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'ın 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 diğer olası saldırılar hakkında araştırmalar yapılarak, onları tespit etme veya önleme yolları geliştirilebilir.

Matrix

MITRE ATT&CK Matrix Nedir?

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

Matris Türleri

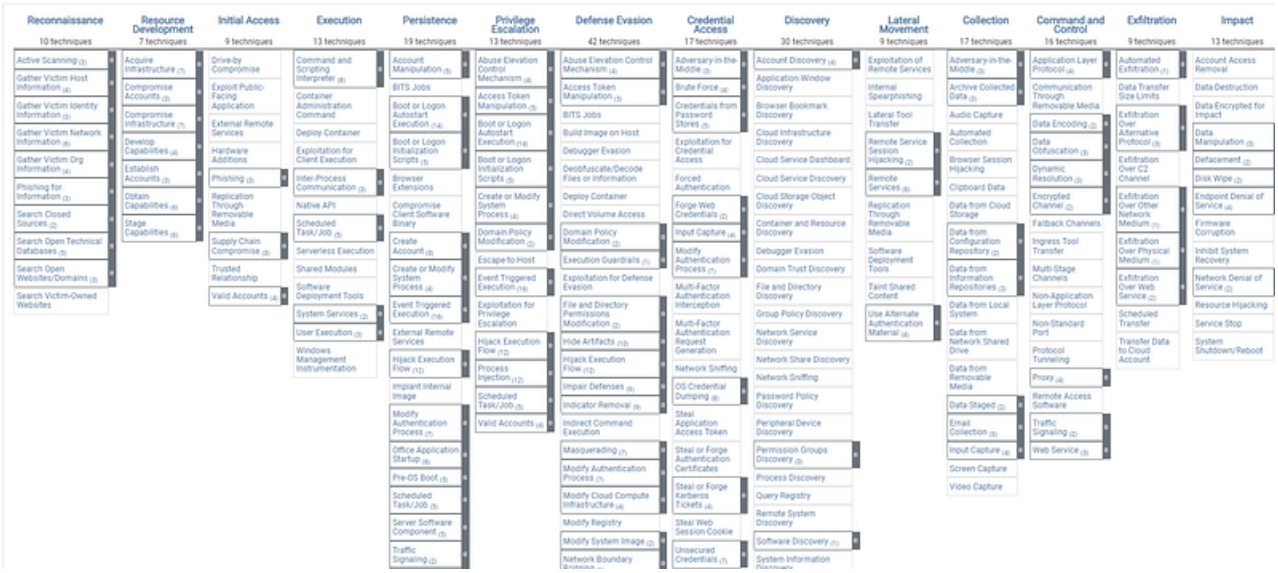
MITRE ATT&CK Çerçevesi içinde platform türlerine göre 3 farklı matris oluşturulmuştur:

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, diğer matrislere dahil edilenden daha fazla dijital sistem içermekte ve daha yaygın kullanılmaktadır, bu nedenle diğer matrislere göre bu matriste daha fazla bilgi bulunmaktadır. Kurumsal matris genellikle büyük organizasyonlara yönelik siber saldırıları anlamak için kullanılır.

Aşağıdaki görüntü, kurumsal matrisi detaylı olarak göstermektedir:



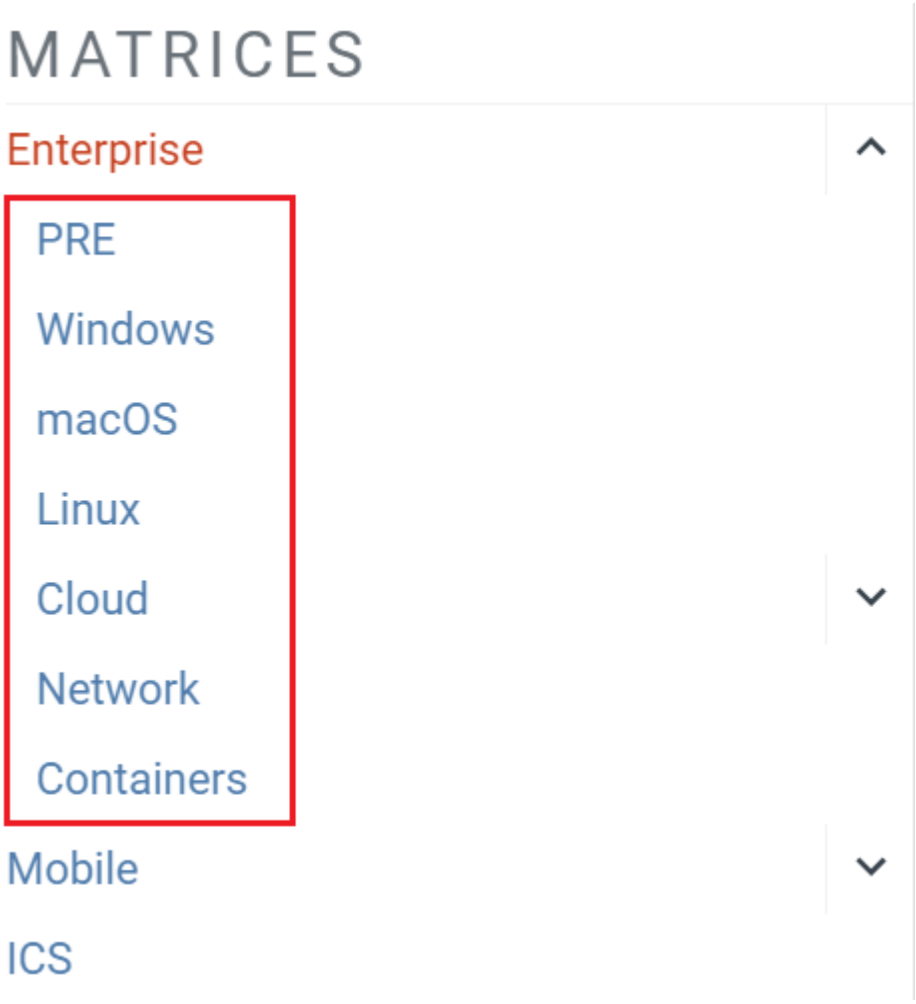
Enterprise Matrix

Enterprise Matris'in altında 7 adet alt matris bulunmaktadır:

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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:

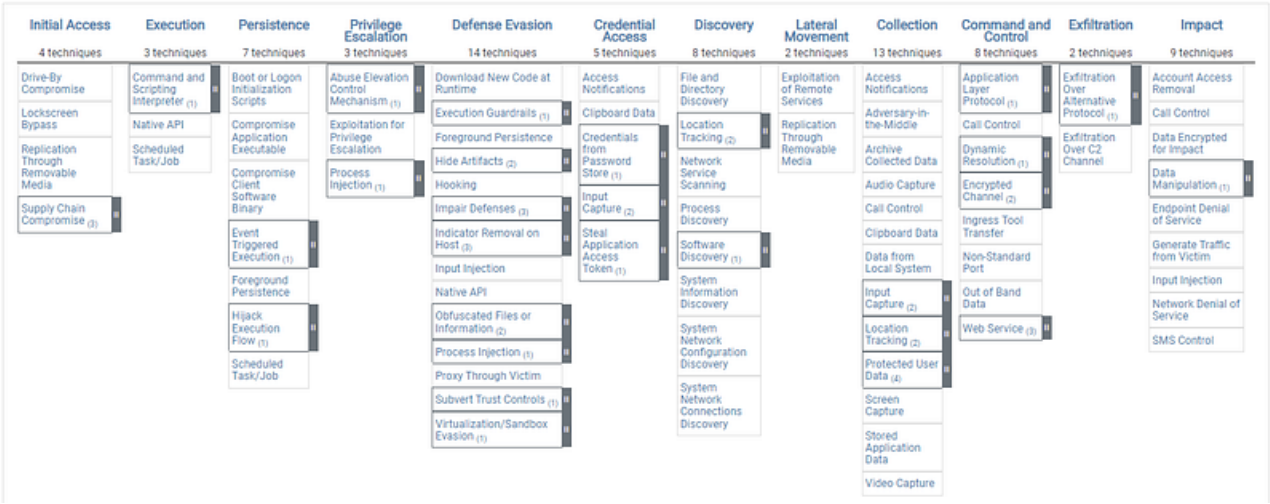
Enterprise Matris: https://attack.mitre.org/matrices/enterprise/



