
MITRE ATT&CK Framework



MITRE Hakkında Giriş Bilgisi

Dijital sistemler var olduğundan beri siber saldırganlar, zamanın saldırı vektörlerini kullanarak sistemlere siber saldırılar gerçekleştirmişlerdir. Geçmişte, siber saldırılar basit ve anlaşılır saldırı yöntemlerinden oluşuyordu, çünkü karmaşık ve büyük dijital sistemler yoktu. Ancak zaman içinde dijital sistemler büyüdü ve daha karmaşık dijital yapılar haline geldi, bu da siber saldırıları daha gelişmiş yöntemlerle anlamak zorlaştırdı. Bu durum aynı zamanda siber saldırıların tespitini de zorlaştırmaktadır. Bugün, bir siber saldırıyı tam anlamıyla anlamak için, siber saldırıların adımlarını ve ayrıntılarını belirli gruplar için uygun bir şekilde modellemek gerekmektedir. Bu modelleme ihtiyacını karşılayan önemli çerçevelerden biri MITRE ATT&CK çerçevesidir.

MITRE'ye Giriş

MITRE Nedir?

MITRE, 1958 yılında ABD'de kurulan, ulusal güvenliği yeni yollarla ilerletmek ve kamu yararına bağımsız danışman olarak hizmet etmek için yenilikçi çözümler üreten bir kuruluştur. MITRE'nin çalışma alanları arasında Siber Güvenlik, Havacılık, Yapay Zeka ve Makine Öğrenimi, Havacılık ve Ulaşım, Savunma ve İstihbarat, Hükümet İnovasyonu, Sağlık, İç Güvenlik ve Telekom yer almaktadır.

MITRE ATT&CK Framework Nedir?

MITRE ATT&CK, Adversary Tactics, Techniques, and Common Knowledge (Saldırgan Taktikleri, Teknikleri ve Ortak Bilgiler) kısaltmasıyla bilinen bir bilgi veritabanı çerçevesidir. MITRE tarafından 2013 yılında tanıtılan ve teknoloji ile birlikte sürekli olarak geliştirilen bir çerçevedir. MITRE ATT&CK çerçevesi sayesinde siber saldırılar sistemli bir şekilde analiz edilebilir. Siber saldırılar belirli aşamalara bölünebilir ve her aşamada kullanılan yöntemler derinlemesine analiz edilerek, siber güvenlikle ilgili çalışmalarda kullanılabilir. MITRE ATT&CK Framework, siber güvenlik sektöründeki her çalışan için önemli bir kaynaktır.

MITRE ATT&CK Framework SOC Analistleri için Neden Önemlidir?

MITRE ATT&CK Framework, siber saldırıların her adımının detaylı bir şekilde ele alındığı için SOC Analistleri, siber saldırının her aşaması için hangi adımların atılması gerektiğini net bir şekilde görebilir ve referans olarak kullanabilir. Bu şekilde, siber saldırılara karşı geliştirilen saldırı tespit ve azaltma teknikleri daha etkili bir şekilde kullanılabilir, siber saldırılar haritalanabilir, detaylı bir rapor yazılabilir ve saldırının ayrıntıları daha sonra kullanmak üzere arşivlenebilir. Bu çerçeve, siber saldırıların net bir yol haritasını sağladığı için, henüz gerçekleşmemiş

olabilecek diğerk olası saldırılar hakkında arařtırmalar yapılarak, onları tespit etme veya önleme yolları geliştirilebilir.

Matrix

MITRE ATT&CK Matrix Nedir?

MITRE ATT&CK Matrix, siber saldırganların saldırı yöntemlerini sınıflandırmak ve görselleřtirmek için kullanılan bir yöntemdir. Matrisler neredeyse her konu için özelleřtirilebilir ve kullanışlı görseller haline getirilebilir. MITRE, saldırgan davranışının ayrıntılarını görselleřtirmek için MITRE ATT&CK matrislerini oluşturmuřtur.

Matris Türleri

MITRE ATT&CK Çerçevesi içinde platform türlerine göre 3 farklı matris oluşturulmuřtur:

1. Enterprise Matrix (Kurumsal Matris)
2. Mobile Matrix (Mobil Matris)
3. ICS (Industrial Control Systems) Matrix (Endüstriyel Kontrol Sistemleri Matrisi)

Enterprise Matrix (Kurumsal Matris)

Kurumsal Matrix, MITRE tarafından oluşturulan ilk matristir. Bu matris, diğerk matrislere dahil edilenden daha fazla dijital sistem içermekte ve daha yaygın kullanılmaktadır, bu nedenle diğerk matrislere göre bu matriste daha fazla bilgi bulunmaktadır. Kurumsal matris genellikle büyük organizasyonlara yönelik siber saldırıları anlamak için kullanılır.

Ařağıdaki görüntü, kurumsal matrisi detaylı olarak göstermektedir:

