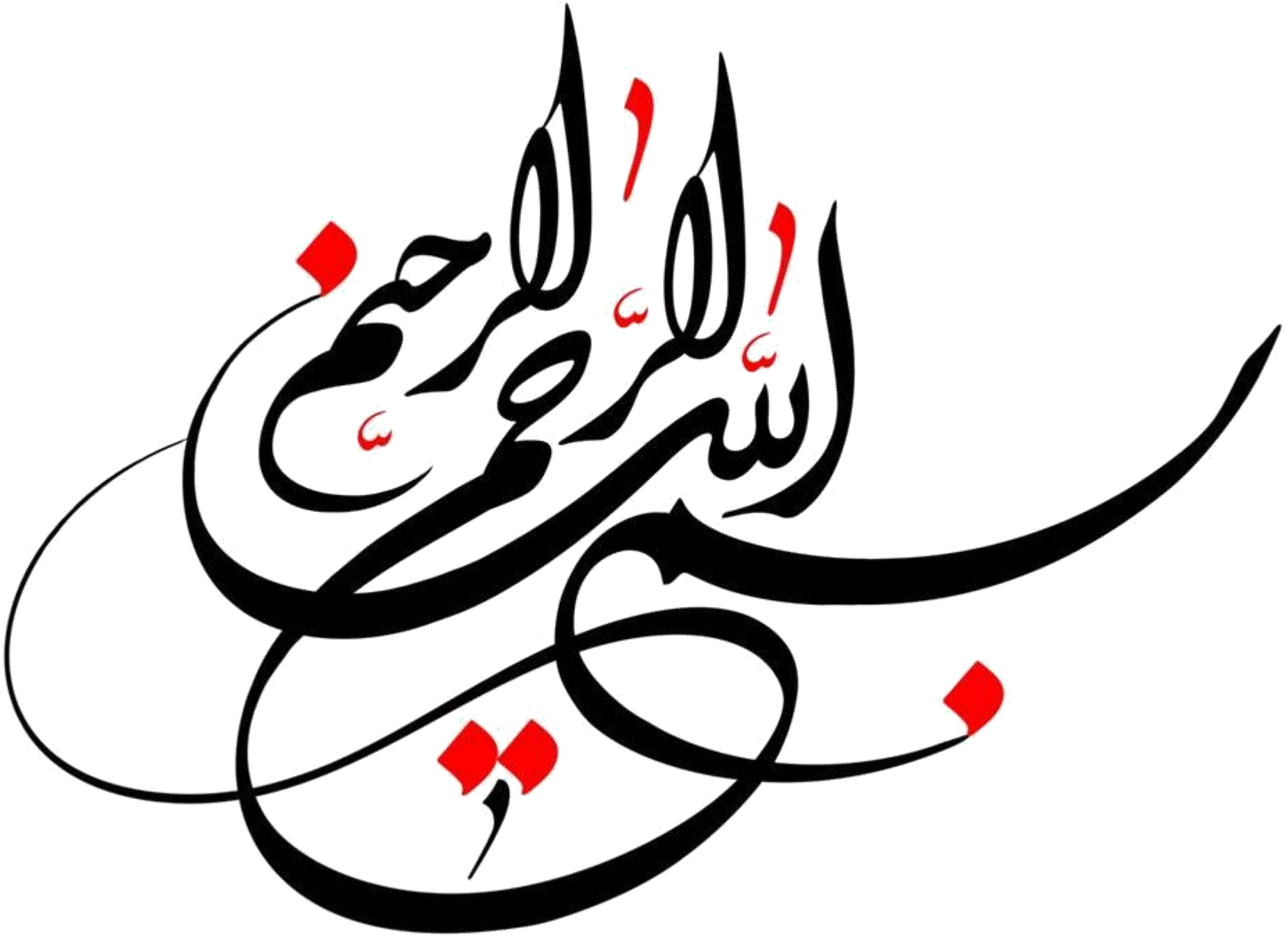


شماره سند: PPT_2/404/5566_421/1404_1/2_1.0

آموخته‌های حملات سایبری

از تهدیدشناسی تا دفاع پیشگیرانه

شرکت نرم‌افزاری امن‌پرداز

عناوین

تهدیدشناسی فضای کشور

مدل‌سازی حملات سایبری

گروه‌های مهاجم فعال در کشور

تکنیک‌های نفوذ پراستفاده

مطالعه موردی حملات سایبری

پرونده ۱)
حمله در سطح مجازی‌ساز

پرونده ۲)
حمله زنجیره تأمین

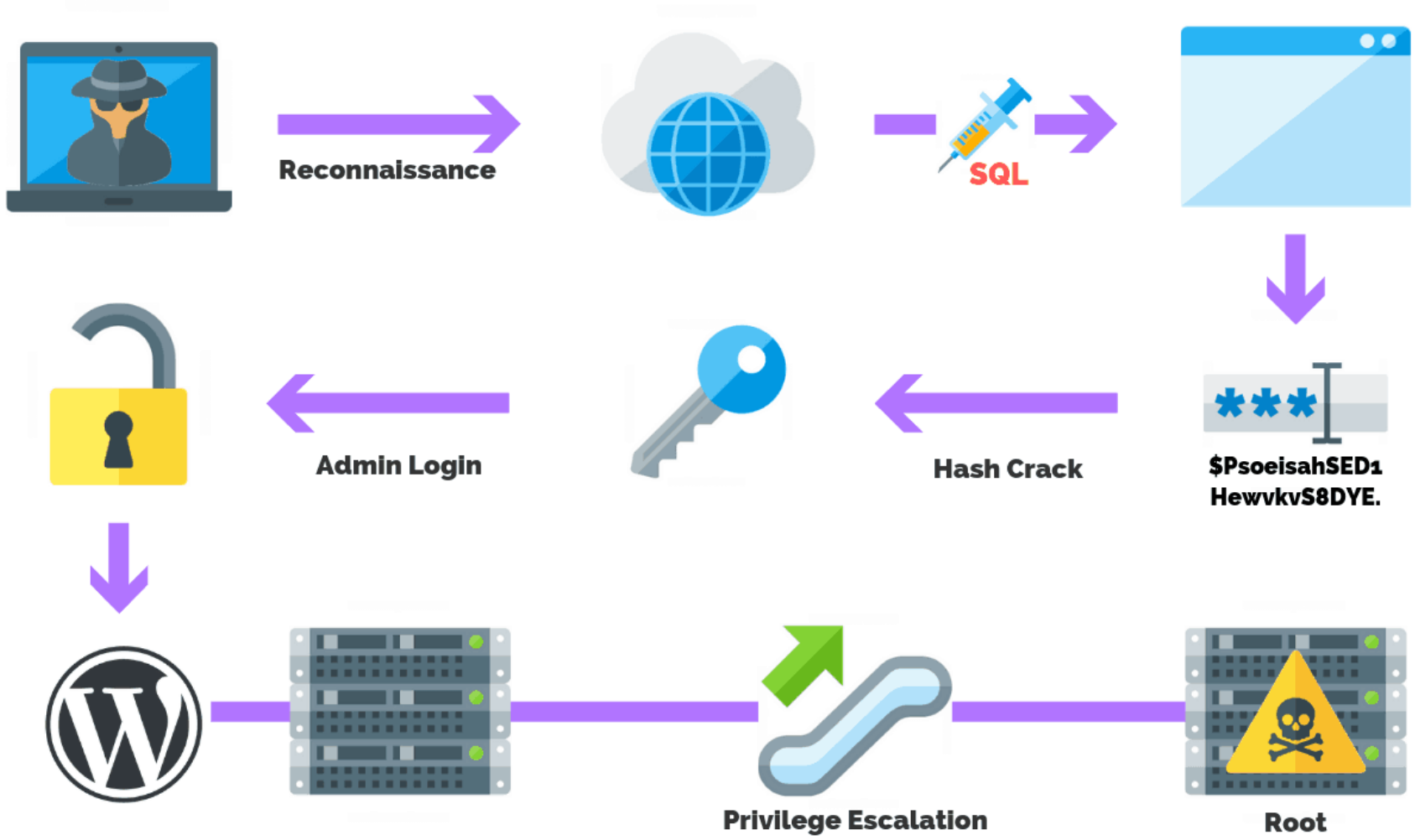
پرونده ۳)
آلوده‌سازی سفت‌افزار

درس آموخته‌های حملات سایبری

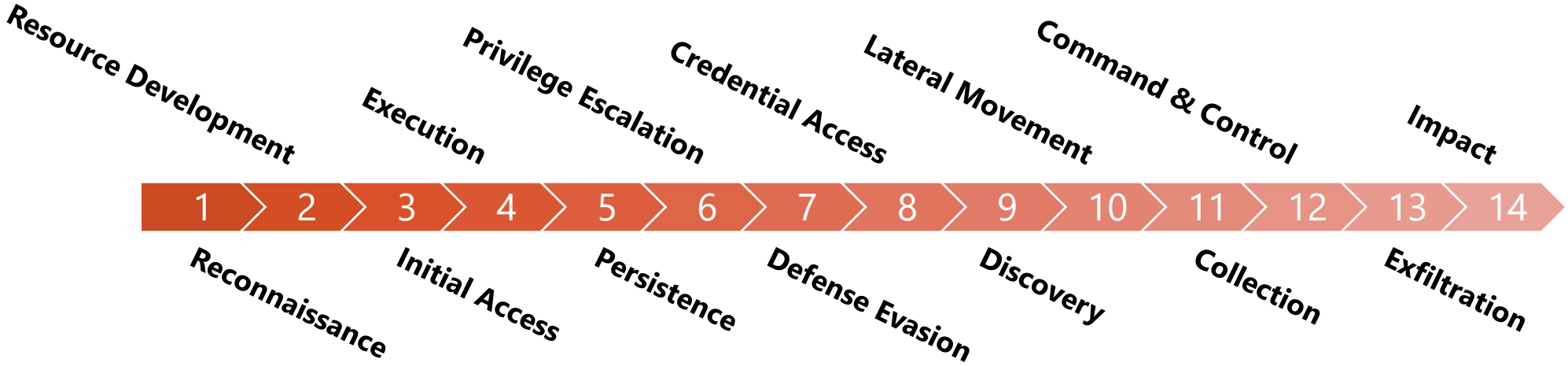
و روش‌های مقابله

مدل‌سازی حملات سایبری

مثالی از یک حمله سایبری



مدل‌سازی 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 اکانت ها، تروجان، بات نت

