exfiltration (0/1)                 | Account Access Removal           |
| Scanning IP Blocks                       | Acquire Infrastructure (0/8)         | Drive-by Compromise                 | Command and Scripting Interpreter (1/9) | BITS Jobs                                  | Access Token Manipulation (0/5)            | Access Token Manipulation (0/5)                   | Brute Force (0/4)                              | Application Window Discovery                      | Internal Spearphishing                      | Archive Collected Data (0/3)             | Communication Through Removable Media | Data Transfer Size Limits                    | Data Destruction                 |
| Vulnerability Scanning                   | Compromise Accounts (0/3)            | Exploit Public-Facing Application   | AppleScript                             | Boot or Logon Autostart Execution (1/14)   | Account Manipulation (0/6)                 | BITS Jobs                                         | Credentials from Password Stores (0/6)         | Browser Information Discovery                     | Lateral Tool Transfer                       | Audio Capture                            | Content Injection                     | Exfiltration Over Alternative Protocol (0/3) | Data Encrypted for Impact        |
| Wordlist Scanning                        | Compromise Infrastructure (0/7)      | External Remote Services            | Cloud API                               | Active Setup                               | Boot or Logon Autostart Execution (1/14)   | Build Image on Host                               | Exploitation for Credential Access             | Cloud Infrastructure Discovery                    | Remote Service Session Hijacking (0/2)      | Automated Collection                     | Data Encoding (0/2)                   | Exfiltration Over C2 Channel                 | Data Manipulation (0/3)          |
| Gather Victim Host Information (0/4)     | Develop Capabilities (0/4)           | Hardware Additions                  | JavaScript                              | Authentication Package                     | Active Setup                               | Debugger Evasion                                  | Forced Authentication                          | Cloud Service Dashboard                           | Remote Services (1/8)                       | Browser Session Hijacking                | Data Obfuscation (0/2)                | Exfiltration Over Other Network Medium (0/1) | Defacement (1/2)                 |
| Gather Victim Identity Information (0/3) | Establish Accounts (0/3)             | Phishing (0/4)                      | Network Device CLI                      | Kernel Modules and Extensions              | Authentication Package                     | Deobfuscate/Decode Files or Information           | Forge Web Credentials (0/2)                    | Cloud Service Discovery                           | Cloud Services                              | Clipboard Data                           | Dynamic Resolution (0/3)              | Exfiltration Over Physical Medium (0/1)      | External Defacement              |
| Gather Victim Network Information (0/6)  | Obtain Capabilities (0/6)            | Replication Through Removable Media | PowerShell                              | Login Items                                | Kernel Modules and Extensions (0/2)        | Deploy Container                                  | Input Capture (0/4)                            | Cloud Storage Object Discovery                    | Direct Cloud VM Connections                 | Data from Cloud Storage                  | Encrypted Channel (0/2)               | Exfiltration Over Web Service (0/4)          | Internal Defacement              |
| Gather Victim Org Information (0/4)      | Stage Capabilities (0/6)             | Supply Chain Compromise (0/3)       | Python                                  | LSASS Driver                               | Logon Items                                | Direct Volume Access                              | Modify Authentication Process (0/8)            | Container and Resource Discovery                  | Distributed Component Object Model          | Data from Configuration Repository (0/2) | Fallback Channels                     | Scheduled Transfer                           | Disk Wipe (0/2)                  |
| Phishing for Information (0/4)           | Valid Accounts (2/4)                 | Trusted Relationship                | Unix Shell                              | Port Monitors                              | LSASS Driver                               | Domain Policy Modification (0/2)                  | Multi-Factor Authentication Interception       | Debugger Evasion                                  | Remote Desktop Protocol                     | Data from Information Repositories (0/2) | Ingress Tool Transfer                 | Transfer Data to Cloud Account               | Endpoint Denial of Service (0/4) |
| Search Closed Sources (0/2)              | Default Accounts                     | Cloud Accounts                      | Visual Basic                            | Print Processors                           | Port Monitors                              | Execution Guardrails (0/1)                        | Multi-Factor Authentication Request Generation | File and Directory Permissions Modification (0/2) | SMB/Windows Admin Shares                    | Data from Local System                   | Multi-Stage Channels                  | Network Denial of Service (0/2)              | Financial Theft                  |
| Search Open Technical Databases (0/5)    | Domain Accounts                      | Default Accounts                    | Windows Command Shell                   | Re-opened Applications                     | Print Processors                           | Exploitation for Defense Evasion                  | Multi-Factor Authentication Request Generation | Hide Artifacts (0/11)                             | SSH                                         | Data from Network Shared Drive           | Non-Application Layer Protocol        | Resource Hijacking                           | Firmware Corruption              |
| Search Open Websites/Domains (0/3)       | Local Accounts                       | Default Accounts                    | Container Administration Command        | Registry Run Keys / Startup Folder         | Print Processors                           | File and Directory Permissions Modification (0/2) | Network Sniffing                               | Hijack Execution Flow (0/12)                      | VNC                                         | Data from Removable Media                | Protocol Tunneling                    | Service Stop                                 |                                  |
| Search Victim-Owned Websites             |                                      |                                     | Deployment Container                    | Security Support Provider                  | Re-opened Applications                     | Hide Artifacts (0/11)                             | OS Credential Dumping (1/8)                    | Impair Defenses (1/11)                            | Windows Remote Management                   | Data from Staged (0/2)                   | Proxy (2/4)                           | System Shutdown/Reboot                       |                                  |
|                                          |                                      |                                     | Execution for Client                    | Shortcut Modification                      | Security Support Provider                  | Impair Defenses (1/11)                            | /etc/passwd and /etc/shadow                    | Disable or Modify Cloud Firewall                  | Software Deployment Tools                   | Email Collection (0/3)                   | External Proxy                        |                                              |                                  |
|                                          |                                      |                                     | Native API                              | Time Providers                             | Shortcut Modification                      | Disable or Modify Cloud Firewall                  | Cached Domain Credentials                      | Disable or Modify Linux Audit System              | Taint Shared Content                        | Input Capture (0/4)                      | Internal Proxy                        |                                              |                                  |
|                                          |                                      |                                     | Scheduled Task/Job (1/5)                | Winlogon Helper DLL                        | Time Providers                             | Disable or Modify Cloud Logs                      | DCSync                                         | Disable or Modify System Firewall                 | Use Alternate Authentication Material (0/4) | Screen Capture                           | Multi-hop Proxy                       |                                              |                                  |
|                                          |                                      |                                     | At                                      | XDG Autostart Entries                      | Time Providers                             | Disable or Modify Linux Audit System              | LSA Secrets                                    | Disable or Modify Tools                           |                                             | Video Capture                            | Remote Access Software                |                                              |                                  |
|                                          |                                      |                                     | Container Orchestration Job             | Boot or Logon Initialization Scripts (0/5) | Winlogon Helper DLL                        | Disable or Modify System Firewall                 | LSASS Memory                                   | Disable or Modify Tools                           |                                             |                                          | Traffic Signaling                     |                                              |                                  |
|                                          |                                      |                                     | Cron                                    | Shortcut Modification                      | XDG Autostart Entries                      | Disable or Modify Tools                           | NTDS                                           | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | Scheduled Task                          | Time Providers                             | Boot or Logon Initialization Scripts (0/5) | Disable or Modify Tools                           | Proc Filesystem                                | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | Systemd Timers                          | Winlogon Helper DLL                        | Create or Modify System Process (1/4)      | Disable or Modify Tools                           | Security Account Manager                       | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | Serverless Execution                    | XDG Autostart Entries                      | Launch Agent                               | Disable or Modify Tools                           | Steal Application Access Token                 | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | Shared Modules                          | Boot or Logon Initialization Scripts (0/5) | Launch Daemon                              | Disable or Modify Tools                           | Steal or Forge Authentication Certificates     | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | Software Deployment Tools               | Create or Modify System Process (1/4)      | Systemd Service                            | Disable or Modify Tools                           | Steal Web Session Cookie                       | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | System Services (1/2)                   | Launch Agent                               | Windows Service                            | Disable or Modify Tools                           | Unsecured Credentials (1/8)                    | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | Launchctl                               | Launch Daemon                              | Event Triggered Execution (0/16)           | Disable or Modify Tools                           | Bash History                                   | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | Service Execution                       | Systemd Service                            | External Remote Services                   | Disable or Modify Tools                           |                                                | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | User Execution (0/3)                    | Windows Service                            | Hijack Execution                           | Disable or Modify Tools                           |                                                | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     | Windows Management Instrumentation      | Event Triggered Execution (0/16)           |                                            | Disable or Modify Tools                           |                                                | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     |                                         | External Remote Services                   |                                            | Disable or Modify Tools                           |                                                | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |
|                                          |                                      |                                     |                                         | Hijack Execution                           |                                            | Disable or Modify Tools                           |                                                | Disable or Modify Tools                           |                                             |                                          |                                       |                                              |                                  |