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (1)	Acquire Infrastructure (1)	Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (2)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary in the Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary in the Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (4)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (4)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (4)	Compromise Infrastructure (1)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Credentials from Password Stores (3)	Browser Bookmark Discovery	Audio Capture	Exfiltration Over Alternative Protocol (3)	Data Encoding (2)	Data Encrypted for Impact	Data Encrypted for Impact
Gather Victim Network Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Debugger Evasion	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Data Manipulation (3)	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Cloud Service Dashboard	Remote Services (4)	Browser Session Hijacking	Dynamic Resolution (2)	Exfiltration Over C2 Channel	Defacement (2)
Phishing for Information (2)	Obtain Capabilities (4)	Replication Through Removable Media	Scheduled Task/Job (2)	Compromise Client Software Binary	Domain Policy Modification (2)	Domain Policy Modification (2)	Direct Volume Access	Cloud Storage Object Discovery	Clipboard Data	Software Deployment Tools	Encrypted Channel (2)	Exfiltration Over Other Network Medium (2)	Endpoint Denial of Service (4)
Search Closed Sources (2)	Stage Capabilities (4)	Supply Chain Compromise (4)	Serverless Execution	Create Account (2)	Event Triggered Execution (14)	Event Triggered Execution (14)	Input Capture (4)	Container and Resource Discovery	Data from Cloud Storage	Taint Shared Content	Feedback Channels	Exfiltration Over Physical Medium (2)	Firmware Corruption
Search Open Technical Databases (2)	Search Open Websites/Domains (2)	Trusted Relationship	Software Deployment Tools	Create or Modify System Process (4)	Event Triggered Execution (14)	Event Triggered Execution (14)	Modify Authentication Process (2)	Debugger Evasion	Data from Configuration Repository (2)	Use Alternate Authentication Material (4)	Ingress Tool Transfer	Exfiltration Over Physical Medium (2)	Inhibit System Recovery
Search Victim-Owned Websites		Valid Accounts (4)	System Services (2)	External Remote Services	Event Triggered Execution (14)	Event Triggered Execution (14)	Multi-Factor Authentication Interception	Domain Trust Discovery	Data from Information Repositories (3)	Non-Application Layer Protocol	Multi-Stage Channels	Exfiltration Over Physical Medium (2)	Network Denial of Service (2)
			Windows Management Instrumentation	Hijack Execution Flow (12)	Process Injection (12)	Process Injection (12)	Multi-Factor Authentication Interception	File and Directory Discovery	Data from Local System	Non-Standard Port	Scheduled Transfer	Exfiltration Over Physical Medium (2)	Resource Hijacking
				Indicator Removal (2)	Scheduled Task/Job (2)	Scheduled Task/Job (2)	Network Service Discovery	Network Service Discovery	Data from Network Shared Drive	Protocol Tunneling	Transfer Data to Cloud Account	Exfiltration Over Physical Medium (2)	Service Stop
				Modify Authentication Process (2)	Office Application Startup (4)	Office Application Startup (4)	OS Credential Dumping (4)	Network Share Discovery	Data from Removable Media	Proxy (4)	Remote Access Software	Exfiltration Over Physical Medium (2)	System Shutdown/Reboot
				Pre-OS Boot (2)	Scheduled Task/Job (2)	Scheduled Task/Job (2)	Steal Application Access Token	Password Policy Discovery	Data Staged (2)	Trusted Relationship	Traffic Signaling (2)	Exfiltration Over Physical Medium (2)	System Shutdown/Reboot
				Server Software Component (2)	Server Software Component (2)	Server Software Component (2)	Steal or Forge Authentication Credentials	Peripheral Device Discovery	Email Collection (2)	Web Service (4)	Web Service (4)	Exfiltration Over Physical Medium (2)	System Shutdown/Reboot
				Traffic Signaling (2)	Traffic Signaling (2)	Traffic Signaling (2)	Steal or Forge Authentication Credentials	Permission Groups Discovery (2)	Input Capture (4)			Exfiltration Over Physical Medium (2)	System Shutdown/Reboot
							Steal Web Session Cookie	Query Registry	Screen Capture			Exfiltration Over Physical Medium (2)	System Shutdown/Reboot
							Unsecured Credentials (1)	Software Discovery (1)				Exfiltration Over Physical Medium (2)	System Shutdown/Reboot
							Unsecured Credentials (1)	System Information Discovery				Exfiltration Over Physical Medium (2)	System Shutdown/Reboot

Enterprise Matrix

Enterprise Matris'in altında 7 adet alt matris bulunmaktadır:

- PRE:** Bu alt matris, siber saldırıların Planlama ve Keşif aşamasına odaklanır. Saldırganların saldırı için bilgi toplama ve hazırlık yapmak için kullandıkları teknikleri ve taktikleri içerir.
- Windows:** Windows alt matrisi, özellikle Windows işletim sistemlerine yönelik saldırı teknikleri ve taktiklerini ele almaktadır. Windows tabanlı saldırıların çeşitli yönlerini kapsar ve zayıflıklar, ayrıcalıklar, süreklilik ve daha fazlası hakkında bilgi sağlar.
- macOS:** macOS alt matrisi, macOS işletim sistemlerine yönelik saldırı tekniklerini ve taktiklerini özel olarak ele alır. macOS tabanlı saldırıların çeşitli yönlerini kapsar ve zayıflıklar, ayrıcalıklar, süreklilik ve daha fazlası hakkında bilgi sağlar.
- Linux:** Linux alt matrisi, Linux işletim sistemlerine yönelik saldırı tekniklerini ve taktiklerini ele almaktadır. Linux tabanlı saldırıların çeşitli yönlerini kapsar ve zayıflıklar, ayrıcalıklar, süreklilik ve daha fazlası hakkında bilgi sağlar.
- Cloud:** Cloud alt matrisi, bulut tabanlı sistemlere yönelik saldırı tekniklerini ve taktiklerini ele almaktadır. Bulut tabanlı saldırıların çeşitli yönlerini kapsar ve güvenlik açıkları, kimlik doğrulama, veri sızıntısı ve daha fazlası hakkında bilgi sağlar.
- Network:** Network alt matrisi, ağlara yönelik saldırı tekniklerini ve taktiklerini ele almaktadır. Ağ tabanlı saldırıların çeşitli yönlerini kapsar ve ağ güvenliği, trafiği izleme, kimlik avı ve daha fazlası hakkında bilgi sağlar.
- Containers:** Containers alt matrisi, konteyner tabanlı sistemlere yönelik saldırı tekniklerini ve taktiklerini ele almaktadır. Konteyner tabanlı saldırıların çeşitli yönlerini kapsar ve konteyner güvenliği, ayrıcalıklar, saldırı yüzeyi ve daha fazlası hakkında bilgi sağlar.

Daha fazla bilgi için Kurumsal Matris ve alt matrislere aşağıdaki bağlantıyı kullanarak erişebilirsiniz:

Enterprise Matris: <https://attack.mitre.org/matrices/enterprise/>

MATRICES

Enterprise

PRE

Windows

macOS

Linux

Cloud

Network

Containers

Mobile

ICS

Mobil Matris

Mobil matris, mobil cihazlar için hazırlanan ve mobil cihazların siber güvenliği hakkında bilgi içeren bir matristir. Bu matris, bireysel ve kurumsal mobil cihazların güvenliğini sağlamak için kullanılabilir. Kurumsal Matris ile karşılaştırıldığında, daha az bilgi içermektedir.