انجام اقدام نهایی حمله سایبری

گروه‌های مهاجم فعال در کشور

PIG.006-GhiyamTaSarneguni

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 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 (0/5)	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 (0/3)	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	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	Login 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)		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 (0/3)	Ingress Tool Transfer	Transfer Data to Cloud Account	Endpoint Denial of Service (0/4)
Search Closed Sources (0/2)		Valid Accounts (2/4)	Visual Basic	Print Processors	Port Monitors	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery	SMB/Windows Admin Shares	Data from Local System	Multi-Stage Channels		Financial Theft
Search Open Technical Databases (0/5)		Cloud Accounts	Windows Command Shell	Re-opened Applications	Print Processors	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery	SSH	Data from Network Shared Drive	Non-Application Layer Protocol		Firmware Corruption
Search Open Websites/Domains (0/3)		Default Accounts	Container Administration Command	Registry Run Keys / Startup Folder	Re-opened Applications	File and Directory Permissions Modification (0/2)	OS Credential Dumping (1/8)	File and Directory Discovery	VNC	Data from Removable Media	Non-Standard Port		Inhibit System Recovery
Search Victim-Owned Websites		Domain Accounts	Deploy Container	Security Support Provider	Registry Run Keys / Startup Folder	Hide Artifacts (0/11)	/etc/passwd and /etc/shadow	Group Policy Discovery	Windows Remote Management	Data Staged (0/2)	Protocol Tunneling		Network Denial of Service (0/2)
		Local Accounts	Exploitation for Client Execution	Shortcut Modification	Security Support Provider	Hijack Execution Flow (0/12)	Cached Domain Credentials	Log Enumeration	Replication Through Removable Media	Email Collection (0/3)	Proxy (2/4)		Resource Hijacking
			Inter-Process Communication (0/3)	Time Providers	Shortcut Modification	Impair Defenses (1/11)	DCSync	Network Service Discovery	Software Deployment Tools	Input Capture (0/4)	Domain Fronting		Service Stop
			Native API	Winlogon Helper DLL	Time Providers	Disable or Modify Cloud Firewall	LSA Secrets	Network Share Discovery	Taint Shared Content	Screen Capture	External Proxy		System Shutdown/Reboot
			Scheduled Task/Job (1/5)	XDG Autostart Entries	Winlogon Helper DLL	Disable or Modify Cloud Logs	LSASS Memory	Network Sniffing	Use Alternate Authentication Material (0/4)	Video Capture	Internal Proxy		
			At	Boot or Logon Initialization Scripts (0/5)	XDG Autostart Entries	Disable or Modify Linux Audit System	NTDS	Password Policy Discovery			Multi-hop Proxy		
			Container Orchestration Job	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Disable or Modify System Firewall	Proc Filesystem	Peripheral Device Discovery			Remote Access Software		
			Cron	Compromise Client Software Binary	Create or Modify System Process (1/4)	Disable or Modify Tools	Security Account Manager	Permission Groups Discovery (0/3)			Traffic Signaling		
			Scheduled Task	Create Account (0/3)	Launch Agent	Disable Windows Event Logging	Steal Application Access Token	Process Discovery					
			Systemd Timers	Create or Modify System Process (1/4)	Launch Daemon	Downgrade Attack	Steal or Forge Authentication Certificates	Query Registry					
			Serverless Execution	Launch Agent	Systemd Service	Impair Command History Logging	Steal or Forge Kerberos Tickets (0/4)	Remote System Discovery					
			Shared Modules	Launch Daemon	Windows Service	Indicator Blocking	Steal Web Session Cookie	Software Discovery (0/1)					
			Software Deployment Tools	Systemd Service	Domain Policy Modification (0/2)	Safe Mode Boot	Unsecured Credentials (1/8)	System Information Discovery					
			System Services (1/2)	Windows Service	Escape to Host	Spoof Security Alerting	Bash History	System Location Discovery (0/1)					
			Launchctl	Event Triggered Execution (0/16)	Event Triggered Execution (0/16)	Impersonation		System Network Configuration Discovery (0/2)					
			Service Execution	External Remote Services	Exploitation for	Indicator Removal (2/9)		System Network Connections Discovery					
			User Execution (0/3)	Hijack Execution		Clear Command History		System Owner/User Discovery					
			Windows Management Instrumentation			Clear Linux or Mac System Logs		System Service Discovery					
								System Time Discovery					
								Virtualization/Sandbox Evasion (0/3)					