Mitre ATT&CK® Navigator v4.9.1

\* PIG: Padvish-Indexed Group

(ح) کلیه حقوق متعلق به شرکت نرم افزاری امن پرداز است



Amnpardaz.com

# PIG.007-EdalatAli

| Reconnaissance<br>10 techniques                                                                                                                                                                                                                                                                                                                                                                                                                  | Resource Development<br>8 techniques                                                                                                                                                                                                                                                                                                     | Initial Access<br>10 techniques                                                                                                                                                                                                                                                                                                                      | Execution<br>14 techniques                                                                                                                                                                                                                                                                                                                                                                                        | Persistence<br>20 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Privilege Escalation<br>14 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Defense Evasion<br>43 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Credential Access<br>17 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Discovery<br>32 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Lateral Movement<br>9 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Collection<br>17 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                | Command and Control<br>17 techniques                                                                                                                                                                                                                                                                                                                                                                                                               | Exfiltration<br>9 techniques                                                                                                                                                                                                                                                                                                                                                                                                           | Impact<br>14 techniques                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active Scanning (0/1)<br>Scanning IP Blocks<br>Vulnerability Scanning<br>Wordlist Scanning<br>Gather Victim Host Information (0/4)<br>Gather Victim Identity Information (0/3)<br>Gather Victim Network Information (0/6)<br>Gather Victim Org Information (0/4)<br>Phishing for Information (0/4)<br>Search Closed Sources (0/2)<br>Search Open Technical Databases (0/5)<br>Search Open Websites/Domains (0/3)<br>Search Victim-Owned Websites | Acquire Access<br>Acquire Infrastructure (0/8)<br>Compromise Accounts (0/3)<br>Compromise Infrastructure (0/7)<br>Develop Capabilities (0/4)<br>Establish Accounts (0/3)<br>Obtain Capabilities (1/6)<br>Code Signing Certificates<br>Digital Certificates<br>Exploits<br>Malware<br>Tool<br>Vulnerabilities<br>Stage Capabilities (0/6) | Content Injection<br>Drive-by Compromise<br>Exploit Public-Facing Application<br>External Remote Services<br>Hardware Additions<br>Phishing (0/4)<br>Replication Through Removable Media<br>Supply Chain Compromise (0/3)<br>Trusted Relationship<br>Valid Accounts (1/4)<br>Cloud Accounts<br>Default Accounts<br>Domain Accounts<br>Local Accounts | Cloud Administration Command<br>Command and Scripting Interpreter (0/9)<br>Container Administration Command<br>Deploy Container<br>Exploitation for Client Execution<br>Inter-Process Communication (0/3)<br>Native API<br>Scheduled Task/Job (0/5)<br>Serverless Execution<br>Shared Modules<br>Software Deployment Tools<br>System Services (0/2)<br>User Execution (0/3)<br>Windows Management Instrumentation | Account Manipulation (0/6)<br>BITS Jobs<br>Boot or Logon Autostart Execution (0/14)<br>Boot or Logon Initialization Scripts (0/5)<br>Browser Extensions<br>Compromise Client Software Binary<br>Create Account (1/3)<br>Cloud Account<br>Domain Account<br>Local Account<br>Create or Modify System Process (0/4)<br>Event Triggered Execution (0/16)<br>External Remote Services<br>Hijack Execution Flow (0/12)<br>Process Injection (0/12)<br>Implant Internal Image<br>Modify Authentication Process (0/8)<br>Office Application Startup (0/6)<br>Power Settings<br>Pre-OS Boot (0/5)<br>Scheduled Task/Job (0/5)<br>Server Software Component (1/5)<br>IIS Components<br>SQL Stored Procedures<br>Terminal Services DLL<br>Transport Agent<br>Web Shell<br>Traffic Signaling (0/2)<br>Valid Accounts (1/4) | Abuse Elevation Control Mechanism (0/5)<br>Access Token Manipulation (0/5)<br>Account Manipulation (0/6)<br>Boot or Logon Autostart Execution (0/14)<br>Boot or Logon Initialization Scripts (0/5)<br>Boot or Logon Initialization Scripts (0/5)<br>Create or Modify System Process (0/4)<br>Domain Policy Modification (0/2)<br>Escape to Host<br>Event Triggered Execution (0/16)<br>Exploitation for Privilege Escalation<br>Hijack Execution Flow (0/12)<br>Process Injection (0/12)<br>Scheduled Task/Job (0/5)<br>Valid Accounts (1/4)<br>Cloud Accounts<br>Default Accounts<br>Domain Accounts<br>Local Accounts<br>Clear Persistence<br>Clear Windows Event Logs<br>File Deletion<br>Network Share Connection Removal<br>Timestamp | Abuse Elevation Control Mechanism (0/5)<br>Access Token Manipulation (0/5)<br>BITS Jobs<br>Build Image on Host<br>Debugger Evasion<br>Deobfuscate/Decode Files or Information<br>Deploy Container<br>Direct Volume Access<br>Domain Policy Modification (0/2)<br>Execution Guardrails (0/1)<br>Exploitation for Defense Evasion<br>File and Directory Permissions Modification (0/2)<br>Hide Artifacts (0/11)<br>Hijack Execution Flow (0/12)<br>Impair Defenses (0/11)<br>Impersonation<br>Indicator Removal (1/9)<br>Clear Command History<br>Clear Linux or Mac System Logs<br>Clear Mailbox Data<br>Clear Network Connection History and Configurations<br>Clear Persistence<br>Clear Windows Event Logs<br>File Deletion<br>Network Share Connection Removal<br>Timestamp<br>Indirect Command Execution<br>Masquerading (0/9)<br>Modify Authentication Process (0/8)<br>Modify Cloud Compute Infrastructure (0/5)<br>Modify Registry | Adversary-in-the-Middle (0/3)<br>Brute Force (1/4)<br>Credential Stuffing<br>Password Cracking<br>Password Guessing<br>Password Spraying<br>Credentials from Password Stores (0/6)<br>Exploitation for Credential Access<br>Forced Authentication<br>Forge Web Credentials (0/2)<br>Input Capture (0/4)<br>Modify Authentication Process (0/8)<br>Multi-Factor Authentication Interception<br>Multi-Factor Authentication Request Generation<br>Network Sniffing<br>OS Credential Dumping (1/8)<br>/etc/passwd and /etc/shadow<br>Cached Domain Credentials<br>DCSync<br>LSA Secrets<br>LSASS Memory<br>NTDS<br>Proc Filesystem<br>Security Account Manager<br>Steal Application Access Token<br>Steal or Forge Authentication Certificates<br>Steal or Forge Kerberos Tickets (0/4)<br>Steal Web Session | Account Discovery (0/4)<br>Application Window Discovery<br>Browser Information Discovery<br>Cloud Infrastructure Discovery<br>Cloud Service Dashboard<br>Cloud Service Discovery<br>Cloud Storage Object Discovery<br>Container and Resource Discovery<br>Debugger Evasion<br>Device Driver Discovery<br>Domain Trust Discovery<br>File and Directory Discovery<br>Group Policy Discovery<br>Log Enumeration<br>Network Service Discovery<br>Network Share Discovery<br>Network Sniffing<br>Password Policy Discovery<br>Peripheral Device Discovery<br>Permission Groups Discovery (0/3)<br>Process Discovery<br>Query Registry<br>Remote System Discovery<br>Software Discovery (0/1)<br>System Information Discovery<br>System Location Discovery (0/1)<br>System Network Configuration Discovery (0/2)<br>System Network Connections Discovery<br>System Owner/User Discovery<br>System Service Discovery<br>System Time Discovery<br>Virtualization/Sandbox Evasion (0/3) | Exploitation of Remote Services<br>Internal Spearphishing<br>Lateral Tool Transfer<br>Remote Service Session Hijacking (0/2)<br>Remote Services (1/8)<br>Cloud Services<br>Direct Cloud VM Connections<br>Distributed Component Object Model<br>Remote Desktop Protocol<br>SMB/Windows Admin Shares<br>SSH<br>VNC<br>Windows Remote Management<br>Replication Through Removable Media<br>Software Deployment Tools<br>Taint Shared Content<br>Use Alternate Authentication Material (0/4) | Adversary-in-the-Middle (0/3)<br>Archive Collected Data (0/3)<br>Audio Capture<br>Automated Collection<br>Browser Session Hijacking<br>Clipboard Data<br>Data from Cloud Storage<br>Data from Configuration Repository (0/2)<br>Data from Information Repositories (0/3)<br>Data from Local System<br>Data from Network Shared Drive<br>Data from Removable Media<br>Data Staged (0/2)<br>Email Collection (0/3)<br>Input Capture (0/4)<br>Screen Capture<br>Video Capture | Application Layer Protocol (0/4)<br>Communication Through Removable Media<br>Content Injection<br>Data Encoding (0/2)<br>Data Obfuscation (0/3)<br>Dynamic Resolution (0/3)<br>Encrypted Channel (0/2)<br>Fallback Channels<br>Ingress Tool Transfer<br>Multi-Stage Channels<br>Non-Application Layer Protocol<br>Non-Standard Port<br>Protocol Tunneling<br>Proxy (0/4)<br>Remote Access Software<br>Traffic Signaling (0/2)<br>Web Service (0/3) | Automated Exfiltration (0/1)<br>Data Transfer Size Limits<br>Exfiltration Over Alternative Protocol (0/3)<br>Exfiltration Over C2 Channel<br>Exfiltration Over Other Network Medium (0/1)<br>Exfiltration Over Physical Medium (0/1)<br>Exfiltration Over Web Service (0/4)<br>Scheduled Transfer<br>Transfer Data to Cloud Account<br>Network Denial of Service (0/2)<br>Resource Hijacking<br>Service Stop<br>System Shutdown/Reboot | Account Access Removal<br>Data Destruction<br>Data Encrypted for Impact<br>Data Manipulation (0/3)<br>Defacement (1/2)<br>External Defacement<br>Internal Defacement<br>Disk Wipe (0/2)<br>Endpoint Denial of Service (0/4)<br>Financial Theft<br>Firmware Corruption<br>Inhibit System Recovery<br>Network Denial of Service (0/2)<br>Resource Hijacking<br>Service Stop<br>System Shutdown/Reboot |