Mobil Matris'e aşağıdaki bağlantıyı kullanarak ulaşabilir ve daha fazla bilgi edinebilirsiniz:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
4 techniques	3 techniques	7 techniques	3 techniques	14 techniques	5 techniques	8 techniques	2 techniques	13 techniques	8 techniques	2 techniques	9 techniques
<ul style="list-style-type: none"> Drive-By Compromise Lockscreen Bypass Replication Through Removable Media Supply Chain Compromise (3) 	<ul style="list-style-type: none"> Command and Scripting Interpreter (1) Native API Scheduled Task/Job 	<ul style="list-style-type: none"> Boot or Logon Initialization Scripts Compromise Application Executable Compromise Client Software Binary Event Triggered Execution (1) Foreground Persistence Hijack Execution Flow (1) Scheduled Task/Job 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism (1) Exploitation for Privilege Escalation Process Injection (1) 	<ul style="list-style-type: none"> Download New Code at Runtime Execution Guardrails (1) Foreground Persistence Hide Artifacts (2) Hooking Impair Defenses (3) Indicator Removal on Host (3) Input Injection Native API Obfuscated Files or Information (2) Process Injection (1) Proxy Through Victim Subvert Trust Controls (1) Virtualization/Sandbox Evasion (1) 	<ul style="list-style-type: none"> Access Notifications Clipboard Data Credentials from Password Store (1) Input Capture (2) Steal Application Access Token (1) 	<ul style="list-style-type: none"> File and Directory Discovery Location Tracking (2) Network Service Scanning Process Discovery Software Discovery (1) System Information Discovery System Network Configuration Discovery System Network Connections Discovery 	<ul style="list-style-type: none"> Exploitation of Remote Services Replication Through Removable Media 	<ul style="list-style-type: none"> Access Notifications Adversary-In-the-Middle Archive Collected Data Audio Capture Call Control Clipboard Data Data from Local System Input Capture (2) Location Tracking (2) Protected User Data (4) Screen Capture Stored Application Data Video Capture 	<ul style="list-style-type: none"> Application Layer Protocol (1) Call Control Dynamic Resolution (1) Encrypted Channel (2) Ingress Tool Transfer Non-Standard Port Out of Band Data Web Service (3) 	<ul style="list-style-type: none"> Exfiltration Over Alternative Protocol (1) Exfiltration Over C2 Channel 	<ul style="list-style-type: none"> Account Access Removal Call Control Data Encrypted for Impact Data Manipulation (1) Endpoint Denial of Service Generate Traffic from Victim Input Injection Network Denial of Service SMS Control

Mobil Matris, 2 adet alt matris içermektedir:

1. **Android:** Android alt matrisi, Android işletim sistemine yönelik saldırı tekniklerini ve taktiklerini ele almaktadır. Android tabanlı cihazlara yönelik saldırıların çeşitli yönlerini kapsar ve güvenlik açıkları, zararlı yazılımlar, kullanıcı izinleri ve daha fazlası hakkında bilgi sağlar.
2. **iOS:** iOS alt matrisi, iOS işletim sistemine yönelik saldırı tekniklerini ve taktiklerini ele almaktadır. iOS tabanlı cihazlara yönelik saldırıların çeşitli yönlerini kapsar ve güvenlik açıkları, zararlı yazılımlar, kullanıcı izinleri ve daha fazlası hakkında bilgi sağlar.

MATRICES

Enterprise

Mobile

Android

iOS

ICS

ICS Matrix

ICS Matrix, endüstriyel kontrol sistemlerindeki cihazların siber güvenliği için toplanan bilgileri içeren matristir. Bu matris, bir ICS'nin siber güvenliğini sağlamak ve analiz etmek için kullanılabilir.

ICS Matrix: <https://attack.mitre.org/matrices/ics/>

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Tactics (Taktikler)

Taktik, siber saldırganın amacını ve eyleminin nedenini ifade eder.

Taktikler, siber saldırgan davranışlarını gruplandırmak ve saldırı adımlarını görmek için kullanılan en önemli MITRE ATT&CK Framework bileşenlerinden biridir. Taktikler matrisin üst satırında yer alır.

Örnek olarak, kurumsal matristeki taktikler aşağıdaki görüntüde gösterilmektedir:

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
19 techniques	7 techniques	9 techniques	11 techniques	11 techniques	11 techniques	42 techniques	17 techniques	20 techniques	9 techniques	17 techniques	15 techniques	9 techniques	11 techniques
Active Scanning (1)	Acquire Infrastructure (1)	Drive-by Compromise	Command and Scripting Interference (1)	Account Manipulation (1)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Adversary in-the-Middle (1)	Account Discovery (1)	Exploitation of Remote Services	Adversary in-the-Middle (1)	Application Layer Protocol (1)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (1)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (1)	Access Token Manipulation (1)	Brute Force (1)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1)	Communication Through Removable Media	Data Transfer Side Limits	Data Destruction
Gather Victim Identity Information (1)	Compromise Infrastructure (1)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (1)	Boot or Logon Autostart Execution (1)	Boot or Logon Autostart Execution (1)	Credentials from Password Stores (1)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (1)	Exfiltration Over Alternative Protocol (1)	Data Encrypted for Impact
Gather Victim Network Information (1)	Develop Capabilities (1)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (1)	Boot or Logon Initialization Scripts (1)	Boot or Logon Initialization Scripts (1)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (1)	Automated Collection	Data Obfuscation (1)	Exfiltration Over C2 Channel	Data Manipulation (1)
Gather Victim Org Information (1)	Establish Accounts (1)	Phishing (1)	Inter-Process Communication (1)	Browser Extensions	Create or Modify System Process (1)	Create or Modify System Process (1)	Forced Authentication	Cloud Service Dashboard	Remote Services (1)	Clipboard Data	Dynamic Resolution (1)	Exfiltration Over Other Network Medium (1)	Defacement (1)
Privilege for Information (1)	Obtain Capabilities (1)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (1)	Domain Policy Modification (1)	Forge Web Credentials (1)	Cloud Storage Object Discovery	Application Through Removable Media	Encrypted Channel (1)	Feedback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (1)
Search Closed Sources (1)	Stage Capabilities (1)	Supply Chain Compromise (1)	Scheduled Task/Job (1)	Create Account (1)	Escape to Host	Escape to Host	Input Capture (1)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Ingress Tool Transfer	Exfiltration Over Web Service (1)	Firmware Corruption
Search Open Technical Databases (1)	Trusted Relationship	Serverless Execution	Shared Modules	Event Triggered Execution (1)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (1)	Data from Configuration Repository (1)	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
Search Open Webserver/Domains (1)	Valid Accounts (1)	User Execution (1)	Software Deployment Tools	External Remote Services	Hijack Execution Flow (1)	Hijack Execution Flow (1)	Multi-Factor Authentication Request Generation	File and Directory Permissions Modification (1)	Network Service Discovery	Data from Information Repositories (1)	Non-Standard Port	System Shutdown/Reboot	Resource Hijacking
Search Victim-Owned Websites		Windows Management Instrumentation	System Services (1)	Process Injection (1)	Process Injection (1)	Process Injection (1)	Network Sniffing	Network Share Discovery	Network Share Discovery	Data from Network Shared Drive	Protocol Tunneling		