MITRE ATT&CK® Navigator v4.9.1

* PIG: Padvish-Indexed Group

PIG.007-EdalatAli

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

MITRE ATT&CK® Navigator v4.9.1

* PIG: Padvish-Indexed Group

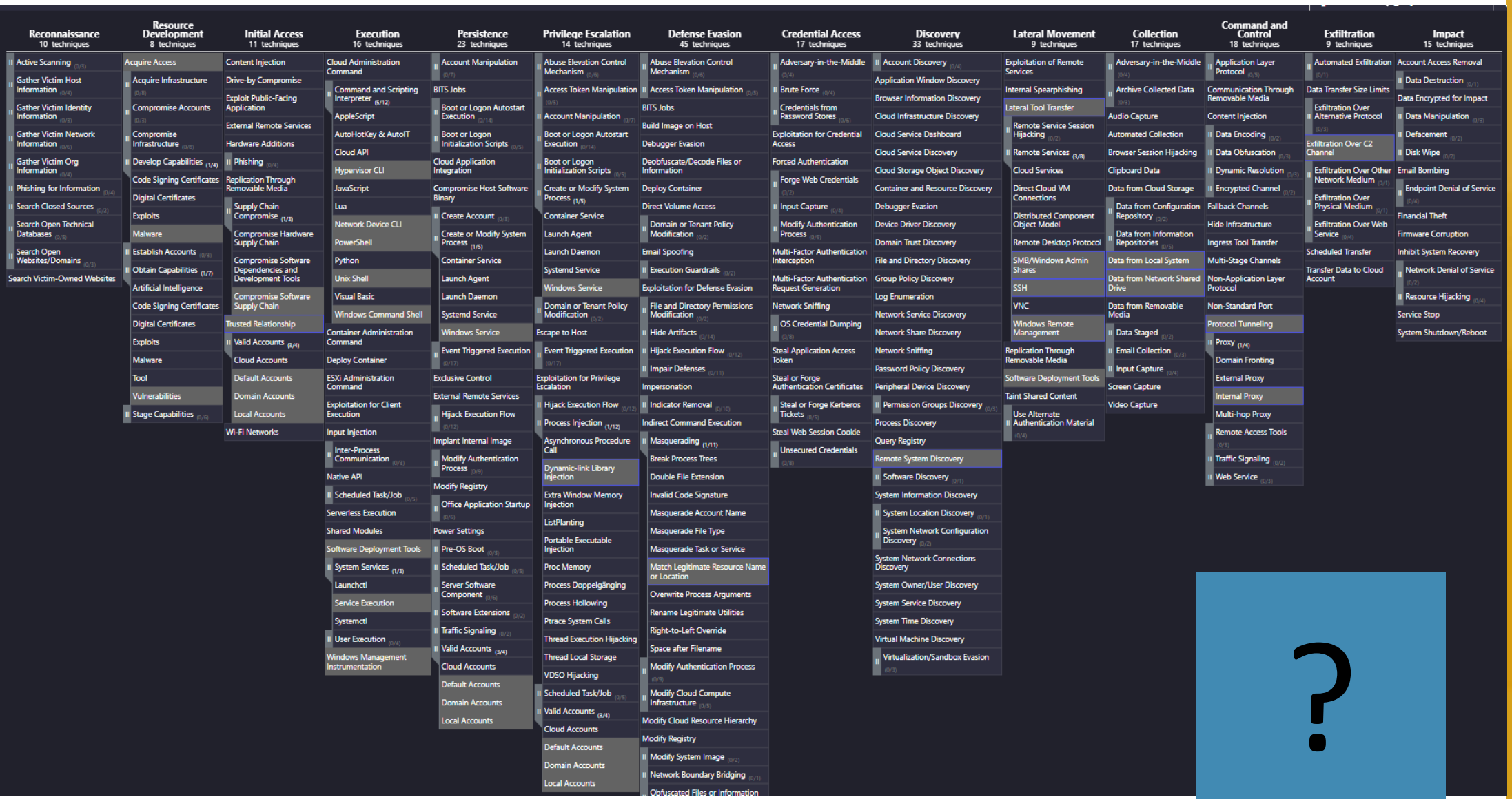
PIG.008-GonjeshkeDarande

* PIG: Padvish-Indexed Group

از است

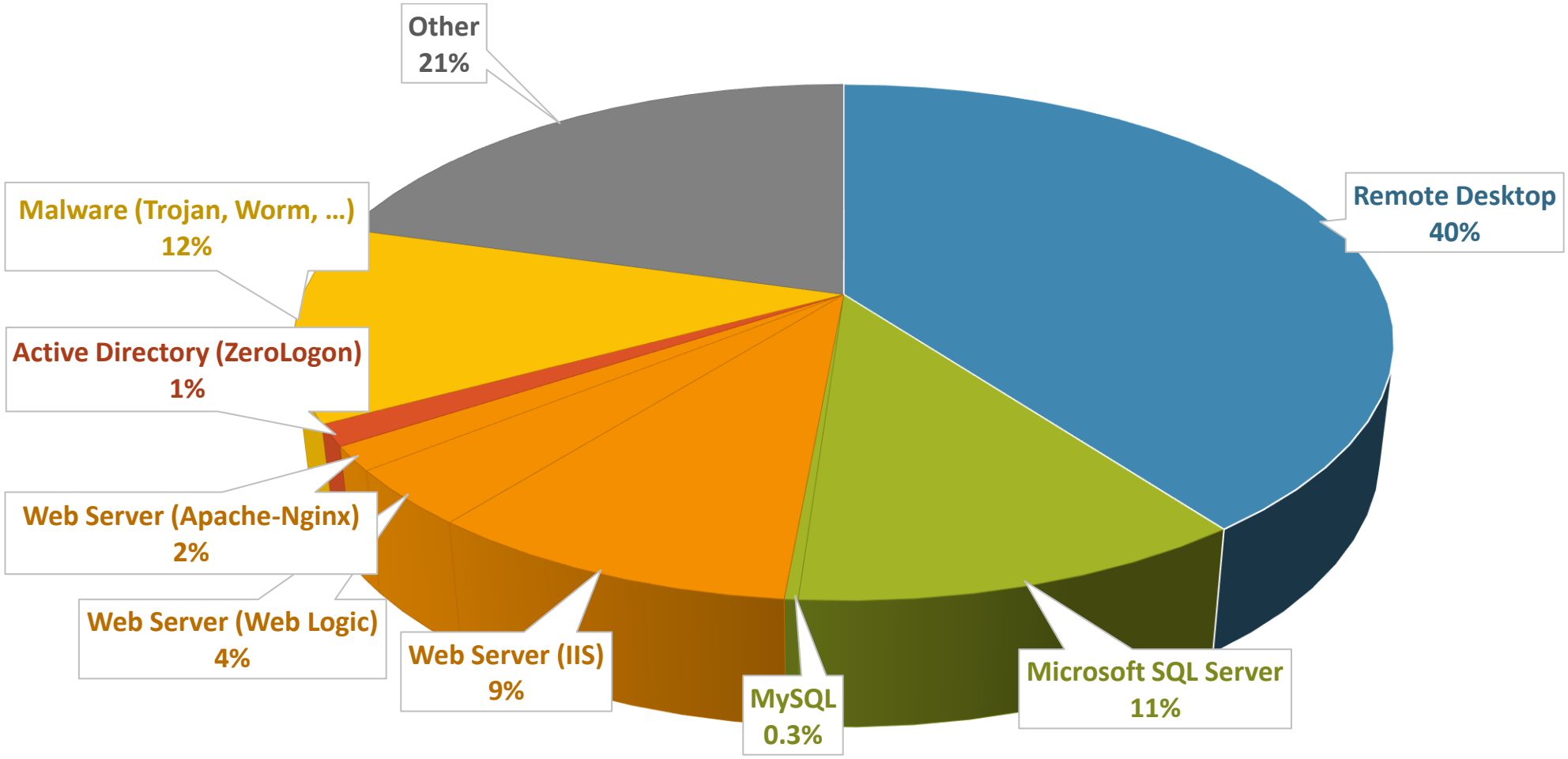
z.com

PIG.009-Chameleon



* PIG: Padvish-Indexed Group

روش نفوذ اولیه – در حملات سایبری اخیر



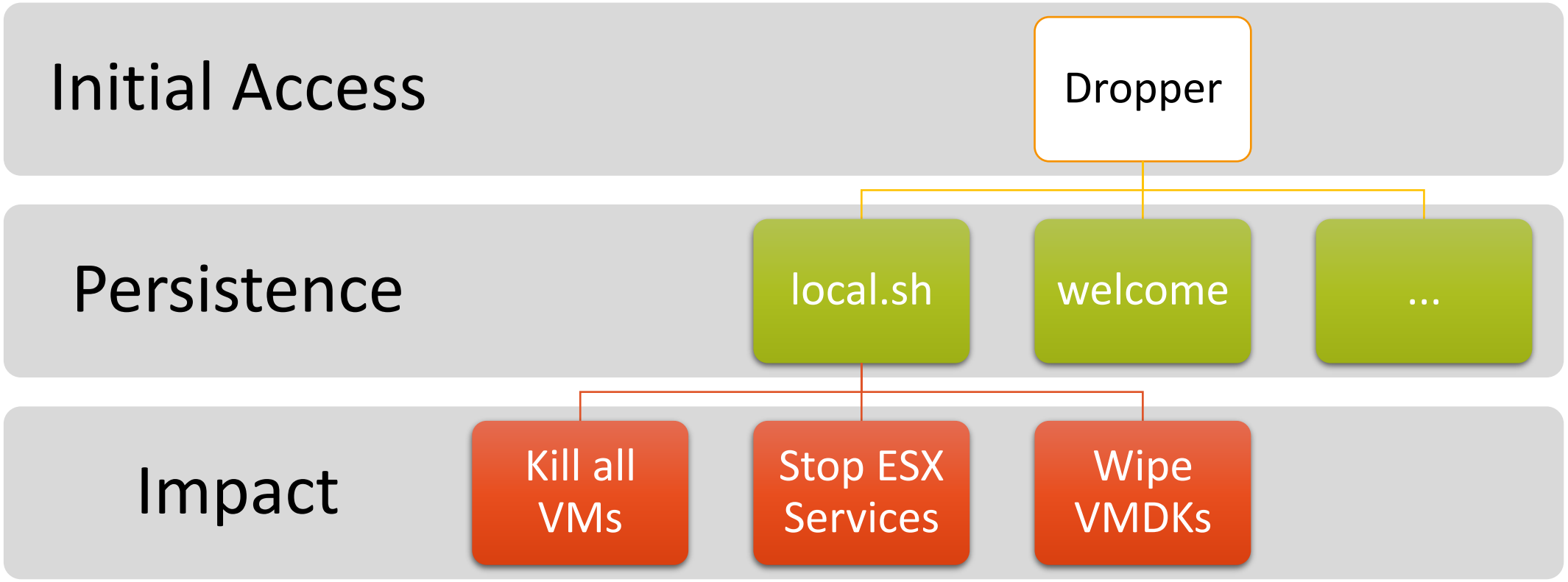
Source: Amnpardaz CSIRT 2024

مطالعه موردی حملات سایبری

پرونده اول

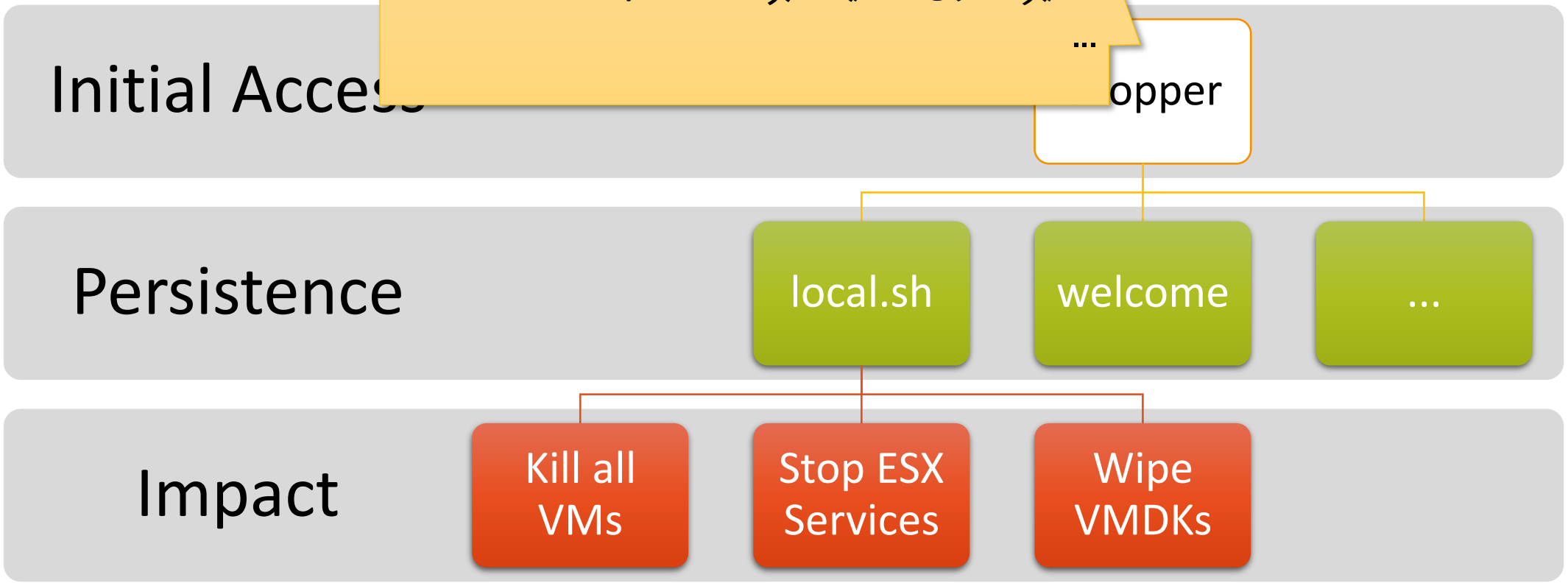
حمله در سطح مجازی‌سازی (Hyper-visor)

BreakESX



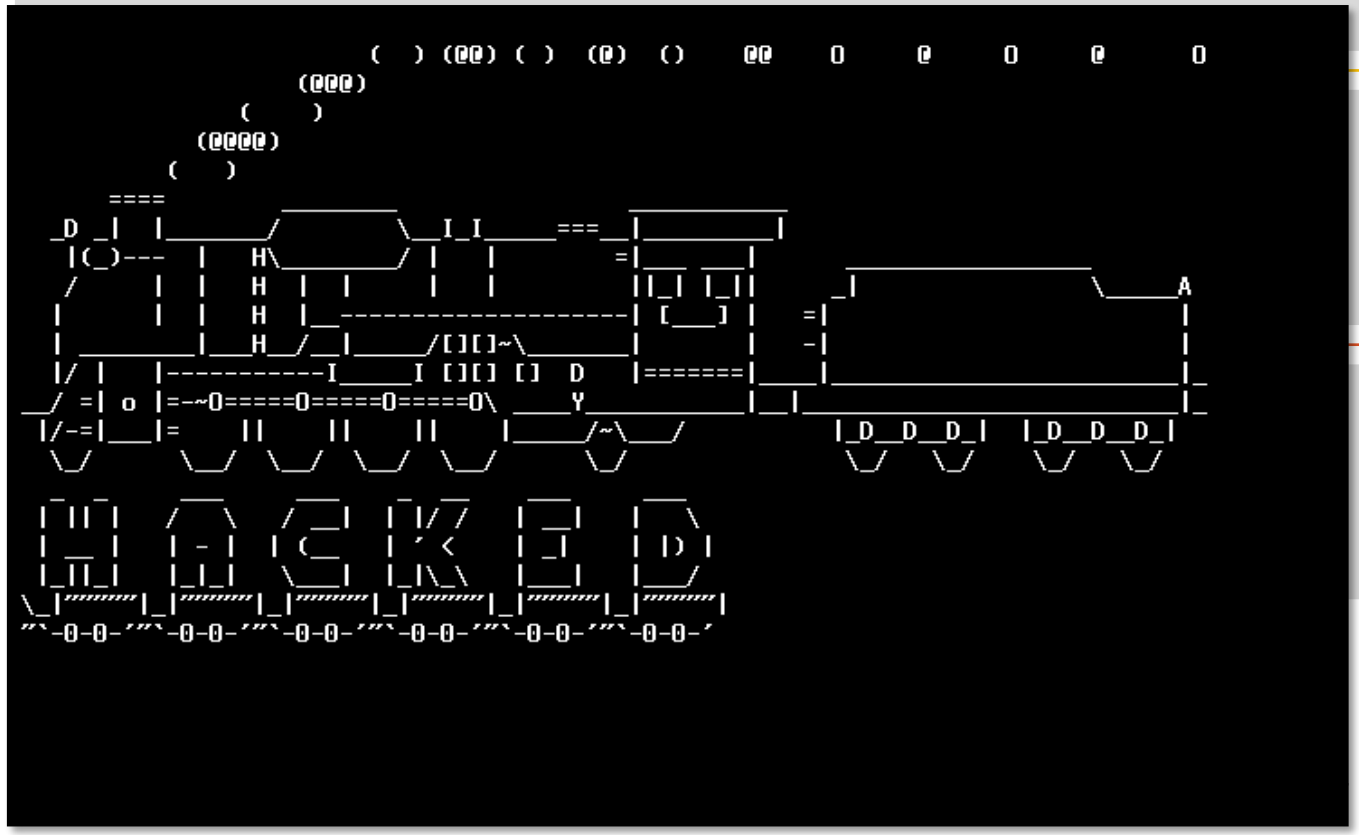
BreakESX