MITRE ATT&CK® Navigator v4.9.1





# PIG.008-GonjeshkeDarande

| Reconnaissance<br>10 techniques                                                                                                                                                                                                                                                                                                                                             | Resource Development<br>8 techniques                                                                                                                                                                                              | Initial Access<br>10 techniques                                                                                                                                                                                                                                           | Execution<br>14 techniques                                                                                                                                                                                                                                                                                                                                                                                                                          | Persistence<br>20 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Privilege Escalation<br>14 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Defense Evasion<br>43 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Credential Access<br>17 techniques                                                                                                                                                                                                                                                                                                                                                                                                                            | Discovery<br>32 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Lateral Movement<br>9 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Collection<br>17 techniques                                                                                                                                                                                                                                                                                                                                                                                                                                                | Command and Control<br>17 techniques                                                                                                                                                                                                                                                                                                                                                                                                               | Exfiltration<br>9 techniques                                                                                                                                                                                                                                                                                                        | Impact<br>14 techniques                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active Scanning (0/3)<br>Gather Victim Host Information (0/4)<br>Gather Victim Identity Information (0/3)<br>Gather Victim Network Information (0/6)<br>Gather Victim Org Information (0/4)<br>Phishing for Information (0/4)<br>Search Closed Sources (0/2)<br>Search Open Technical Databases (0/5)<br>Search Open Websites/Domains (0/3)<br>Search Victim-Owned Websites | Acquire Access<br>Acquire Infrastructure (0/8)<br>Compromise Accounts (0/3)<br>Compromise Infrastructure (0/7)<br>Develop Capabilities (0/4)<br>Establish Accounts (0/3)<br>Obtain Capabilities (0/6)<br>Stage Capabilities (0/6) | Content Injection<br>Drive-by Compromise<br>Exploit Public-Facing Application<br>External Remote Services<br>Hardware Additions<br>Phishing (0/4)<br>Replication Through Removable Media<br>Supply Chain Compromise (0/3)<br>Trusted Relationship<br>Valid Accounts (0/4) | Cloud Administration Command<br>Command and Scripting Interpreter (0/9)<br>Container Administration Command<br>Deploy Container<br>Exploitation for Client Execution<br>Inter-Process Communication (0/3)<br>Native API<br>Scheduled Task/Job (0/5)<br>Serverless Execution<br>Shared Modules<br>Software Deployment Tools<br>System Services (1/2)<br>Launchctl<br>Service Execution<br>User Execution (0/3)<br>Windows Management Instrumentation | Account Manipulation (0/6)<br>BITS Jobs<br>Boot or Logon Autostart Execution (1/14)<br>Active Setup<br>Authentication Package<br>Kernel Modules and Extensions<br>Login Items<br>LSASS Driver<br>Port Monitors<br>Print Processors<br>Re-opened Applications<br>Registry Run Keys / Startup Folder<br>Security Support Provider<br>Shortcut Modification<br>Time Providers<br>Winlogon Helper DLL<br>XDG Autostart Entries<br>Boot or Logon Initialization Scripts (0/5)<br>Browser Extensions<br>Compromise Client Software Binary<br>Create Account (0/3)<br>Create or Modify System Process (1/4)<br>Launch Agent<br>Launch Daemon<br>Systemd Service<br>Windows Service<br>Event Triggered Execution (0/16)<br>External Remote Services<br>Hijack Execution | Abuse Elevation Control Mechanism (0/5)<br>Access Token Manipulation (0/5)<br>Account Manipulation (0/6)<br>Boot or Logon Autostart Execution (1/14)<br>Boot or Logon Initialization Scripts (0/5)<br>Create or Modify System Process (1/4)<br>Domain Policy Modification (0/2)<br>Escape to Host<br>Event Triggered Execution (0/16)<br>Exploitation for Privilege Escalation<br>Hijack Execution Flow (0/12)<br>Process Injection (0/12)<br>Scheduled Task/Job (0/5)<br>Valid Accounts (0/4) | Abuse Elevation Control Mechanism (0/5)<br>Access Token Manipulation (0/5)<br>BITS Jobs<br>Build Image on Host<br>Debugger Evasion<br>Deobfuscate/Decode Files or Information<br>Deploy Container<br>Direct Volume Access<br>Domain Policy Modification (0/2)<br>Execution Guardrails (0/1)<br>Exploitation for Defense Evasion<br>File and Directory Permissions Modification (0/2)<br>Hide Artifacts (0/11)<br>Hijack Execution Flow (0/12)<br>Impair Defenses (0/11)<br>Impersonation | Adversary-in-the-Middle (0/3)<br>Brute Force (0/4)<br>Credentials from Password Stores (0/6)<br>Exploitation for Credential Access<br>Forced Authentication<br>Forge Web Credentials (0/2)<br>Input Capture (0/4)<br>Modify Authentication Process (0/8)<br>Multi-Factor Authentication Interception<br>Multi-Factor Authentication Request Generation<br>Network Sniffing<br>OS Credential Dumping (0/8)<br>Steal Application Access Token<br>Steal or Forge | Account Discovery (0/4)<br>Application Window Discovery<br>Browser Information Discovery<br>Cloud Infrastructure Discovery<br>Cloud Service Dashboard<br>Cloud Service Discovery<br>Cloud Storage Object Discovery<br>Container and Resource Discovery<br>Debugger Evasion<br>Device Driver Discovery<br>Domain Trust Discovery<br>File and Directory Discovery<br>Group Policy Discovery<br>Log Enumeration<br>Network Service Discovery<br>Network Share Discovery<br>Network Sniffing<br>Password Policy Discovery<br>Peripheral Device Discovery | Exploitation of Remote Services<br>Internal Spearphishing<br>Lateral Tool Transfer<br>Remote Service Session Hijacking (0/2)<br>Remote Services (0/8)<br>Replication Through Removable Media<br>Software Deployment Tools<br>Taint Shared Content<br>Use Alternate Authentication Material (0/4)<br>Group Policy Discovery<br>Log Enumeration<br>Network Service Discovery<br>Network Share Discovery<br>Network Sniffing<br>Password Policy Discovery<br>Peripheral Device Discovery | Adversary-in-the-Middle (0/3)<br>Archive Collected Data (0/3)<br>Audio Capture<br>Automated Collection<br>Browser Session Hijacking<br>Clipboard Data<br>Data from Cloud Storage<br>Data from Configuration Repository (0/2)<br>Data from Information Repositories (0/3)<br>Data from Local System<br>Data from Network Shared Drive<br>Data from Removable Media<br>Data Staged (0/2)<br>Email Collection (0/3)<br>Input Capture (0/4)<br>Screen Capture<br>Video Capture | Application Layer Protocol (0/4)<br>Communication Through Removable Media<br>Content Injection<br>Data Encoding (0/2)<br>Data Obfuscation (0/3)<br>Dynamic Resolution (0/3)<br>Encrypted Channel (0/2)<br>Fallback Channels<br>Ingress Tool Transfer<br>Multi-Stage Channels<br>Non-Application Layer Protocol<br>Non-Standard Port<br>Protocol Tunneling<br>Proxy (0/4)<br>Remote Access Software<br>Traffic Signaling (0/2)<br>Web Service (0/3) | Automated Exfiltration (0/1)<br>Data Transfer Size Limits<br>Exfiltration Over Alternative Protocol (0/3)<br>Exfiltration Over C2 Channel<br>Exfiltration Over Other Network Medium (0/1)<br>Exfiltration Over Physical Medium (0/1)<br>Exfiltration Over Web Service (0/4)<br>Scheduled Transfer<br>Transfer Data to Cloud Account | Account Access Removal<br>Data Destruction<br>Data Encrypted for Impact<br>Data Manipulation (0/3)<br>Defacement (0/2)<br>Disk Wipe (0/2)<br>Endpoint Denial of Service (0/4)<br>Financial Theft<br>Firmware Corruption<br>Inhibit System Recovery<br>Network Denial of Service (0/2)<br>Resource Hijacking<br>Service Stop<br>System Shutdown/Reboot |