Taktiklerin Türleri

Taktikler genellikle saldırının amacını ve nedenini ifade ettikleri için genel ifadelerden oluşur. Bu nedenle, her matris için taktikler büyük ölçüde benzerdir.

Örneğin, aşağıdaki görüntü, kurumsal matrise ait Initial Access(İlk Erişim) taktiği hakkında detaylı bilgileri göstermektedir:

[Home](#) > [Tactics](#) > [Enterprise](#) > [Initial Access](#)

Initial Access

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

ID: TA0001

Created: 17 October 2018

Last Modified: 19 July 2019

[Version](#) [Permalink](#)

Techniques

Techniques: 9

ID	Name	Description
T1189	Drive-by Compromise	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token .

Enterprise Taktikleri

Taktikler, ATT&CK tekniği veya alt tekniklerinin “neden”ini temsil eder. Bu, saldırganın eylem gerçekleştirmesinin taktiksel hedefidir: bir eylemi gerçekleştirmenin nedenidir. Örneğin, bir saldırgan kimlik bilgilerine erişmek isteyebilir.

Aşağıdaki listede 14 farklı taktik sıralanmıştır.

Enterprise Tactics: <https://attack.mitre.org/tactics/enterprise/>

ID	Name	Description
TA0043	Reconnaissance	Saldırgan, gelecekteki operasyonları planlamak için kullanabilecekleri bilgileri toplamaya çalışıyor.
TA0042	Resource Development	Saldırgan, operasyonları desteklemek için kullanabilecekleri kaynakları oluşturmaya çalışıyor.
TA0001	Initial Access	Saldırgan, ağınıza girmeye çalışıyor.
TA0002	Execution	Saldırgan, zararlı kodu çalıştırmaya çalışıyor.
TA0003	Persistence	Saldırgan, elde ettiği kavrama noktasını sürdürmeye çalışıyor.
TA0004	Privilege Escalation	Saldırgan, daha yüksek düzeyde izinler elde etmeye çalışıyor.
TA0005	Defense Evasion	Saldırgan, tespit edilmekten kaçınmaya çalışıyor.
TA0006	Credential Access	Saldırgan, hesap adlarını ve parolaları çalmaya çalışıyor.
TA0007	Discovery	Saldırgan, çevrenizi anlamaya çalışıyor.
TA0008	Lateral Movement	Saldırgan, çevrenizde hareket etmeye çalışıyor.
TA0009	Collection	Saldırgan, hedeflerine ilgi duyduğu verileri toplamaya çalışıyor.
TA0011	Command n Control	Saldırgan, etkilenen sistemlerle iletişim kurarak onları kontrol etmeye çalışıyor.
TA0010	Exfiltration	Saldırgan, veri çalmaya çalışıyor.
TA0040	Impact	Saldırgan, sistemlerinizi ve verilerinizi manipüle etmeye, kesintiye uğratmaya veya yok etmeye çalışıyor.

TACTICS

Enterprise



Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

Mobil Taktikleri

Aşağıdaki listede 14 farklı taktik sıralanmıştır.

Mobile Tactics: <https://attack.mitre.org/tactics/mobile/>

ID	Name	Description
TA0027	Initial Access	Saldırgan, cihazınıza girmeye çalışıyor.
TA0041	Execution	Saldırgan, zararlı kodu çalıştırmaya çalışıyor.
TA0028	Persistence	Saldırgan, elde ettiği kavrama noktasını sürdürmeye çalışıyor.
TA0029	Privilege Escalation	Saldırgan, daha yüksek düzeyde izinler elde etmeye çalışıyor.
TA0030	Defense Evasion	Saldırgan, tespit edilmekten kaçınmaya çalışıyor.
TA0031	Credential Access	Saldırgan, hesap adlarını, parolaları veya diğer gizli bilgileri çalmaya çalışıyor, bu bilgiler kaynaklara erişimi sağlıyor.
TA0032	Discovery	Saldırgan, çevrenizi anlamaya çalışıyor.
TA0033	Lateral Movement	Saldırgan, çevrenizde hareket etmeye çalışıyor.
TA0035	Collection	Saldırgan, hedeflerine ilgi duyduğu verileri toplamaya çalışıyor.
TA0037	Command n Control	Saldırgan, etkilenen cihazlarla iletişim kurarak onları kontrol etmeye çalışıyor.
TA0036	Exfiltration	Saldırgan, veri çalmaya çalışıyor.
TA0034	Impact	Saldırgan, cihazlarınızı ve verilerinizi manipüle etmeye, kesintiye uğratmaya veya yok etmeye çalışıyor.
TA0038	Network Effects	Saldırgan, cihaza gelen veya cihazdan giden ağ trafiğini kesmek veya manipüle etmeye çalışıyor.
TA0039	Remote Service Effects	Saldırgan, uzaktan hizmetleri kullanarak cihazı kontrol etmeye veya izlemeye çalışıyor.

TACTICS

Mobile



Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Network Effects

Remote Service Effects

ICS Taktikleri

Aşağıdaki listede 12 farklı taktik sıralanmıştır.