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



BreakESX

Initial Access



Droppe

welcome

...

Wipe VMDKs

نمایش پیام در صورت:

- UEFI Secure Boot
- عدم اجرای صحیح local.sh

BreakESX

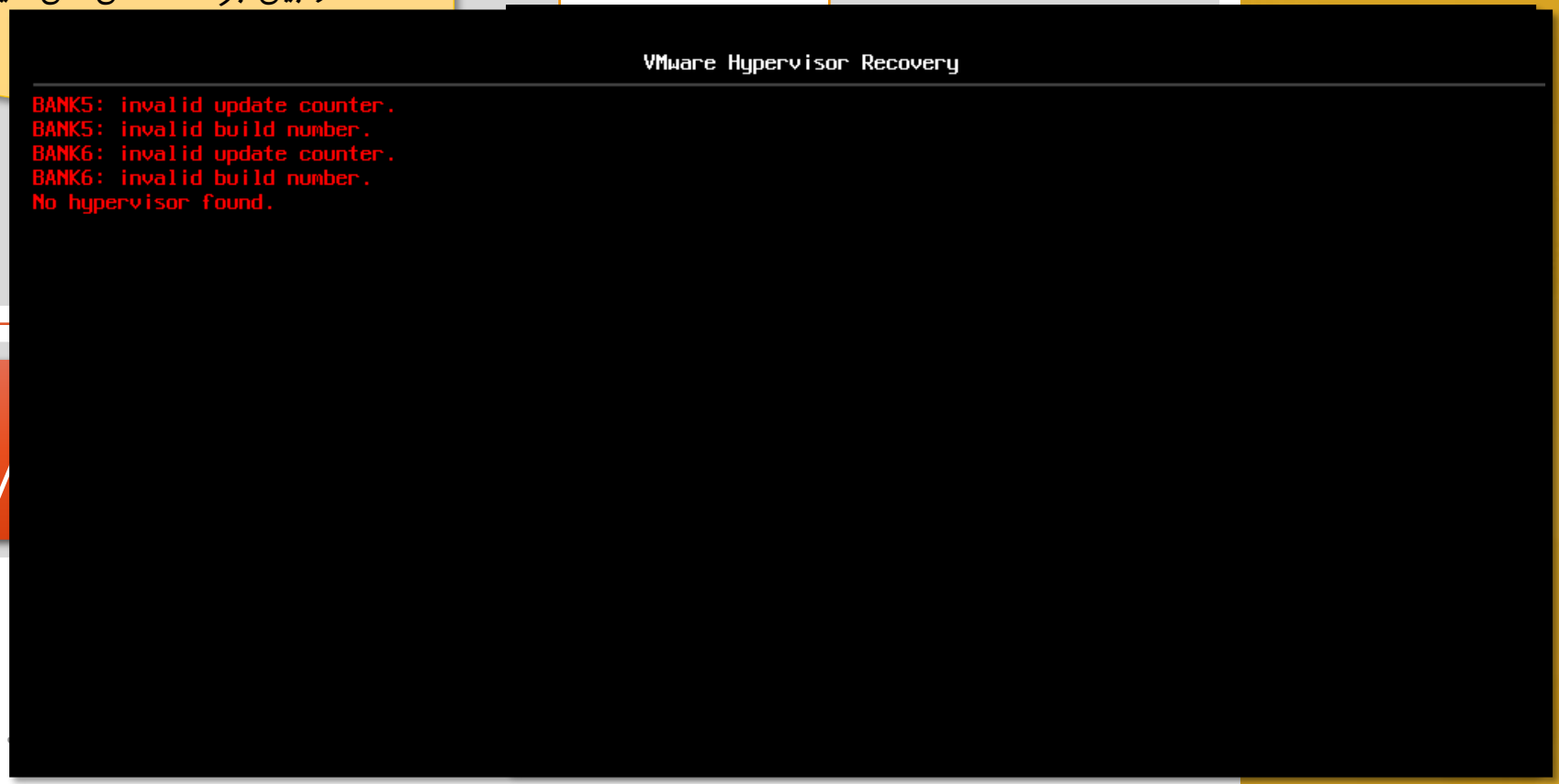
1. بستن پردازه‌های مدیریتی
2. توقف کلیه ماشین‌های مجازی
3. متوقف‌سازی سرویس‌های حیاتی سیستم عامل VMware ESXi
4. غیرفعال کردن کلیه دسترسی‌ها از راه دور
5. تخریب اطلاعات بوت سیستم‌عامل (و خود اسکریپت بدافزار)
6. از بین بردن کامل کل دیسک‌های ماشین‌های مجازی

Dropper

Persistence

Impact

Kill
VM



پرونده دوم

PIG.009-Chamelon

حمله زنجیره تامین

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 مستقیما قابل حمله نیستند.
  - معمولا 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.