MITRE ATT&CK® Navigator v4.9.1

\* PIG: Padvish-Indexed Group

ز است



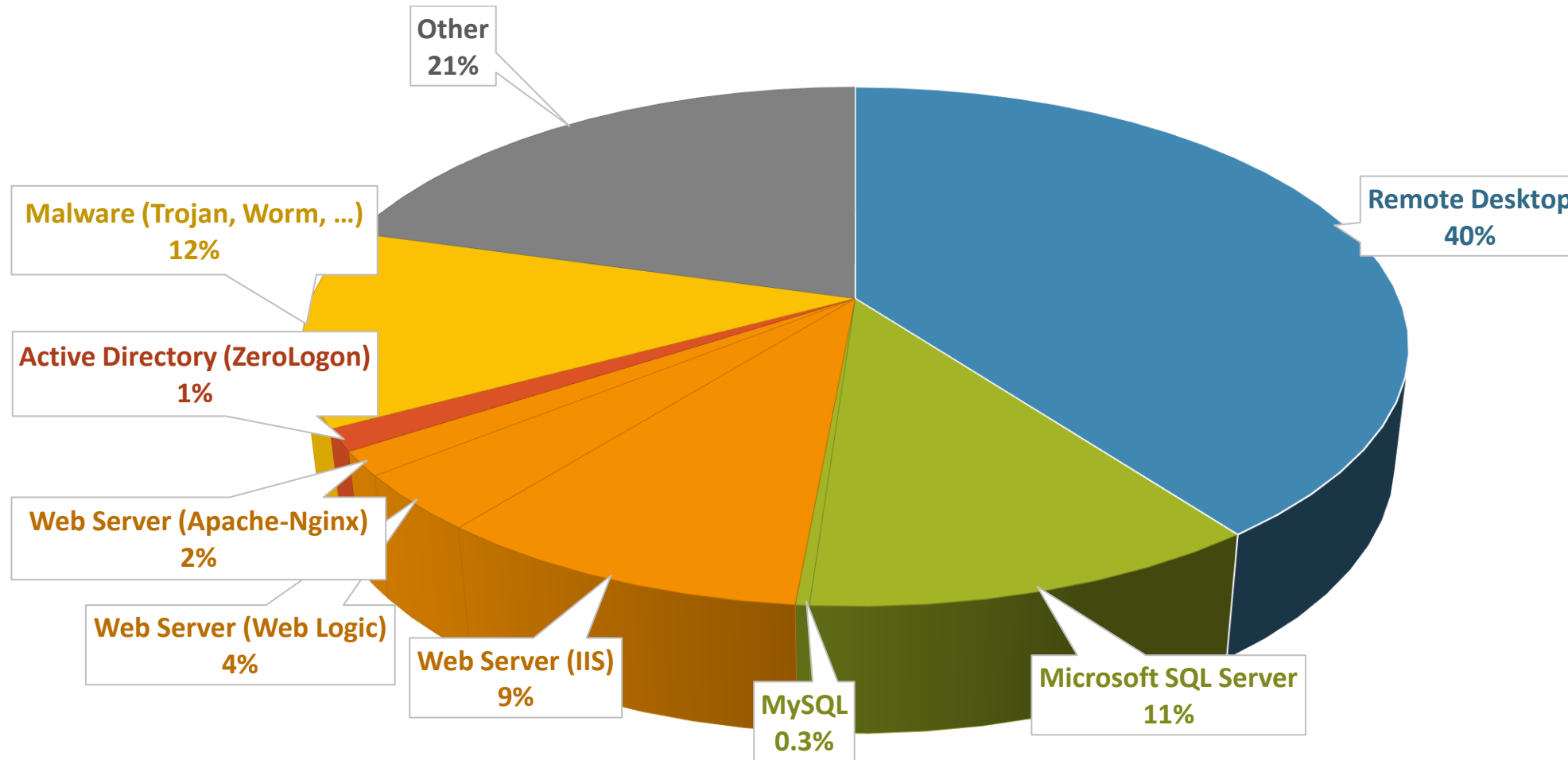
iz.com

# PIG.009-Chameleon

| Reconnaissance<br>10 techniques          | Resource Development<br>8 techniques | Initial Access<br>11 techniques                              | Execution<br>16 techniques               | Persistence<br>23 techniques                         | Privilege Escalation<br>14 techniques        | Defense Evasion<br>45 techniques             | Credential Access<br>17 techniques                   | Discovery<br>33 techniques                        | Lateral Movement<br>9 techniques            | Collection<br>17 techniques              | Command and Control<br>18 techniques        | Exfiltration<br>9 techniques                 | Impact<br>15 techniques          |
|------------------------------------------|--------------------------------------|--------------------------------------------------------------|------------------------------------------|------------------------------------------------------|----------------------------------------------|----------------------------------------------|------------------------------------------------------|---------------------------------------------------|---------------------------------------------|------------------------------------------|---------------------------------------------|----------------------------------------------|----------------------------------|
| Active Scanning (0/1)                    | Acquire Access (0/8)                 | Content Injection (0/3)                                      | Cloud Administration Command (0/12)      | Account Manipulation (0/7)                           | Abuse Elevation Control Mechanism (0/6)      | Abuse Elevation Control Mechanism (0/6)      | Adversary-in-the-Middle (0/4)                        | Account Discovery (0/4)                           | Exploitation of Remote Services (0/2)       | Adversary-in-the-Middle (0/4)            | Application Layer Protocol (0/5)            | Automated Exfiltration (0/1)                 | Account Access Removal (0/1)     |
| Gather Victim Host Information (0/4)     | Acquire Infrastructure (0/8)         | Drive-by Compromise (0/3)                                    | Command and Scripting Interpreter (0/12) | BITS Jobs (0/3)                                      | Access Token Manipulation (0/5)              | Access Token Manipulation (0/5)              | Brute Force (0/4)                                    | Application Window Discovery (0/2)                | Internal Spearphishing (0/2)                | Archive Collected Data (0/3)             | Communication Through Removable Media (0/2) | Data Transfer Size Limits (0/1)              | Data Destruction (0/1)           |
| Gather Victim Identity Information (0/3) | Compromise Accounts (0/3)            | Exploit Public-Facing Application (0/3)                      | AppleScript (0/3)                        | Boot or Logon Autostart Execution (0/14)             | Account Manipulation (0/7)                   | Account Manipulation (0/7)                   | Credentials from Password Stores (0/4)               | Browser Information Discovery (0/2)               | Lateral Tool Transfer (0/2)                 | Audio Capture (0/2)                      | Content Injection (0/2)                     | Data Encrypted for Impact (0/3)              | Data Encrypted for Impact (0/3)  |
| Gather Victim Network Information (0/4)  | Compromise Infrastructure (0/4)      | External Remote Services (0/3)                               | AutoHotKey & AutoIT (0/3)                | Boot or Logon Autostart Initialization Scripts (0/9) | Boot or Logon Autostart Execution (0/14)     | Boot or Logon Autostart Execution (0/14)     | Exploitation for Credential Access (0/2)             | Cloud Infrastructure Discovery (0/2)              | Remote Service Session Hijacking (0/2)      | Automated Collection (0/2)               | Data Encoding (0/2)                         | Exfiltration Over Alternative Protocol (0/3) | Data Manipulation (0/3)          |
| Gather Victim Org Information (0/4)      | Develop Capabilities (1/4)           | Hardware Additions (0/3)                                     | Cloud API (0/3)                          | Cloud Application Integration (0/3)                  | Boot or Logon Initialization Scripts (0/5)   | Boot or Logon Initialization Scripts (0/5)   | Forced Authentication (0/2)                          | Cloud Service Dashboard (0/2)                     | Remote Services (0/8)                       | Browser Session Hijacking (0/2)          | Data Obfuscation (0/3)                      | Exfiltration Over C2 Channel (0/2)           | Disk Wipe (0/2)                  |
| Phishing for Information (0/4)           | Code Signing Certificates (0/2)      | Phishing (0/4)                                               | Hypervisor CLI (0/3)                     | Compromise Host Software Binary (0/5)                | Create or Modify System Process (1/5)        | Create or Modify System Process (1/5)        | Forge Web Credentials (0/2)                          | Cloud Storage Object Discovery (0/2)              | Cloud Services (0/2)                        | Data from Cloud Storage (0/2)            | Dynamic Resolution (0/3)                    | Exfiltration Over Other Network Medium (0/1) | Email Bombing (0/2)              |
| Search Closed Sources (0/2)              | Digital Certificates (0/2)           | Replication Through Removable Media (0/3)                    | JavaScript (0/3)                         | Container Service (0/3)                              | Container Service (0/3)                      | Container Service (0/3)                      | Input Capture (0/4)                                  | Container and Resource Discovery (0/2)            | Direct Cloud VM Connections (0/2)           | Data from Configuration Repository (0/2) | Encrypted Channel (0/2)                     | Exfiltration Over Physical Medium (0/1)      | Endpoint Denial of Service (0/4) |
| Search Open Technical Databases (0/2)    | Exploits (0/2)                       | Supply Chain Compromise (1/3)                                | Lua (0/3)                                | Create Account (0/3)                                 | Launch Agent (0/3)                           | Launch Agent (0/3)                           | Modify Authentication Process (0/2)                  | Debugger Evasion (0/2)                            | Distributed Component Object Model (0/2)    | Data from Information Repositories (0/3) | Fallback Channels (0/2)                     | Exfiltration Over Web Service (0/4)          | Financial Theft (0/2)            |
| Search Open Websites/Domains (0/3)       | Malware (0/2)                        | Compromise Hardware Supply Chain (0/3)                       | Network Device CLI (0/3)                 | Create or Modify System Process (1/5)                | Launch Daemon (0/3)                          | Launch Daemon (0/3)                          | Multi-Factor Authentication Interception (0/2)       | Device Driver Discovery (0/2)                     | Remote Desktop Protocol (0/2)               | Data from Local System (0/2)             | Hide Infrastructure (0/2)                   | Scheduled Transfer (0/2)                     | Firmware Corruption (0/2)        |
| Search Victim-Owned Websites (0/3)       | Establish Accounts (0/3)             | Compromise Software Dependencies and Development Tools (0/3) | PowerShell (0/3)                         | Container Service (0/3)                              | Systemd Service (0/3)                        | Systemd Service (0/3)                        | Multi-Factor Authentication Request Generation (0/2) | Domain Trust Discovery (0/2)                      | SMB/Windows Admin Shares (0/2)              | Data from Network Shared Drive (0/2)     | Ingress Tool Transfer (0/2)                 | Transfer Data to Cloud Account (0/2)         | Network Denial of Service (0/2)  |
|                                          | Obtain Capabilities (1/7)            | Compromise Software Supply Chain (0/3)                       | Python (0/3)                             | Launch Agent (0/3)                                   | Domain or Tenant Policy Modification (0/2)   | Domain or Tenant Policy Modification (0/2)   | Network Sniffing (0/2)                               | File and Directory Permissions Modification (0/2) | SSH (0/2)                                   | Data from Removable Media (0/2)          | Non-Application Layer Protocol (0/2)        | Resource Hijacking (0/4)                     | Service Stop (0/2)               |
|                                          | Artificial Intelligence (0/2)        | Trusted Relationship (0/3)                                   | Unix Shell (0/3)                         | Launch Daemon (0/3)                                  | Escape to Host (0/2)                         | Escape to Host (0/2)                         | OS Credential Dumping (0/6)                          | Network Service Discovery (0/2)                   | VNC (0/2)                                   | Data Staged (0/2)                        | Non-Standard Port (0/2)                     | System Shutdown/Reboot (0/2)                 |                                  |
|                                          | Code Signing Certificates (0/2)      | Valid Accounts (0/4)                                         | Visual Basic (0/3)                       | Systemd Service (0/3)                                | Event Triggered Execution (0/17)             | Event Triggered Execution (0/17)             | Steal Application Access Token (0/2)                 | Network Share Discovery (0/2)                     | Windows Remote Management (0/2)             | Email Collection (0/3)                   | Protocol Tunneling (0/2)                    |                                              |                                  |
|                                          | Digital Certificates (0/2)           | Cloud Accounts (0/4)                                         | Windows Command Shell (0/3)              | Windows Service (0/3)                                | Exploitation for Privilege Escalation (0/12) | Exploitation for Privilege Escalation (0/12) | Steal or Forge Authentication Certificates (0/5)     | Network Sniffing (0/2)                            | Replication Through Removable Media (0/2)   | Input Capture (0/4)                      | Domain Fronting (0/2)                       |                                              |                                  |
|                                          | Exploits (0/2)                       | Default Accounts (0/4)                                       | Container Administration Command (0/12)  | Exclusive Control (0/12)                             | Process Injection (1/12)                     | Process Injection (1/12)                     | Steal or Forge Kerberos Tickets (0/5)                | Password Policy Discovery (0/2)                   | Software Deployment Tools (0/2)             | Screen Capture (0/4)                     | External Proxy (0/2)                        |                                              |                                  |
|                                          | Malware (0/2)                        | Domain Accounts (0/4)                                        | Deploy Container (0/17)                  | External Remote Services (0/12)                      | Masquerading (1/11)                          | Masquerading (1/11)                          | Unsecured Credentials (0/5)                          | Peripheral Device Discovery (0/2)                 | Taint Shared Content (0/2)                  | Video Capture (0/2)                      | Internal Proxy (0/2)                        |                                              |                                  |
|                                          | Tool (0/2)                           | Local Accounts (0/4)                                         | ESXi Administration Command (0/12)       | Hijack Execution Flow (0/12)                         | Indirect Command Execution (0/12)            | Indirect Command Execution (0/12)            |                                                      | Permission Groups Discovery (0/3)                 | Use Alternate Authentication Material (0/4) |                                          | Multi-hop Proxy (0/2)                       |                                              |                                  |
|                                          | Vulnerabilities (0/2)                |                                                              | Exploitation for Client Execution (0/12) | Implant Internal Image (0/12)                        | Asynchronous Procedure Call (0/12)           | Asynchronous Procedure Call (0/12)           |                                                      | Process Discovery (0/3)                           |                                             |                                          | Remote Access Tools (0/3)                   |                                              |                                  |
|                                          | Stage Capabilities (0/4)             |                                                              | Input Injection (0/12)                   | Modify Authentication Process (0/9)                  | Dynamic-link Library Injection (0/12)        | Dynamic-link Library Injection (0/12)        |                                                      | Query Registry (0/3)                              |                                             |                                          | Traffic Signaling (0/2)                     |                                              |                                  |
|                                          |                                      |                                                              | Inter-Process Communication (0/3)        | Modify Registry (0/9)                                | Extra Window Memory Injection (0/12)         | Extra Window Memory Injection (0/12)         |                                                      | Remote System Discovery (0/3)                     |                                             |                                          | Web Service (0/3)                           |                                              |                                  |
|                                          |                                      |                                                              | Native API (0/3)                         | Office Application Startup (0/9)                     | ListPlanting (0/12)                          | ListPlanting (0/12)                          |                                                      | Software Discovery (0/7)                          |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | Scheduled Task/Job (0/5)                 | Power Settings (0/9)                                 | Portable Executable Injection (0/12)         | Portable Executable Injection (0/12)         |                                                      | System Information Discovery (0/7)                |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | Serverless Execution (0/5)               | Pre-OS Boot (0/3)                                    | Proc Memory (0/12)                           | Proc Memory (0/12)                           |                                                      | System Location Discovery (0/11)                  |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | Shared Modules (0/5)                     | Scheduled Task/Job (0/3)                             | Process Doppelganging (0/12)                 | Process Doppelganging (0/12)                 |                                                      | System Network Configuration Discovery (0/2)      |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | Software Deployment Tools (0/5)          | Scheduled Task/Job (0/3)                             | Process Hollowing (0/12)                     | Process Hollowing (0/12)                     |                                                      | System Network Connections Discovery (0/2)        |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | System Services (1/3)                    | Server Software Component (0/3)                      | Ptrace System Calls (0/12)                   | Ptrace System Calls (0/12)                   |                                                      | System Owner/User Discovery (0/2)                 |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | Launchctl (0/3)                          | Software Extensions (0/2)                            | Thread Execution Hijacking (0/12)            | Thread Execution Hijacking (0/12)            |                                                      | System Service Discovery (0/2)                    |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | Service Execution (0/3)                  | Traffic Signaling (0/2)                              | Thread Local Storage (0/12)                  | Thread Local Storage (0/12)                  |                                                      | System Time Discovery (0/2)                       |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | Systemctl (0/3)                          | Valid Accounts (0/4)                                 | VOSO Hijacking (0/12)                        | VOSO Hijacking (0/12)                        |                                                      | Virtual Machine Discovery (0/2)                   |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | User Execution (0/4)                     | Cloud Accounts (0/4)                                 | Scheduled Task/Job (0/5)                     | Scheduled Task/Job (0/5)                     |                                                      | Virtualization/Sandbox Evasion (0/3)              |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              | Windows Management Instrumentation (0/4) | Default Accounts (0/4)                               | Valid Accounts (0/4)                         | Valid Accounts (0/4)                         |                                                      |                                                   |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              |                                          | Domain Accounts (0/4)                                | Cloud Accounts (0/4)                         | Cloud Accounts (0/4)                         |                                                      |                                                   |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              |                                          | Local Accounts (0/4)                                 | Default Accounts (0/4)                       | Default Accounts (0/4)                       |                                                      |                                                   |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              |                                          |                                                      | Domain Accounts (0/4)                        | Domain Accounts (0/4)                        |                                                      |                                                   |                                             |                                          |                                             |                                              |                                  |
|                                          |                                      |                                                              |                                          |                                                      | Local Accounts (0/4)                         | Local Accounts (0/4)                         |                                                      |                                                   |                                             |                                          |                                             |                                              |                                  |



# روش نفوذ اولیه - در حملات سایبری اخیر



Source: Amnpardaz CSIRT 2024

(ح) کلیه حقوق متعلق به شرکت نرم‌افزاری امن‌پرداز است



# مطالعه موردی حملات سایبری

# پرونده اول

حمله در سطح مجازی سازی (Hyper-visor)





# BreakESX

Initial Access

Dropper

Persistence

local.sh

welcome

...

Impact

Kill all  
VMs

Stop ESX  
Services

Wipe  
VMDKs



# BreakESX

استقرار فایل local.sh  
استقرار فایل welcome  
بستن پورت‌ها توسط فایروال  
ذخیره‌سازی کانفیگ بوت (autobackup.sh)

Initial Access

...opper

Persistence

local.sh

welcome

...