ICS Tactics: <https://attack.mitre.org/tactics/ics/>

ID	Name	Description
TA0108	Initial Access	Saldırgan, ICS ortamınıza girmeye çalışıyor.
TA0104	Execution	Saldırgan, kod çalıştırmaya veya sistem işlevlerini, parametrelerini ve verilerini izinsiz şekilde manipüle etmeye çalışıyor.
TA0110	Persistence	Saldırgan, ICS ortamındaki yerini korumaya çalışıyor.
TA0111	Privilege Escalation	Saldırgan, daha yüksek düzeyde izinler elde etmeye çalışıyor.
TA0103	Evasion	Saldırgan, güvenlik savunmalarından kaçınmaya çalışıyor.
TA0102	Discovery	Saldırgan, çevrenizi değerlendirmek ve hedeflerinizi belirlemek için bilgi buluyor.
TA0109	Lateral Movement	Saldırgan, ICS ortamınızda hareket etmeye çalışıyor.
TA0100	Collection	Saldırgan, ICS ortamınızla ilgili ilgi duyduğu verileri ve alan bilgisini toplamaya çalışıyor.
TA0101	Command n Control	Saldırgan, ICS ortamınıza erişimi olan kompromize edilmiş sistemleri, denetleyicileri ve platformları ile iletişim kurmaya ve kontrol etmeye çalışıyor.
TA0107	Inhibit Response Function	Saldırgan, güvenlik, koruma, kalite güvence ve operatör müdahale fonksiyonlarının bir arıza, tehlike veya güvensiz duruma yanıt vermesini engellemeye çalışıyor.
TA0106	Impair Process Control	Saldırgan, fiziksel kontrol süreçlerini manipüle etmeye, devre dışı bırakmaya veya zarar vermeye çalışıyor.
TA0105	Impact	Saldırgan, ICS sistemlerinizi, verilerinizi ve çevrelerinizi manipüle etmeye, kesintiye uğratmaya veya yok etmeye çalışıyor.

TACTICS

Enterprise



Mobile



ICS



Initial Access

Execution

Persistence

Privilege Escalation

Evasion

Discovery

Lateral Movement

Collection

Command and Control

Inhibit Response Function

Impair Process Control

Impact

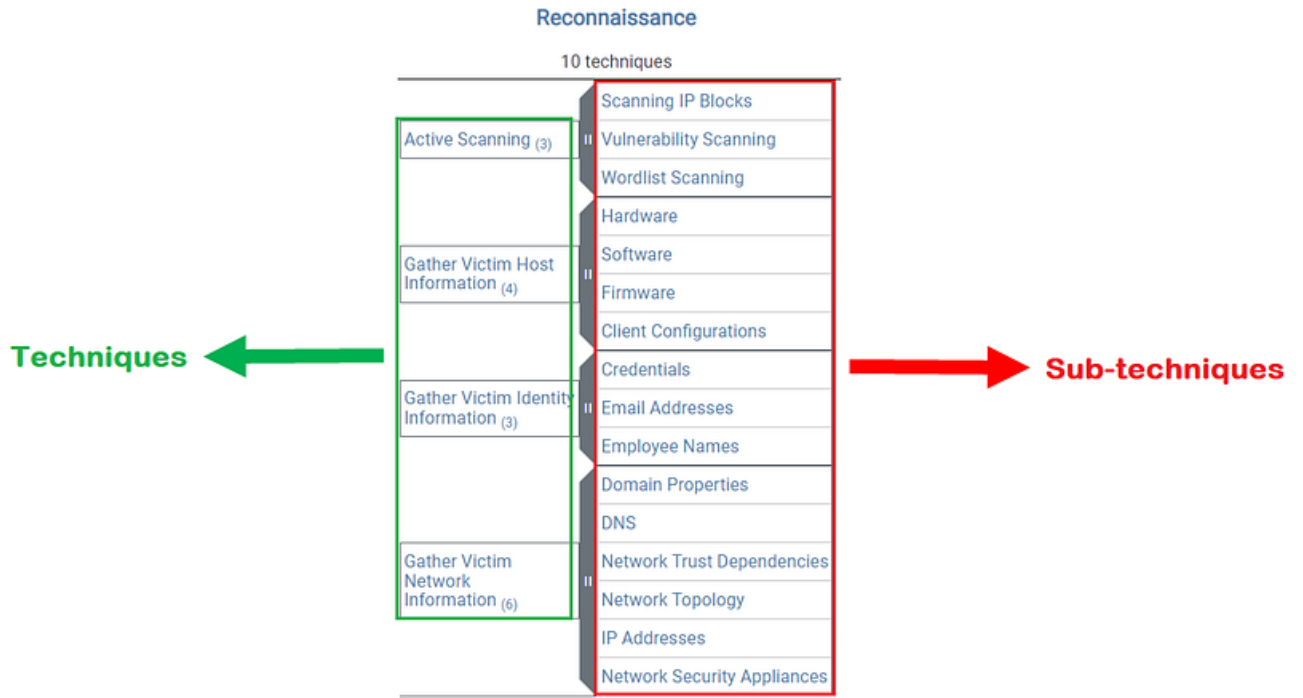
Techniques and Sub-Techniques (Teknikler ve Alt Teknikler)

Matris içindeki taktikler, saldırganların amaçlarını gösterir ancak saldırganın saldırı yöntemi hakkında detaylı bilgi içermez. Bununla birlikte, teknikler ve alt teknikler, saldırganın hedefine ulaşmak için kullandığı yöntemleri ve saldırıyı nasıl gerçekleştirdiğini gösterir. Her teknik/alt teknik, belirli bir taktiğe bağlı olarak matrise dahil edilir. Örneğin, enterprise matrisindeki bazı teknikler aşağıdaki resimde gösterilmiştir:

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	15 techniques	13 techniques	42 techniques	17 techniques	20 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (1)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (2)	Account Manipulation (1)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Adversary in the Middle (2)	Account Discovery (1)	Exploitation of Remote Services	Adversary in the Middle (2)	Application Layer Protocol (1)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (1)	Compromise Accounts (1)	Exploit Public-Facing Application	Container Administration Command	Access Token Manipulation (1)	Access Token Manipulation (1)	Access Token Manipulation (1)	Brute Force (1)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (1)	Compromise Infrastructure (1)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (1)	Boot or Logon Autostart Execution (1)	Boot or Logon Autostart Execution (1)	Credentials from Password Stores (1)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (1)	Develop Capabilities (1)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (1)	Boot or Logon Initialization Scripts (1)	Boot or Logon Initialization Scripts (1)	Build Image on Host	Cloud Infrastructure Discovery	Remote Service Session Hijacking (1)	Automated Collection	Data Obfuscation (1)	Exfiltration Over C2 Channel	Data Manipulation (1)
Gather Victim Org Information (1)	Establish Accounts (1)	Phishing (1)	Inter-Process Communication (1)	Browser Extensions	Browser Extensions	Browser Extensions	Debugger Evasion	Cloud Service Dashboard	Remote Services (1)	Clipboard Data	Dynamic Resolution (1)	Exfiltration Over Other Network Medium (1)	Defacement (1)
Phishing for Information (1)	Obtain Capabilities (1)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (1)	Create or Modify System Process (1)	Deobfuscate/Decode Files or Information	Cloud Service Discovery	Application Through Removable Media	Encrypted Channel (1)	Endpoint Denial of Service (1)	Exfiltration Over Other Network Medium (1)	Disk Wipe (1)
Search Closed Sources (1)	Stage Capabilities (1)	Trusted Relationship	Scheduled Task/Job (1)	Domain Policy Modification (1)	Domain Policy Modification (1)	Domain Policy Modification (1)	Forge Web Credentials (1)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Firmware Corruption	Endpoint Denial of Service (1)	Endpoint Denial of Service (1)
Search Open Technical Databases (1)		Valid Accounts (1)	Serverless Execution	Event Triggered Execution (1)	Event Triggered Execution (1)	Event Triggered Execution (1)	Input Capture (1)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (1)	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Inhibit System Recovery
Search Open Websites/Domains (1)			Software Deployment Tools	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Modify Authentication Process (1)	Domain Trust Discovery	Use Alternate Authentication Material (1)	Data from Information Repositories (1)	Multi-Stage Channels	Exfiltration Over Web Service (1)	Network Denial of Service (1)
Search Victim-Owned Websites			User Execution (1)	HiJack Execution Flow (1)	HiJack Execution Flow (1)	HiJack Execution Flow (1)	Multi-Factor Authentication Interception	File and Directory Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
			Windows Management Instrumentation	Impair Defenses (1)	Impair Defenses (1)	Impair Defenses (1)	Multi-Factor Authentication Request Generation	Group Policy Discovery		Data from Removable Media	Non-Standard Port	Transfer Data to Cloud Account	System Shutdown/Reboot
				Indicator Removal (1)	Indicator Removal (1)	Indicator Removal (1)	Network Sniffing	Network Share Discovery		Data Staged (1)	Protocol Tunneling		
				Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	OS Credential Dumping (1)	Network Sniffing		Email Collection (1)	Proxy (1)		
				Modify Authentication Process (1)	Modify Authentication Process (1)	Modify Authentication Process (1)	OS Credential Dumping (1)	Peripheral Device Discovery		Input Capture (1)	Remote Access Software		
				Office Application Startup (1)	Office Application Startup (1)	Office Application Startup (1)	OS Credential Dumping (1)	Permission Groups Discovery (1)		Screen Capture	Traffic Signaling (1)		
				Pre-OS Boot (1)	Pre-OS Boot (1)	Pre-OS Boot (1)	OS Credential Dumping (1)	Process Discovery		Video Capture	Web Service (1)		
				Scheduled Task/Job (1)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	OS Credential Dumping (1)	Query Registry					
				Server Software Component (1)	Server Software Component (1)	Server Software Component (1)	OS Credential Dumping (1)	Remote System Discovery					
				Traffic Signaling (1)	Traffic Signaling (1)	Traffic Signaling (1)	OS Credential Dumping (1)	Software Discovery (1)					
							Unsecured Credentials (1)	System Information					

Resimdeki matristeki alanların çoğunluğu tekniklerdir. Bazı teknikler alt tekniklere sahipken bazılarının sahip değildir.

Yukarıdaki resimde gösterildiği gibi, matriste tekniklerin adlarının yazıldığı olduğu kutuların yanında gri bölgeler varsa, bu tekniklerin alt tekniklere sahip olduğunu gösterir. Örneğin, “Reconnaissance” taktiğinin altındaki ilk 4 tekniğin alt tekniklerine bakalım:



Teknikler ve Alt-Tekniklerin Tipleri

Teknikler matrislere göre 3 gruba ayrılır:

- Enterprise Techniques
- Mobile Techniques
- ICS Techniques

Enterprise Teknikleri

Enterprise tekniklerinin sayısı oldukça fazladır ve sürekli olarak güncellenir. Mevcut sayılar (10.05.2023) şu şekildedir:

Teknikler: 193

Alt teknikler: 401

Mevcut sayıları aşağıdaki bağlantıdan kontrol edebilirsiniz:

<https://attack.mitre.org/techniques/enterprise/>

Mobile Techniques

Mobil tekniklerin toplam sayısı enterprise tekniklerinden daha azdır ve zaman içinde güncellenir. Mevcut mobil tekniklerin ve alt tekniklerin

sayısı şu şekildedir:

Teknikler: 66

Alt teknikler: 41

Mevcut sayıları aşağıdaki bağlantıdan kontrol edebilirsiniz:

<https://attack.mitre.org/techniques/mobile/>

ICS Techniques

Diğer matrislerin teknikleri gibi ICS teknikleri de zaman içinde güncellenir. Mevcut ICS tekniklerinin ve alt tekniklerin sayısı şu şekildedir:

Teknikler: 79

Alt teknikler: 0

Mevcut sayıları aşağıdaki bağlantıdan kontrol edebilirsiniz:

<https://attack.mitre.org/techniques/ics/>

Prosedür Nedir ?

Prosedür, tekniklerin ve alt-tekniklerin kullanım örneklerini içerir. Basitçe, tekniklerin uygulanması sırasında hangi araç/yazılımın kullanıldığını gösterir. Başka bir deyişle, tekniklerin pratik kullanımı hakkında bilgi verir.

OS Credential Dumping” tekniği için bir prosedür örneği aşağıdaki resimde bulunmaktadır.