SunBurst – Solarwinds حمله

U.S. federal government [edit]

Branch	Institution	Affected part(s) include	Assets accessed	Sources
Executive	Department of Agriculture	National Finance Center		[6][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]
	Department of the Treasury			[1][150][156][149][80][82][75][147][152][153][148][46][155]
Judicial	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 ظاهرا سالم
  - استفاده از درب‌پشتی فقط برای اهداف مهم و دارای ارزش

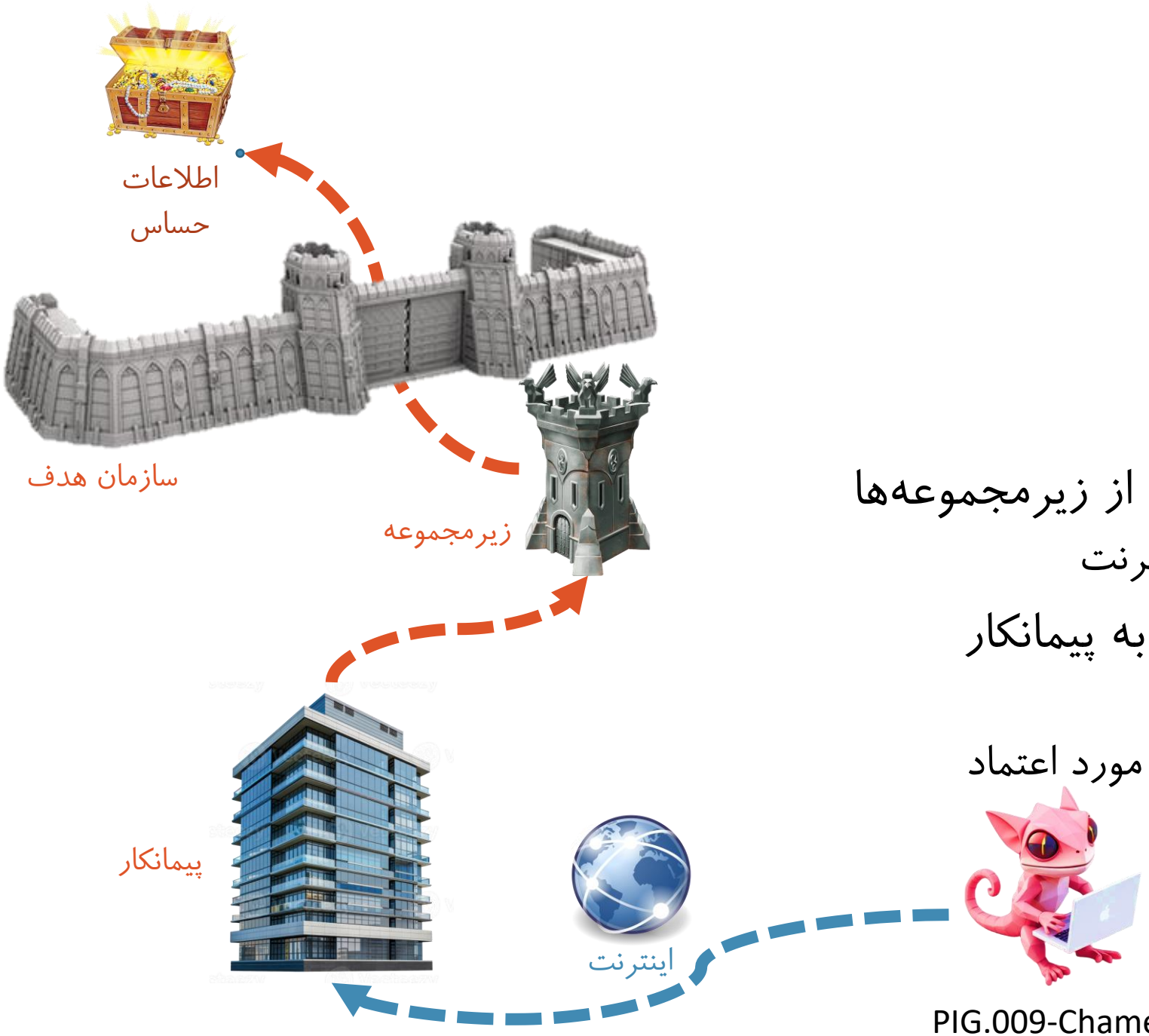
- کشف از طریق بررسی اتفاقات غیرمتعارف در reEye

حمله SSH/xz

- ۲۰۲۴-۰۳-۲۹ **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 اصلا 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 کاملا دور از دسترس:
  - یک شبکه کاملا 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)

محل‌های استقرار – PIG.009-Chamelon

اطلاعات حساس

PIG.009-Chamelon

سازمان هدف

- **سرور اکتیودایرکتوری**
  - 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

ابزارها – PIG.009-Chamelon

اطلاعات حساس

PIG.009-Chamelon

سازمان هدف

- OpenSSH
  - سالم، متن‌باز 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_rsa_key.pub	C:\ProgramData\ssh	1 KB
ssh_host_dsa_key	C:\ProgramData\ssh	2 KB
ssh_host_rsa_key	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