Impact

Kill all  
VMs

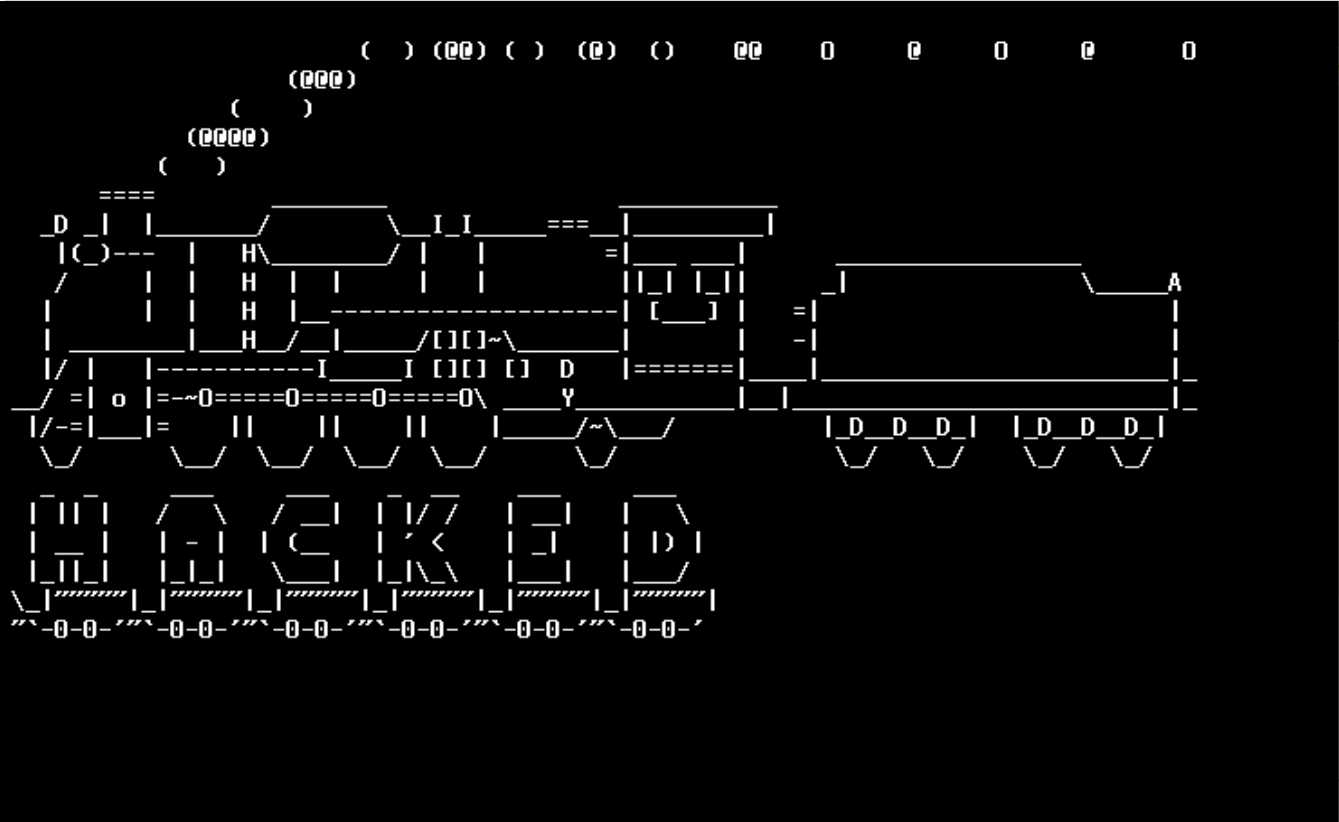
Stop ESX  
Services

Wipe  
VMDKs



# BreakESX

## Initial Access



Dropped

- نمایش پیام در صورت:
- UEFI Secure Boot
  - عدم اجرای صحیح local.sh

welcome

...

Wipe  
VMDKs



# BreakESX

1. بستن پردازنده‌های مدیریتی
2. توقف کلیدهای ماشین‌های مجازی
3. متوقف‌سازی سرویس‌های حیاتی سیستم عامل VMware ESXi
4. غیرفعال کردن کلیدهای دسترسی‌ها از راه دور
5. تخریب اطلاعات بوت سیستم‌عامل (و خود اسکریپت بدافزار)
6. از بین بردن کامل کل دیسک‌های ماشین‌های مجازی

Dropper

Persistence

Impact

Kill  
VM

VMware Hypervisor Recovery

```
BANK5: invalid update counter.  
BANK5: invalid build number.  
BANK6: invalid update counter.  
BANK6: invalid build number.  
No hypervisor found.
```

# پرونده دوم

حمله زنجیره تامین

PIG.009-Chamelon

# حملات زنجیره تامین

## ❖ تعریف

■ حمله به یک هدف اصلی از طریق خدمات یا محصولات مورد استفاده آن

## ❖ انگیزه

- سازمان‌های بزرگ هزینه بیشتری برای دفاع از خود کرده‌اند و مستقیماً قابل حمله نیستند.
- معمولاً سازمان‌ها به محصولات و خدمات مورد استفاده خود اعتماد دارند و آنها را کمتر بررسی می‌کنند.
- هنگامی که هدف اصلی امن‌تر از آن است که بتوان مستقیم به آن حمله کرد، یافتن ضعیف‌ترین زنجیره جهت حمله مدنظر قرار می‌گیرد.
- یک حمله به یک تامین‌کننده، می‌تواند چندین و چند هدف را متاثر کند.





# حمله SunBurst – Solarwinds

U.S. federal government [ edit ]

| Branch    | Institution                                       | Affected part(s) include                                                            | Assets accessed                                  | Sources                                                      |
|-----------|---------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------------------------|
| Executive | Department of Agriculture                         | National Finance Center                                                             |                                                  | [8][146][88][147][148][93]                                   |
|           | Department of Commerce                            | National Telecommunications and Information Administration                          |                                                  | [149][1][150][151][80][82][75][147][152][153][148][154][155] |
|           | Department of Defense                             | Parts of The Pentagon, National Security Agency, Defense Information Systems Agency |                                                  | [1][156][154][155][157][158]                                 |
|           | Department of Energy                              | National Nuclear Security Administration                                            |                                                  | [3][159][160][161][162][152][153][148][154][163][155]        |
|           | Department of Health and Human Services           | National Institutes of Health                                                       |                                                  | [156][75][153][148]                                          |
|           | Department of Homeland Security                   | Cybersecurity and Infrastructure Security Agency                                    | e-mails of top officials                         | [151][150][80][82][75][1][147][153][148][164][165]           |
|           | Department of Justice                             |                                                                                     | ~3000 Microsoft Office 365-hosted email accounts | [166][7][167][168][169][170][144]                            |
|           | Department of Labor                               | Bureau of Labor Statistics                                                          |                                                  | [2]                                                          |
|           | Department of State                               |                                                                                     |                                                  | [1][156][75][153][148][155]                                  |
|           | United States Department of Transportation        | Federal Aviation Administration                                                     |                                                  | [157]                                                        |
| Judicial  | Department of the Treasury                        |                                                                                     |                                                  | [1][150][156][149][80][82][75][147][152][153][148][46][155]  |
|           | Administrative Office of the United States Courts | Case Management/Electronic Case Files                                               | Court documents, including sealed case files     | [171][172][173][174][175][176][177][178][179]                |

❖ ۲۰۲۰-۱۲-۰۳

❖ مشکوک به روسیه

❖ یکی از بزرگترین حوادث سایبری تاریخ آمریکا:

- هک آمریکا : وزارت خزانه‌داری، وزارت بازرگانی، وزارت ک
- هک سازمان‌های متعددی در ناتو، بریتانیا، اروپا و ...
- حداقل ۱۸۰۰۰ نفر نرم‌افزار آلوده را دانلود کردند
- حداقل ۹ ماه عملیات قبل از کشف

❖ ویژگی‌ها

- استقرار کد درب‌پشتی در بیلدسیستم
- توزیع با نسخه‌های بعدی
- تماس با سه دامنه ظاهراً سالم
- استفاده از درب‌پشتی فقط برای اهداف مهم و دارای ارزش

❖ کشف از طریق بررسی اتفاقات غیرمتعارف در reEye

(ح) کلیه حقوق متعلق به



# حمله SSH/xz

❖ ۲۹-۰۳-۲۰۲۴ CVSS 10/10

❖ حمله به کتابخانه XZ، جهت حمله به SSH، جهت حمله به همه سرورهای لینوکس  
❖ بسیار پیشرفته:

- سه سال مشارکت در پروژه جهت کسب اعتماد (JiaT75)
- در اسکریپت‌های متن‌باز! و علی‌رغم بازرسی کد
- تشخیص محیط کمپایل (تزریق فقط در بیلدسیستم اصلی)
- پنهان کردن کد به عنوان ماژول تست
- تزریق کد پیشرفته

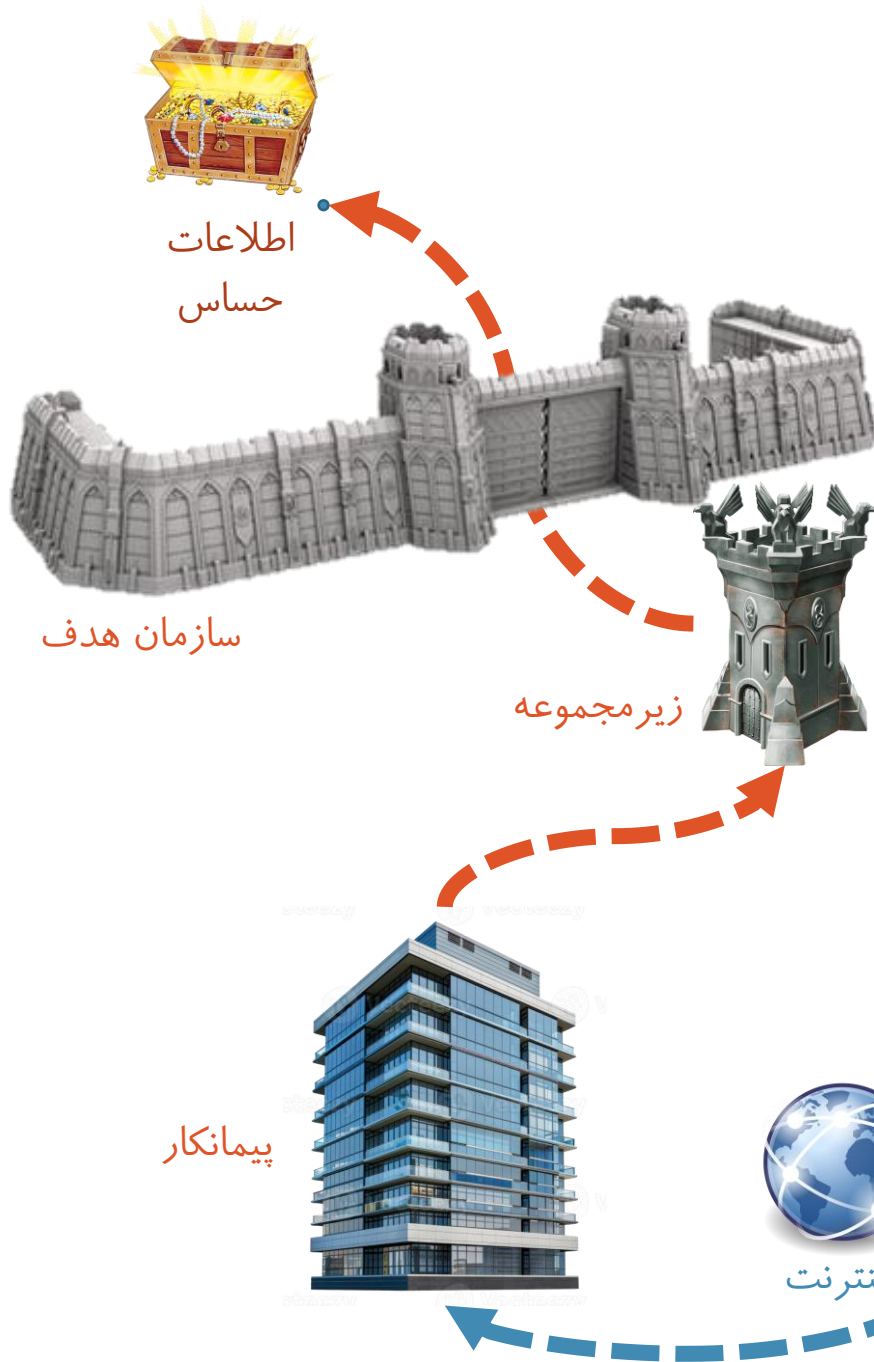
■ جالب آنکه openssh اصلاً از xz استفاده نمی‌کند، بلکه در اغلب توزیع‌ها توسط ماژول دیگری (systemd) جهت لاگبرداری XZ به آن اضافه می‌شود