Prosedürlere tekniklerin bulunduğu sayfa üzerinden de erişilebilir.

Procedure Example

ID	Name	Description
G0087	APT39	APT39 has used different versions of Mimikatz to obtain credentials. ^[6]

Mitigations

Mitigasyonlar, MITRE ATT&CK matrisindeki tekniklere karşı alınabilecek önlemler ve eylemleri ifade eder. Her bir mitigasyonun benzersiz bir kimliği, adı ve açıklaması bulunur, bu da onları anlaşılır kılar. Örneğin, aşağıdaki görsel, enterprise mitigasyonlarından birini göstermektedir.

Filter Network Traffic

Use network appliances to filter ingress or egress traffic and perform protocol-based filtering.
Configure software on endpoints to filter network traffic.

ID: M1037
Version: 1.1
Created: 11 June 2019
Last Modified: 20 June 2020

[Version Permalink](#)

Techniques Addressed by Mitigation

ATT&CK® Navigator Layers ▾

Domain	ID	Name	Use
Enterprise	T1557	Adversary-in-the-Middle	Use network appliances and host-based security software to block network traffic that is not necessary within the environment, such as legacy protocols that may be leveraged for AiTM conditions.
		.001 LLMNR/NBT-NS Poisoning and SMB Relay	Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks. ^{[1][2][3]}
		.002 ARP Cache Poisoning	Consider enabling DHCP Snooping and Dynamic ARP Inspection on switches to create mappings between IP addresses requested via DHCP and ARP tables and tie the values to a

Mitigasyon Tipleri

- Enterprise Mitigations
- Mobile Mitigations
- ICS Mitigations

1. Enterprise Mitigations

Enterprise Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

Mitigations: 43

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.

Bu tarihte güncel olarak enterprise mitigasyonlarının sayısı aşağıdaki gibidir:

Mitigasyonlar: 43

Güncel sayıları görmek için aşağıdaki bağlantıyı kontrol edebilirsiniz:

<https://attack.mitre.org/mitigations/enterprise/>

2. Mobile Mitigations

Mobile Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

Mitigations: 11

ID	Name	Description
M1013	Application Developer Guidance	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.
M1002	Attestation	Enable remote attestation capabilities when available (such as Android SafetyNet or Samsung Knox TIMA Attestation) and prohibit devices that fail the attestation from accessing enterprise resources.

Bu tarihte güncel olarak mobil mitigasyonlarının sayısı aşağıdaki gibidir:

Mitigasyonlar: 11

Güncel sayıları görmek için aşağıdaki bağlantıyı kontrol edebilirsiniz:

<https://attack.mitre.org/mitigations/mobile/>

3. ICS Mitigations

Home > Mitigations > ICS

ICS Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

Mitigations: 51

ID	Name	Description
M0801	Access Management	Access Management technologies can be used to enforce authorization policies and decisions, especially when existing field devices do not provide sufficient capabilities to support user identification and authentication. These technologies typically utilize an in-line network device or gateway system to prevent access to unauthenticated users, while also integrating with an authentication service to first verify user credentials.
M0936	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.

Bu tarihte güncel olarak ICS mitigasyonlarının sayısı aşağıdaki gibidir:

Mitigasyonlar: 51

Güncel sayıları görmek için aşağıdaki bağlantıyı kontrol edebilirsiniz:

ICS Mitigasyonları: <https://attack.mitre.org/mitigations/ics/>

Groups

Gelişmiş Kalıcı Tehdit (Advanced Persistent Threat—APT) Grupları, hedefe yönelik ve sistematik bir şekilde siber saldırıları gerçekleştiren, zaman zaman hükümetlerin desteğiyle hareket eden farklı kişiler ve grupları içerebilen hacker gruplarıdır. APT grupları farklı motivasyonlarla siber saldırılar düzenleyebilir. Örneğin, grup belirli bir misyona sahip olabilir, saldırılarını maddi kazanç için gerçekleştirebilir veya yabancı bir devletin desteğini alarak ulusal ideallerini elde etmek amacıyla saldırılar düzenleyebilir.

MITRE ATT&CK Framework içerisinde APT gruplarıyla ilgili bilgiler toplanır ve hangi APT grubunun hangi sistemlere yönelik hedef aldığı ve hangi siber saldırı tekniklerini uyguladığı belirlenmeye yardımcı olur.

Bu bilgiler, MITRE ATT&CK matrisiyle birlikte bir araya getirilip değerlendirildiğinde, APT grubunun saldırı haritası ortaya çıkar.

Gruplar: 135

Güncel sayıları görmek için aşağıdaki bağlantıyı kontrol edebilirsiniz:

<https://attack.mitre.org/groups/>

Yukarıdaki site ziyaret edildiğinde, sayfanın sol tarafında aşağıdaki gibi bir menü görünecektir:

GROUPS

Overview

admin@338

Ajax Security Team

ALLANITE

Andariel

Aoqin Dragon

APT-C-36

APT1

APT12

APT16

APT17

APT18

APT19

APT28

APT29

Bu menüyü kullanarak, listelenen APT grupları hakkında bilgilere erişilebilir. Örneğin, “Lazarus Group” APT grubu hakkındaki bilgiler aşağıdaki gibi:

Lazarus Group

Lazarus Group is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau.^{[1][2]} The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by **Lazarus Group** correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.^[3]

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name **Lazarus Group** instead of tracking clusters or subgroups, such as **Andariel**, **APT37**, **APT38**, and **Kimsuky**.

ID: G0032

① Associated Groups: Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY

Contributors: Kyaw Pyi Htet, @KyawPyiHtet; Dragos Threat Intelligence

Version: 3.1

Created: 31 May 2017

Last Modified: 23 August 2022

[Version Permalink](#)

Grup Adı: Lazarus Group

Diğer Adları: Hidden Cobra, Guardians of Peace, Zinc, NICKEL ACADEMY, APT38

Açıklama: Lazarus Group, Kuzey Kore ile ilişkilendirilen bir APT grubudur. Finansal hırsızlık, casusluk ve siber sabotaj gibi çeşitli amaçlarla faaliyet gösterir. Grup, banka hırsızlıkları, fidye yazılımları saldırıları ve cryptocurrency hırsızlığı gibi çeşitli saldırılar gerçekleştirmiştir.