ابزارها – PIG.009-Chamelon

Netsh

- ابزار داخلی ویندوز برای تنظیمات پیشرفته شبکه
- پیش‌فرض 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
```

ابزارها – PIG.009-Chamelon

اطلاعات حساس

PIG.009-Chamelon

سازمان هدف

درب‌پشتی Magic Packet

- سواستفاده از اتصالات یک برنامه مجاز
- روی همان پورت گوش داده و در صورت دریافت بایت‌های خاصی، اتصال به کد مخرب هدایت می‌شود
- غیرقابل تشخیص از بیرون
- هم نسخه لینوکسی و هم نسخه ویندوزی

نهان‌افزار ILOBleed

Bloomberg

Subscribe

Newsletter

Iran Hack Startles the Global Cybersecurity Community

By Jordan Robertson

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

GMT+3:30

Support Center

English

SUPPORT ALERTS -

SIGN IN

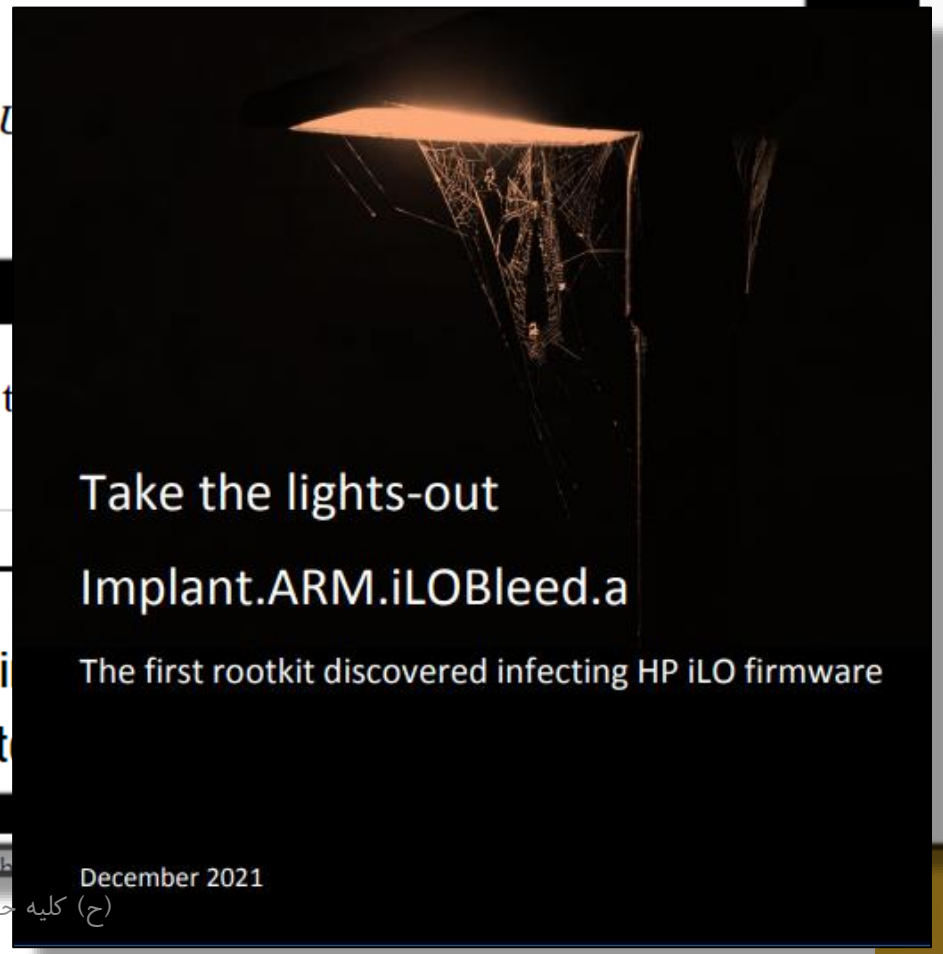