❖ ورود به توزیع‌های بتا Fedora, Debian, ArchLinux, Kali, OpenSUSE, macOS

❖ کشف به علت تاثیر ناخواسته روی کارایی در شرایط خاص



# PIG.009-Chamelon



❖ هدف کاملاً دور از دسترس:

- یک شبکه کاملاً مجزا از اینترنت
- دارای لایه‌های محافظتی متعدد

❖ به جای حمله به هدف، حمله به یکی از زیرمجموعه‌ها

- همچنان غیرقابل دسترس و مجزا از اینترنت

❖ به جای حمله به زیر مجموعه، حمله به پیمانکار

- دارای سرویس‌های اینترنتی
- دارای دسترسی روی لینک اختصاصی و مورد اعتماد

# PIG.009-Chamelon

❖ مسیر قبلی کشف شده و مسدود می‌شود

❖ جایگزینی مسیر جدید بلافاصله پس از مسدود شدن مسیر قبلی  
■ این بار از طریق شبکه ملی و دو مرحله واسط دیگر

❖ استفاده از پورت پراکسی (بدون نصب هیچ ایجنت)





اطلاعات  
حساس

PIG.009-Chamelon



سازمان هدف

# PIG.009-Chamelon – محل‌های استقرار

## ❖ سرور اکتیو دایرکتوری

- از تمام شبکه دیده می‌شود
- مرکز احراز هویت است
- نقاط ضعف فراوانی دارد

## ❖ سرور مانیتورینگ

- تمام شبکه را می‌بیند
- معمولا حاوی اطلاعات احراز هویت روی سرورها است

## ❖ سرور آنتی‌ویروس

- از تمام شبکه دیده می‌شود
- دسترسی به اینترنت دارد

## ❖ سرور آپدیت (WSUS و مشابه)

- از تمام شبکه دیده می‌شود
- دسترسی به اینترنت دارد



اطلاعات  
حساس

PIG.009-Chamelon



سازمان هدف

# ابزارها – PIG.009-Chamelon

OpenSSH ❖

■ سالم، متن باز و دارای پیشینه

■ ابزار کنترل از راه دور

■ ابزارهای دور زدن فایروال (Port Forwarding, Proxy)

| Name                           | Path                                          | Size     |
|--------------------------------|-----------------------------------------------|----------|
| id_rsa                         | C:\Windows\System32\config\systemprofile\.ssh | 3 KB     |
| libcrypto.dll                  | C:\Windows\System32\en                        | 1,746 KB |
| svchost.exe                    | C:\Windows\System32\en                        | 1,042 KB |
| _1674759743.0059986            | C:\Windows                                    | 3 KB     |
| administrators_authorized_keys | C:\ProgramData\ssh                            | 1 KB     |
| sshd.pid                       | C:\ProgramData\ssh                            | 1 KB     |
| ssh_host_ed25519_key.pub       | C:\ProgramData\ssh                            | 1 KB     |
| ssh_host_ed25519_key           | C:\ProgramData\ssh                            | 1 KB     |
| ssh_host_ecdsa_key.pub         | C:\ProgramData\ssh                            | 1 KB     |
| ssh_host_ecdsa_key             | C:\ProgramData\ssh                            | 1 KB     |
| ssh_host_dsa_key.pub           | C:\ProgramData\ssh                            | 1 KB     |
| ssh_host_dsa_key               | C:\ProgramData\ssh                            | 2 KB     |
| ssh_host_rsa_key.pub           | C:\ProgramData\ssh                            | 3 KB     |
| sshd_config                    | C:\ProgramData\ssh                            | 3 KB     |
| OpenSSH%4Operational.evtx      | C:\Windows\System32\winevt\Logs               | 68 KB    |
| OpenSSH%4Admin.evtx            | C:\Windows\System32\winevt\Logs               | 68 KB    |





اطلاعات  
حساس

PIG.009-Chamelon



سازمان هدف

# ابزارها – PIG.009-Chamelon

## Netsh ❖

- ابزار داخلی ویندوز برای تنظیمات پیشرفته شبکه
- پیش فرض نصب شده و قابل استفاده
- امکان Port Forwarding بدون هیچ نشانه‌ی ملموس

```
netsh interface portproxy add v4tov4 listenaddress=<local_ip>  
listenport=<local_port> connectaddress=<remote_ip> connectport=<remote_port>
```

```
netsh interface portproxy show all
```



اطلاعات  
حساس

PIG.009-Chamelon



سازمان هدف

# ابزارها – PIG.009-Chamelon

## درب پستی Magic Packet

❖ سواستفاده از اتصالات یک برنامه مجاز

❖ روی همان پورت گوش داده و در صورت دریافت بایتهای خاصی، اتصال به کد مخرب هدایت می شود

❖ غیرقابل تشخیص از بیرون

❖ هم نسخه لینوکسی و هم نسخه ویندوزی



PIG.008-  
GonjeshkeDarande

# نشان افزار ILOBleed

**Bloomberg**

Subscribe

Newsletter

# Iran Hack Startles the Global Cybersecurity Community

By Jordan Robertson

February 9, 2022, 3:15 PM GMT+3:30  
GMT+3:30

New iLOBleed Rootkit, the first time ever that malware t  
firmware

December 30, 2021 By Pierluigi Paganini

A previously unknown rootkit, dubbed iLOBleed, was used i  
HP Enterprise servers that wiped data off the infected syst