Kaynaklar: APT Groups, Lazarus Group

Saldırılar: Lazarus Group, Hidden Cobra, Guardians of Peace, Zinc, NICKEL ACADEMY, APT38 gibi adlarla da bilinen Lazarus Group, birçok farklı siber saldırı gerçekleştirmiştir. Örnek saldırılar arasında Sony Pictures Entertainment saldırısı, WannaCry fidye yazılım saldırısı ve birçok banka hırsızlığı saldırısı bulunmaktadır.

Yukarıdaki resimde görüldüğü gibi, MITRE ATT&CK Framework'te listelenen her APT grubunun benzersiz bir Grup Kimliği (Group ID), Adı (Name) ve Açıklaması (Description) vardır.

Ayrıca sayfanın alt kısmında, grup tarafından siber saldırılarda kullanılan tekniklere ilişkin bilgilere de erişebilirsiniz.

Techniques Used

ATT&CK® Navigator Layers ▾

Domain	ID	Name	Use
Enterprise	T1134	.002 Access Token Manipulation: Create Process with Token	Lazarus Group keylogger KiloAlfa obtains user tokens from interactive sessions to execute itself with API call <code>CreateProcessAsUserA</code> under that user's context. ^{[3][8]}
Enterprise	T1087	.002 Account Discovery: Domain Account	Lazarus Group has queried an active directory server to obtain the list of accounts, including administrator accounts. ^[9]
Enterprise	T1098	Account Manipulation	Lazarus Group malware WhiskeyDelta-Two contains a function that attempts to rename the administrator's account. ^{[3][10]}
Enterprise	T1583	.001 Acquire Infrastructure: Domains	Lazarus Group has acquired domains related to their campaigns to act as distribution points and C2 channels. ^{[11][9][12]}
		.004 Acquire Infrastructure: Server	Lazarus Group has acquired servers to host their malicious tools. ^[9]
		.006 Acquire Infrastructure: Web Services	Lazarus Group has hosted malicious downloads on Github and Dropbox. ^{[11][13]}

“Lazarus Group” APT grubunun kullandığı bazı yazılımlar aşağıdaki resimde görüldüğü gibi “Techniques” sütunu altında listelenmektedir:

Software

ID	Name	References	Techniques
S0584	AppleJeus	^[11]	Abuse Elevation Control Mechanism: Bypass User Account Control, Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: Unix Shell, Create or Modify System Process: Windows Service, Create or Modify System Process: Launch Daemon, Deobfuscate/Decode Files or Information, Event Triggered Execution: Installer Packages, Exfiltration Over C2 Channel, Hide Artifacts: Hidden Files and Directories, Indicator Removal: File Deletion, Obfuscated Files or Information, Phishing: Spearphishing Link, Scheduled Task/Job: Scheduled Task, Subvert Trust Controls: Code Signing, System Binary Proxy Execution: Msiexec, System Information Discovery, System Services: Launchctl, User Execution: Malicious Link, User Execution: Malicious File, Virtualization/Sandbox Evasion: Time Based Evasion
S0347	AuditCred	^[33]	Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, File and Directory Discovery, Indicator Removal: File Deletion, Ingress Tool Transfer, Obfuscated Files or Information, Process Injection, Proxy

Software

Yazılımlar, dijital sistemlerde çalışmak üzere geliştirilen programlardır. MITRE ATT&CK Framework’ün yazılım bölümünde, APT grupları tarafından kullanılan yazılımlar bulunur.

Her yazılımın benzersiz bir kimliği (ID), adı ve açıklaması bulunur. Örneğin, aşağıdaki görüntü, yazılımın ID’sini, adını ve açıklamasını göstermektedir:

ID	Name	Associated Software	Description
S0066	3PARA RAT		3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda.
S0065	4H RAT		4H RAT is malware that has been used by Putter Panda since at least 2007.

Yazılım hakkında detaylı bilgilere ulaşmak için yazılım adına tıklayabilir ve ilgili yazılım sayfasına erişebilirsiniz. Örneğin, “3PARA RAT” yazılımının sayfası aşağıdaki görüntüde gösterilmiştir:

[Home](#) > [Software](#) > 3PARA RAT

3PARA RAT

3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda.
[1]

ID: S0066

① Type: MALWARE

① Platforms: Windows

Version: 1.1

Created: 31 May 2017

Last Modified: 30 March 2020

[Version Permalink](#)

Techniques Used

ATT&CK® Navigator Layers ▾

Domain	ID	Name	Use
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	3PARA RAT uses HTTP for command and control. ^[1]
Enterprise	T1573	.001 Encrypted Channel: Symmetric	3PARA RAT command and control commands are encrypted within the HTTP C2 channel using the DES algorithm in CBC mode with a key derived from the MD5 hash of the string

Yukarıdaki görüntü, “3PARA RAT” yazılımı hakkında detaylı bilgiler içeren sayfayı göstermektedir. Bu sayfadaki bilgiler, yazılımın hangi teknikleri kullandığını ve hangi APT grubunun bu yazılımı kullandığını içerir.

MITRE ATT&CK Framework’e birçok yazılım dahil edilmiş olup, isimler/ID’ler/Açıklamalar zaman içinde sürekli güncellenir ve yeni eklenen yazılımlarla birlikte artar. Bu eğitimin hazırlandığı dönemdeki yazılım sayısı aşağıdaki gibidir:

Software: 718

Mevcut yazılım sayısını aşağıdaki bağlantıyı kontrol ederek görebilirsiniz:

<https://attack.mitre.org/software/>

Bu siteyi ziyaret ettiğinizde, sayfanın sol tarafında aşağıdaki görüntüdeki gibi bir menü göreceksiniz, Bu menü aracılığıyla listelenen yazılımlar hakkında detaylı bilgilere sahip olabilirsiniz.

SOFTWARE

Overview

3PARA RAT

4H RAT

AADInternals

ABK

ACAD/Medre.A

Action RAT

adbupd

AdFind

Adups

ADVSTORESHELL

Agent Smith

Agent Tesla

Agent.btz

Allwinner

By [Doğukan Kaya](#) on [May 25, 2023](#).

[Canonical link](#)

Exported from [Medium](#) on June 1, 2023.