New iLOBleed Rootkit, the first time ever that malware t

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



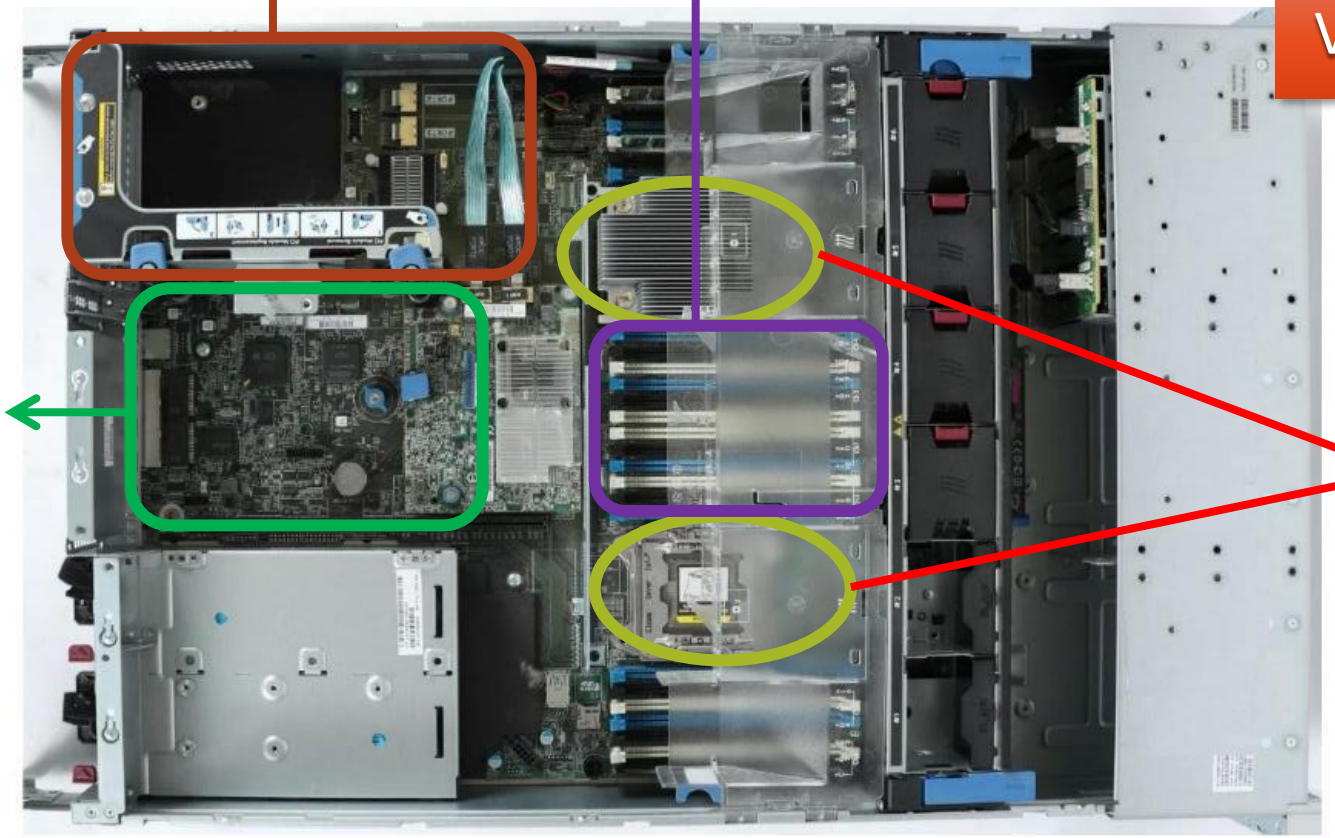
HP Server

Never turned off

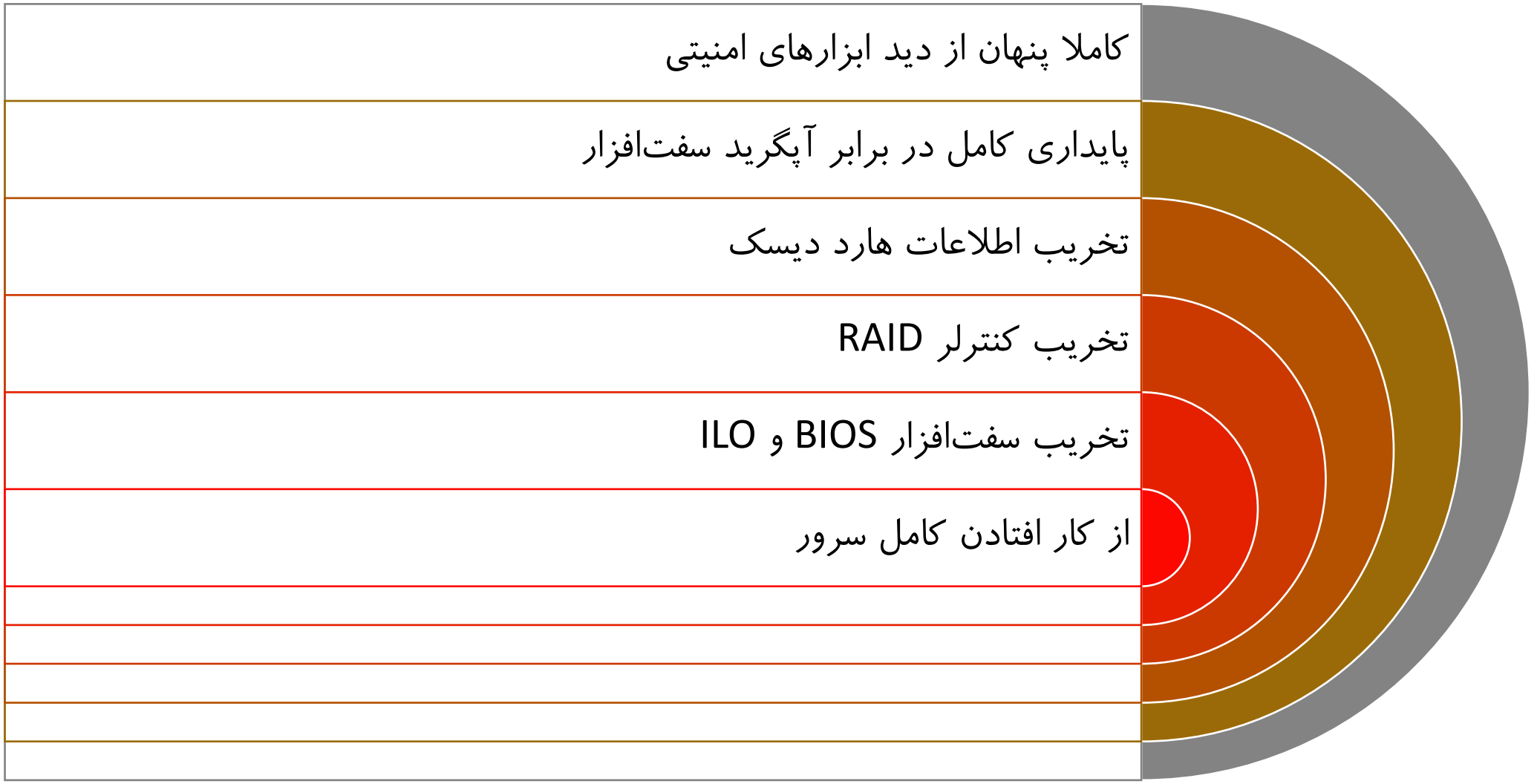
Complete Control

Never checked

Virtually, **a god** in the HP servers



ویژگی‌های نهان‌افزار Implant.ARM.iLOBleed.a



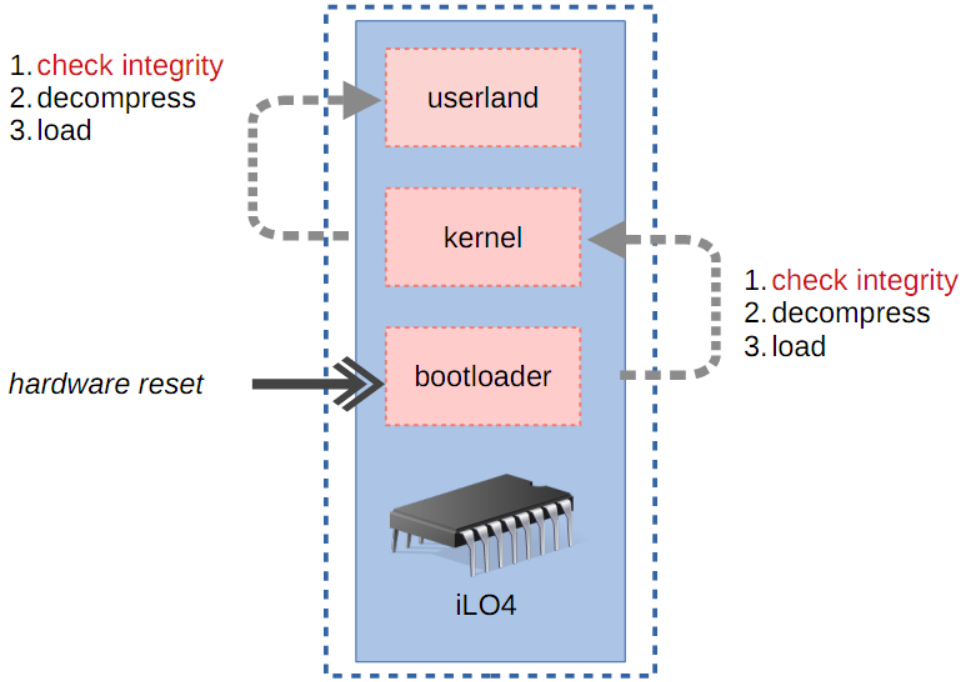
علائم آلودگی

نسخه آلوده
(رابط کاربری قدیمی)

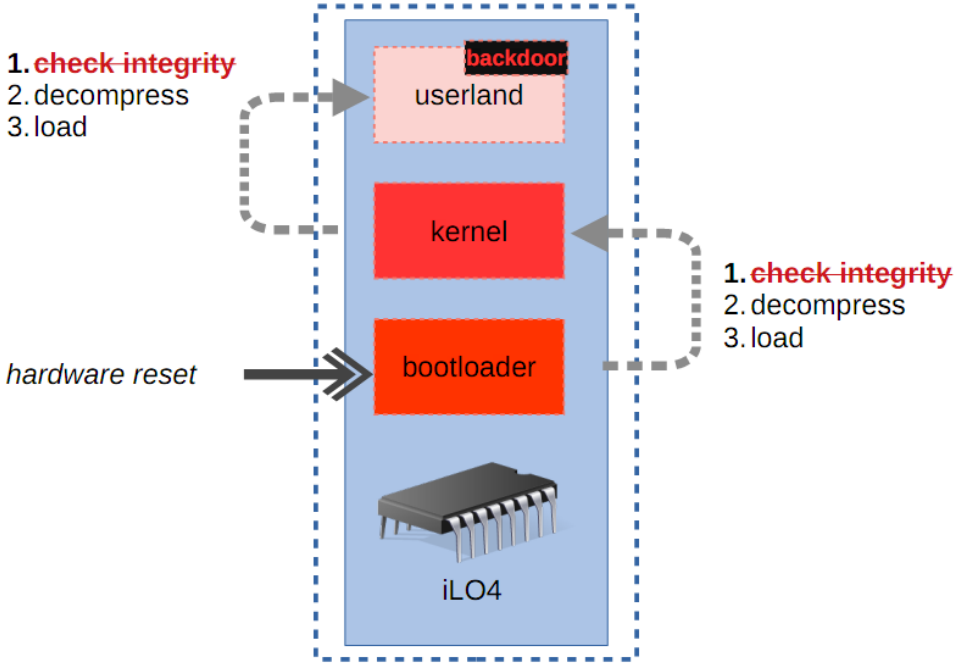
نسخه واقعی

پنل مدیریتی HP ILO

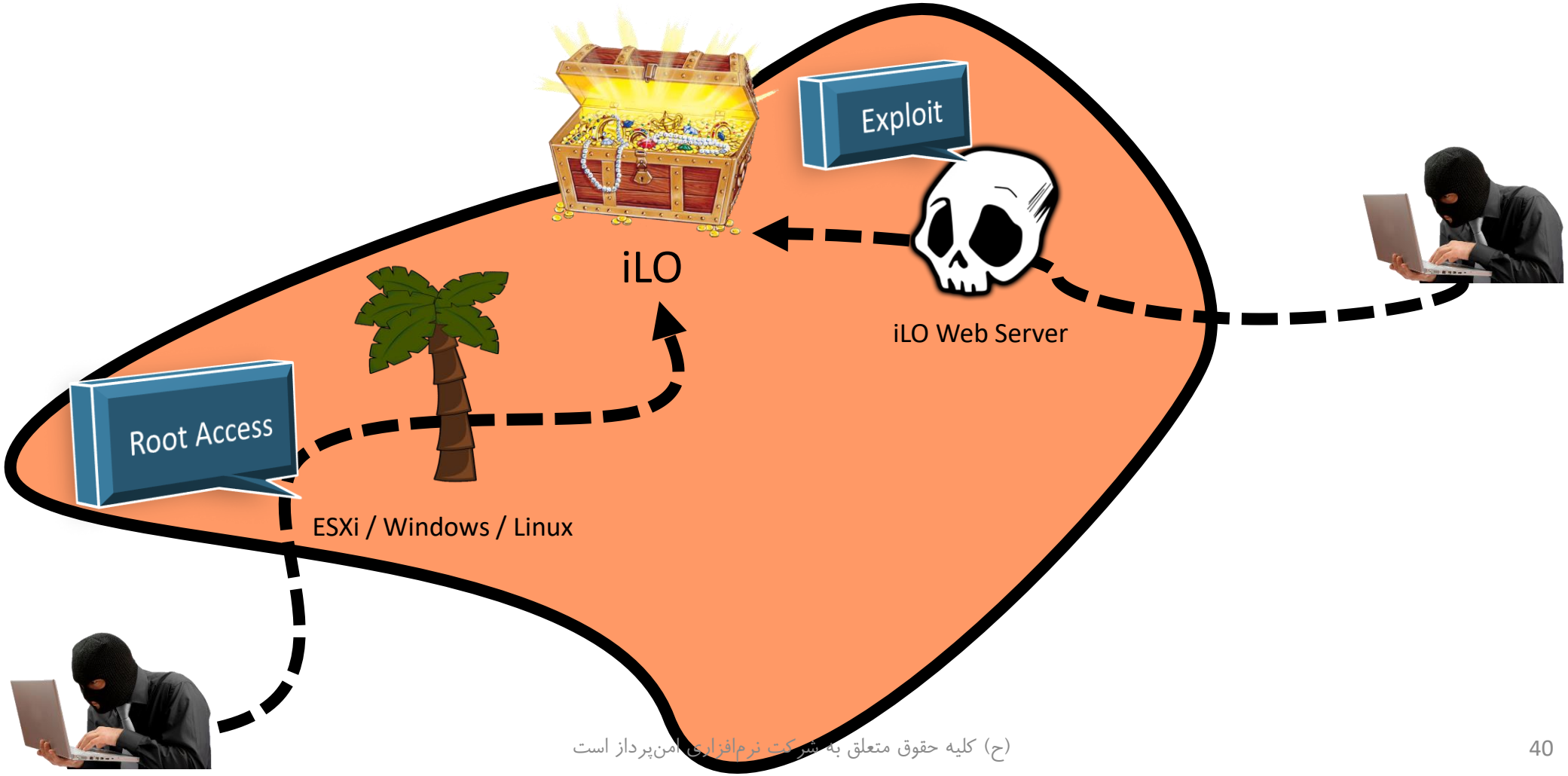
فرآیند بوت شدن سفت‌افزار ILO



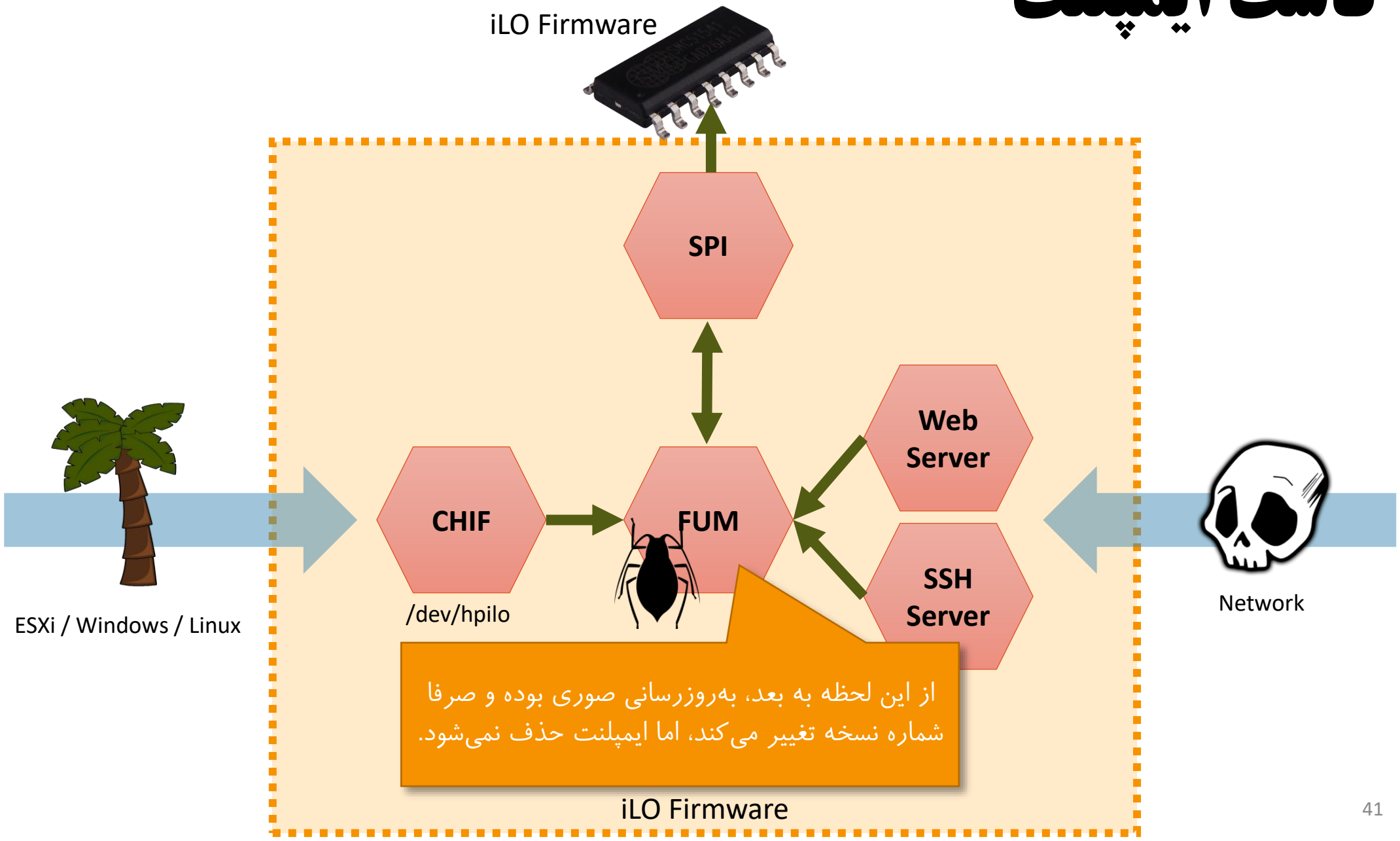
پس از آلودگی ...



کاشت implant در سفت‌افزار HP iLO

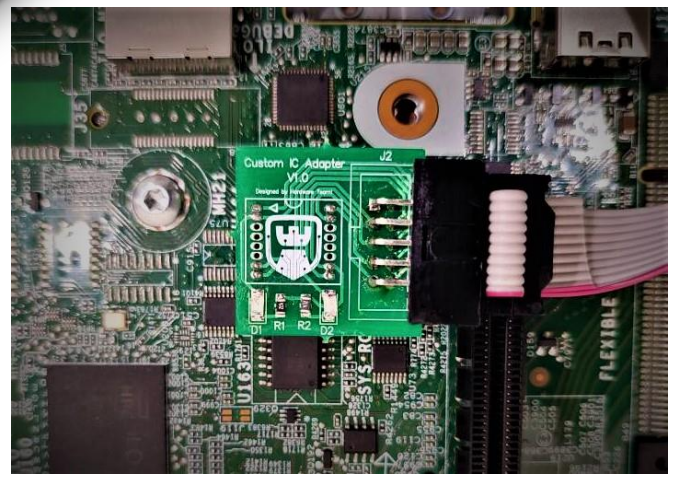