Take the lights-out  
Implant.ARM.iLOBleed.a

The first rootkit discovered infecting HP iLO firmware

December 2021

(ج) کلیه حقوق متعلق به شرکت نرم‌افزاری امن‌پرداز است

Amnpardaz.com

# HP Server

Never turned off

Complete Control

Never checked

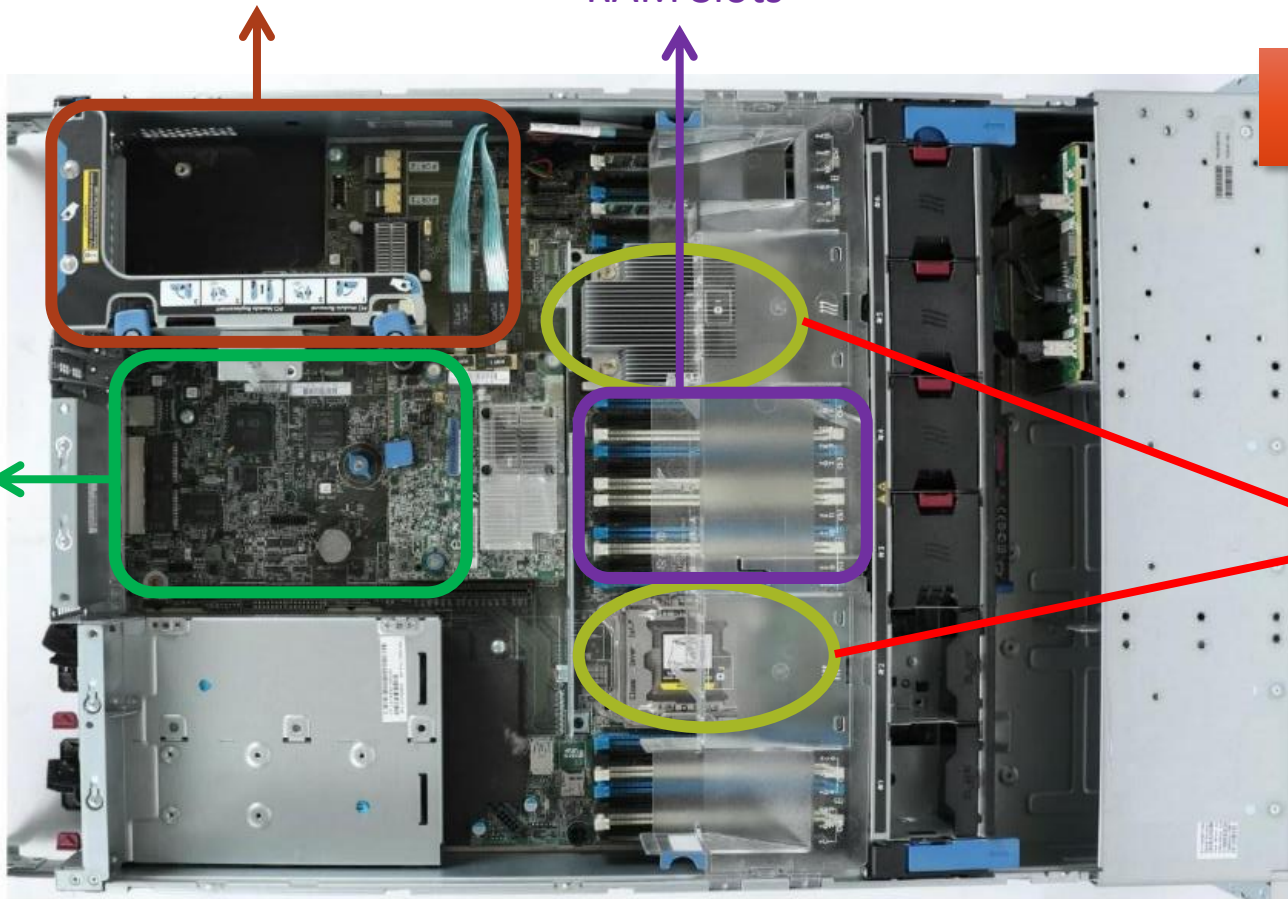
Virtually, a god in the HP servers

Internal & External  
RAID Controller

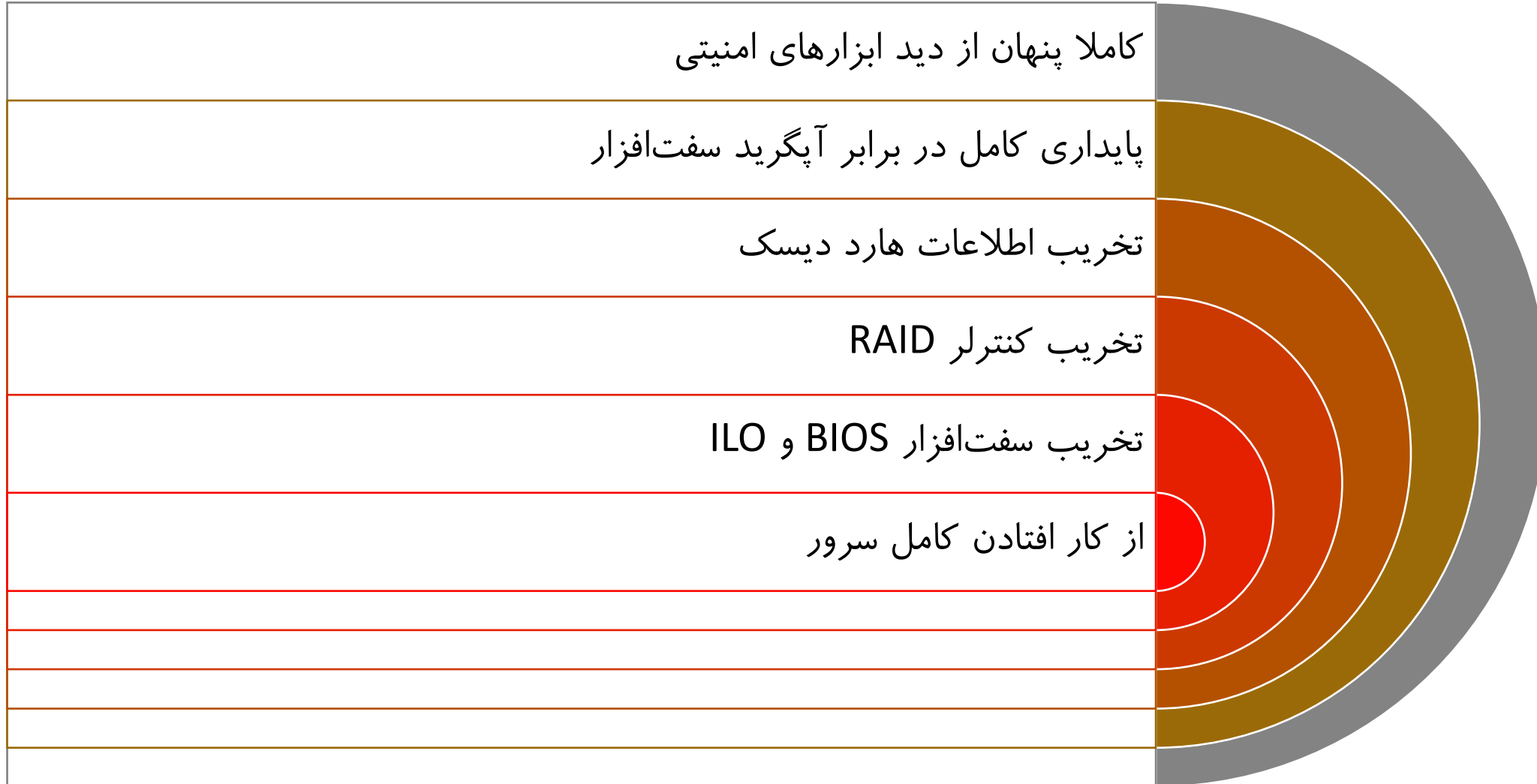
RAM Slots

ILO Panel

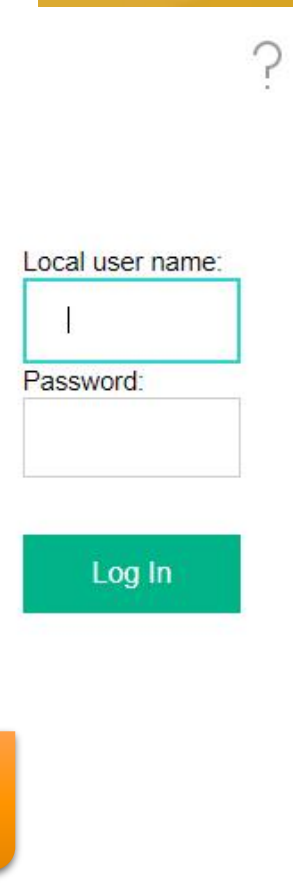
Intel Xeon  
Processors



# ویژگی‌های نهان افزار Implant.ARM.iLOBleed.a



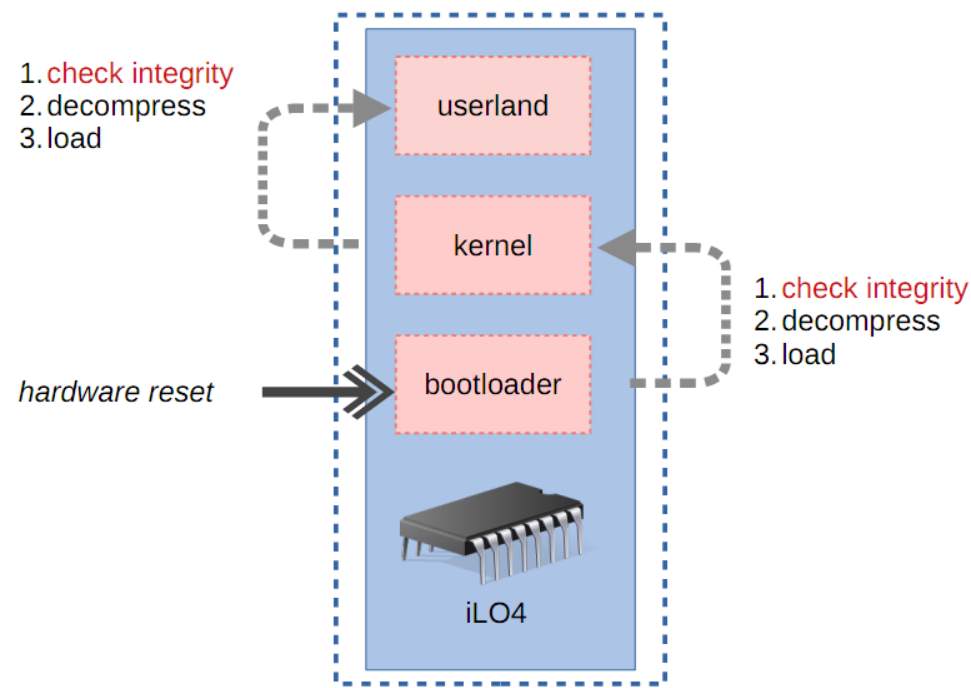
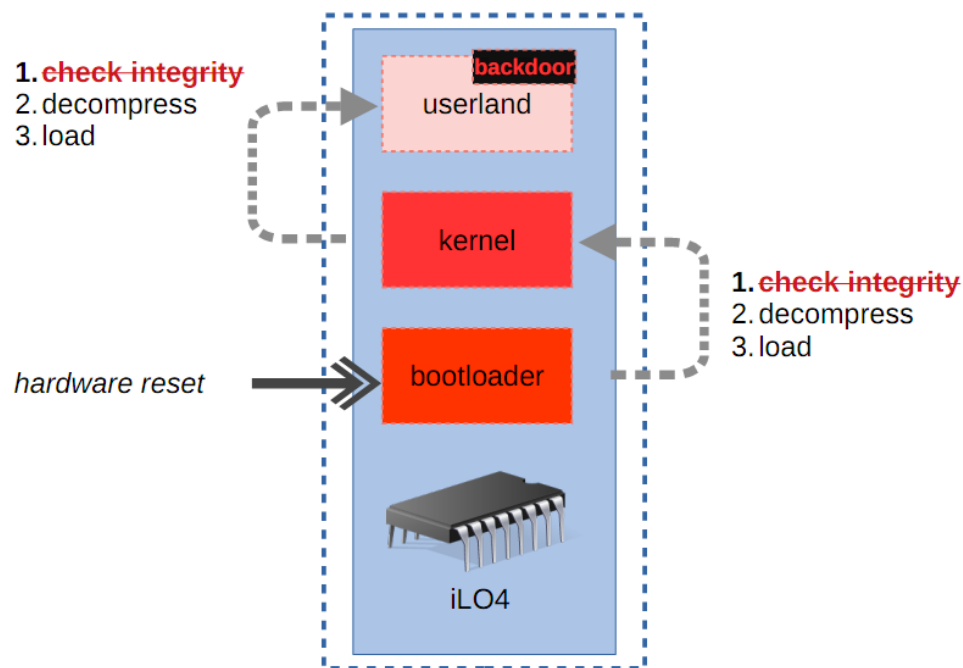
# علائم آلودگی