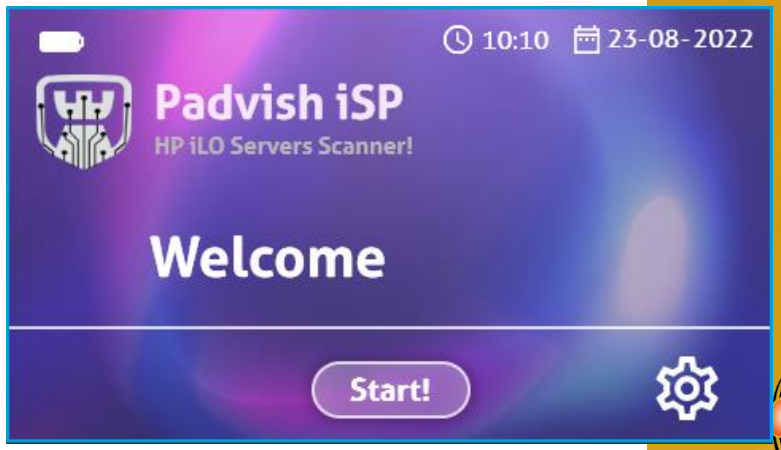
کاشت ایمپلنت



Padvish iLO Scanner

- بررسی اصالت سفت افزار iLO سرور
- پشتیبانی از سرورهای G7 تا G11
- قابلیت پاکسازی سفت‌افزار iLO





راهکار مقابله با حملات سایبری

به ابزار نمی‌توان تکیه کرد

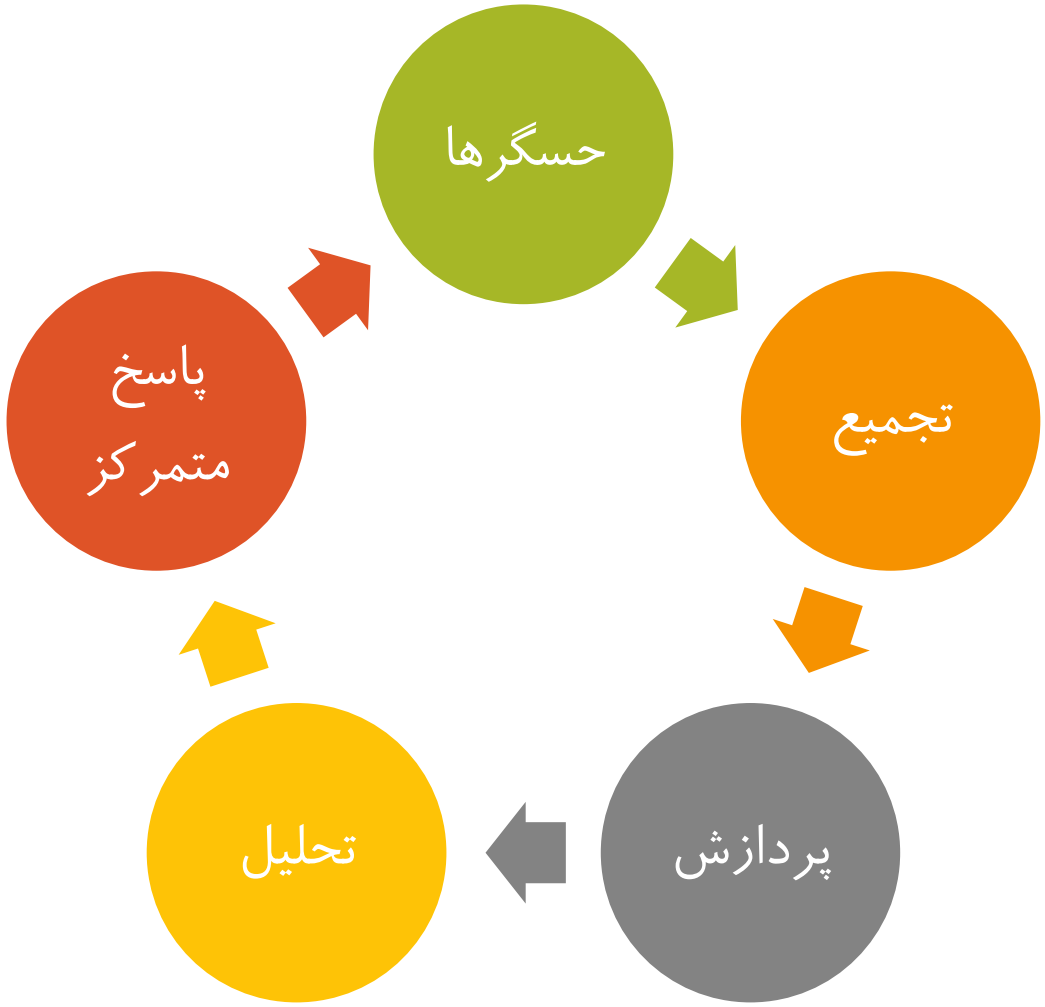
- «ابزار»های امنیتی، با «ابزار»های هک مقابله می‌کنند...

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

مرکز MXDR

- دفاع در عمق
- تهدیدات درون شبکه
- مقابله از درون
- رسیدگی و مقابله نقطه به نقطه

مرز سایبری

- قرار دادن مواضع در عمق
- تهدیدات برون شبکه
- مقابله از بیرون
- کاهش تهدیدات در کل شبکه

سخنرانی کلیدی کنفرانس انجمن رمز >>

آموخته‌های حملات سایبری
از تهدیدشناسی تا دفاع پیشگیرانه

در ادامه
شبیه‌سازی زنده حمله سایبری >>

سناریوی حمله