# پنل مدیریتی HP ILO

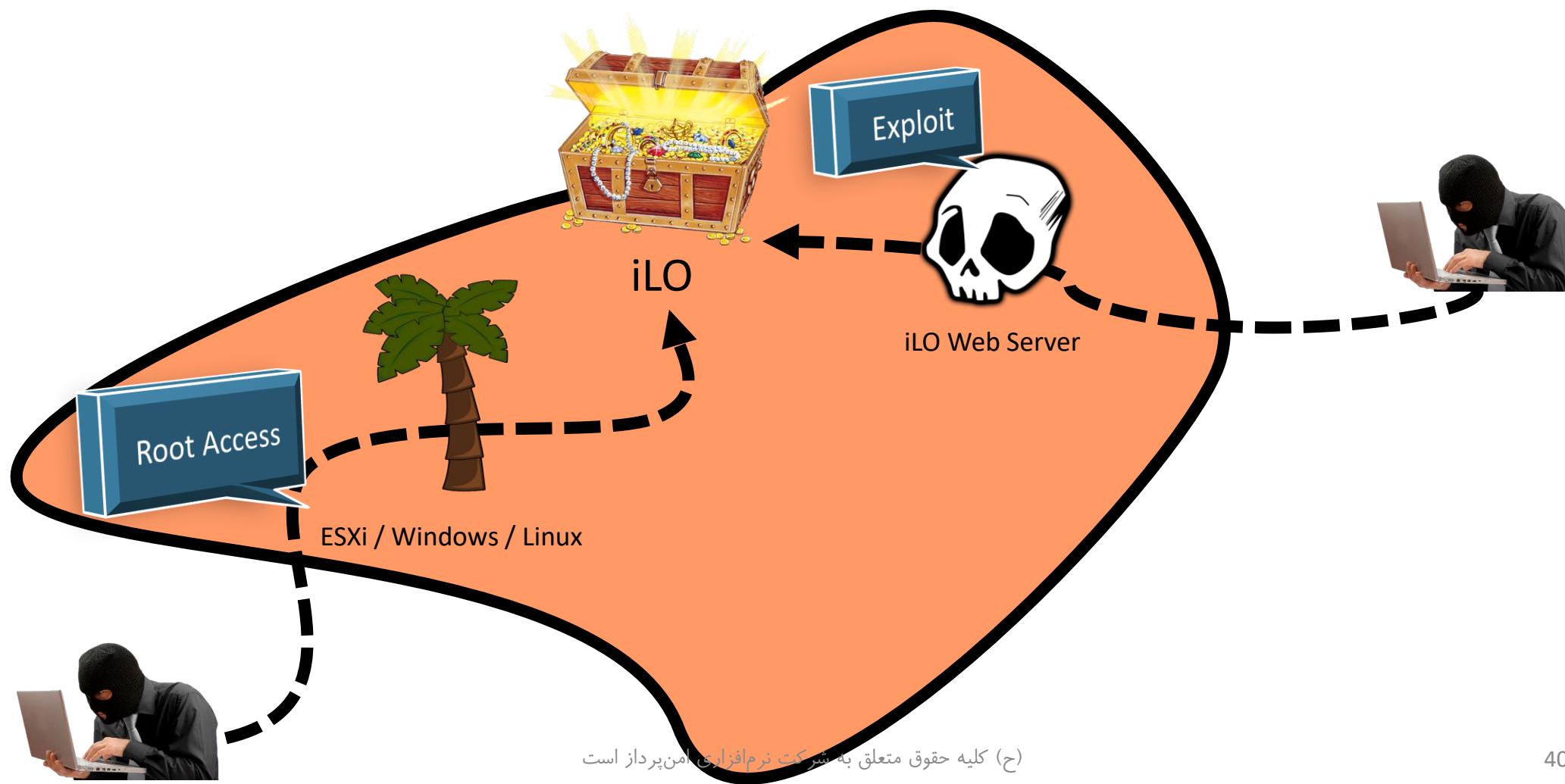
## فرآیند بوت شدن سفت افزار ILO

## پس از آلودگی ...



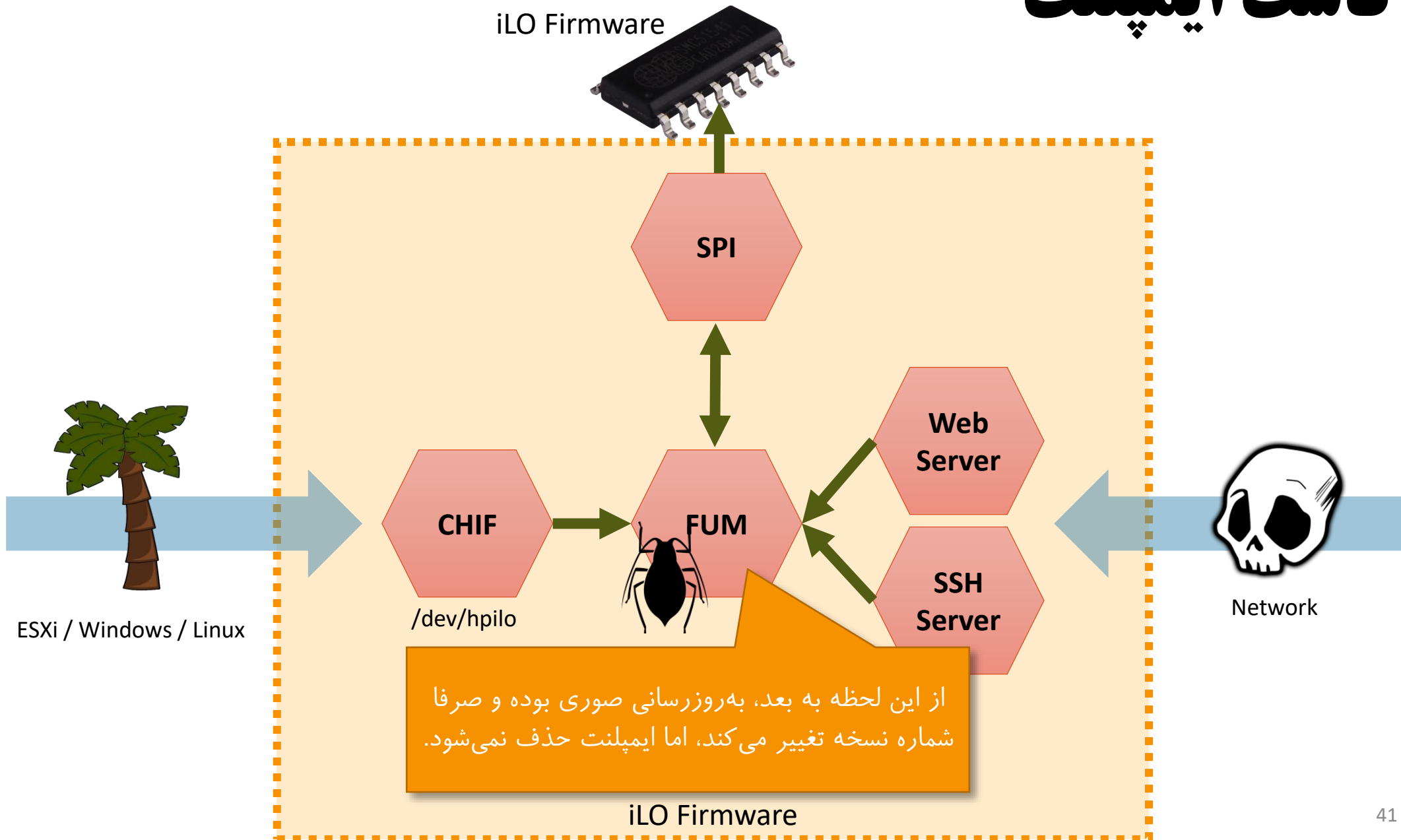


# کاشت implant در سفت افزار HP iLO





# کاشت ایمپلنت

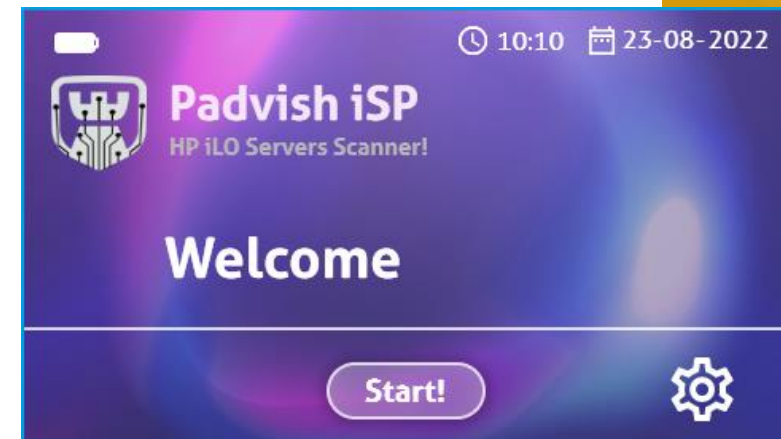


# Padvish iLO Scanner

❖ بررسی اصالت سفت افزار iLO سرور

❖ پشتیبانی از سرورهای G7 تا G11

❖ قابلیت پاکسازی سفت افزار iLO



# راهکار مقابله با حملات سایبری

# به ابزار نمی‌توان تکیه کرد

❖ «ابزار»های امنیتی، با «ابزار»های هک مقابله می‌کنند...

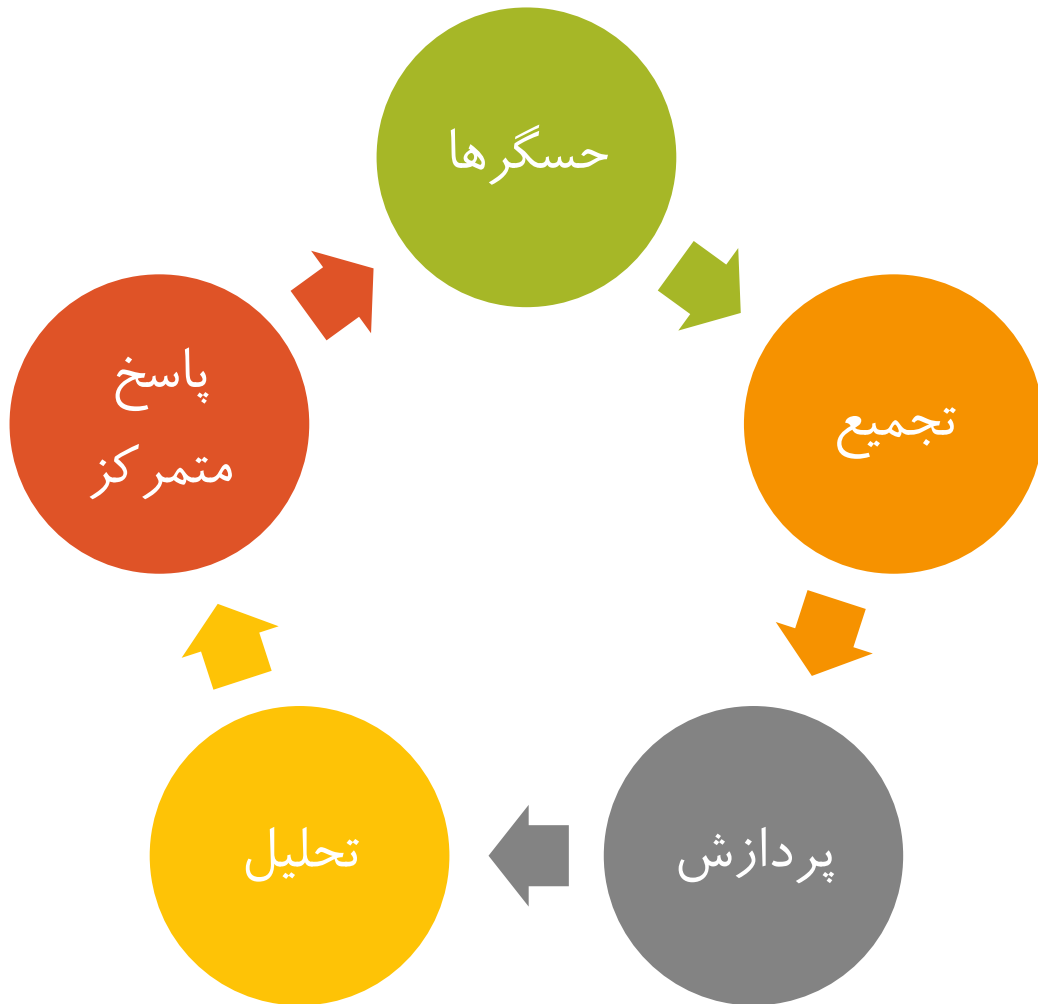
| ابزار امنیتی | تهدید امنیتی                     |
|--------------|----------------------------------|
| Antivirus    | Malware, Rootkit, Virus, Trojans |
| Firewall     | Illegal Connections              |
| IPS          | Network Exploits                 |
| WAF          | Web Attacks                      |
| ...          |                                  |

❖ اما با هکرها، فقط هکرها می‌توانند مقابله کنند...



# مقابله با حملات سایبری

- ❖ ابزار قابل اعتماد و دقیق
- ❖ نیروی انسانی متخصص
- ❖ پایش مستمر
- ❖ دفاع متمرکز
- ❖ دفاع چند لایه



# استراتژی دفاع سایبری

## مرز سایبری

قرار دادن مواضع در عمق

تهدیدات برون شبکه

مقابله از بیرون

کاهش تهدیدات در کل شبکه

## مرکز MXDR

دفاع در عمق

تهدیدات درون شبکه

مقابله از درون

رسیدگی و مقابله نقطه به نقطه

سخنرانی کلیدی کنفرانس انجمن رمز <<

(ح) کلیه حقوق برای شرکت نرم افزاری امن پرداز محفوظ است



# آموخته‌های حملات سایبری از تهدیدشناسی تا دفاع پیشگیرانه

در ادامه  
شبیه‌سازی زنده حمله سایبری >>



# سناریوی حمله