Mobil Matris

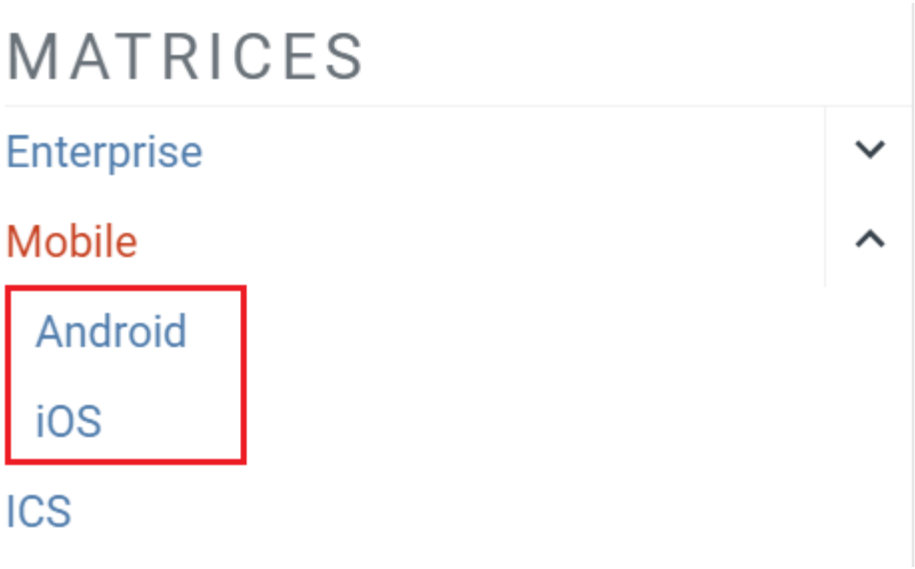
Mobil matris, mobil cihazlar için hazırlanan ve mobil cihazların siber güvenliği hakkında bilgi içeren bir matristir. Bu matris, bireysel ve kurumsal mobil cihazların güvenliğini sağlamak için kullanılabilir. Kurumsal Matris ile karşılaştırıldığında, daha az bilgi içermektedir.

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



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.



ICS Matrix

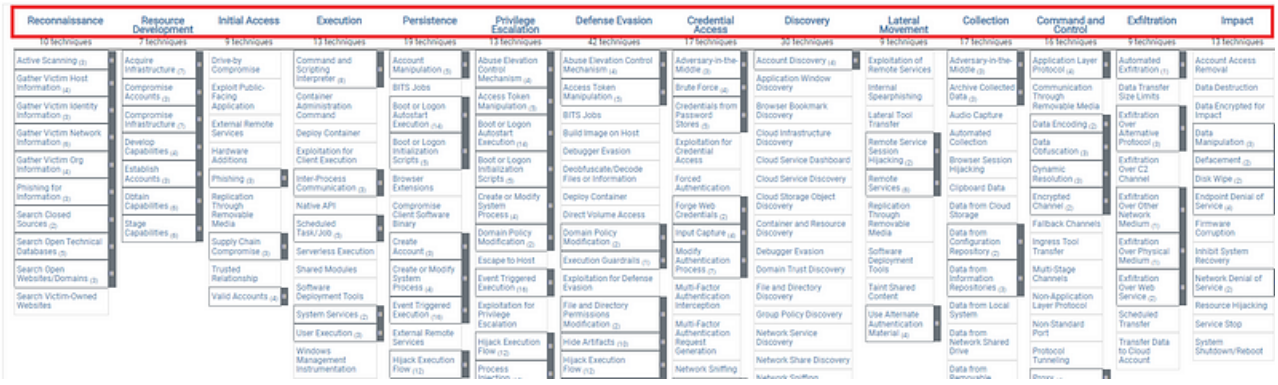
ICS Matrix, endüstriyel kontrol sistemlerindeki cihazların siber güvenliği için toplanan bilgileri içeren matristir. Bu matris, bir ICS'nin siber güvenliğini sağlamak ve analiz etmek için kullanılabilir.

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

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.

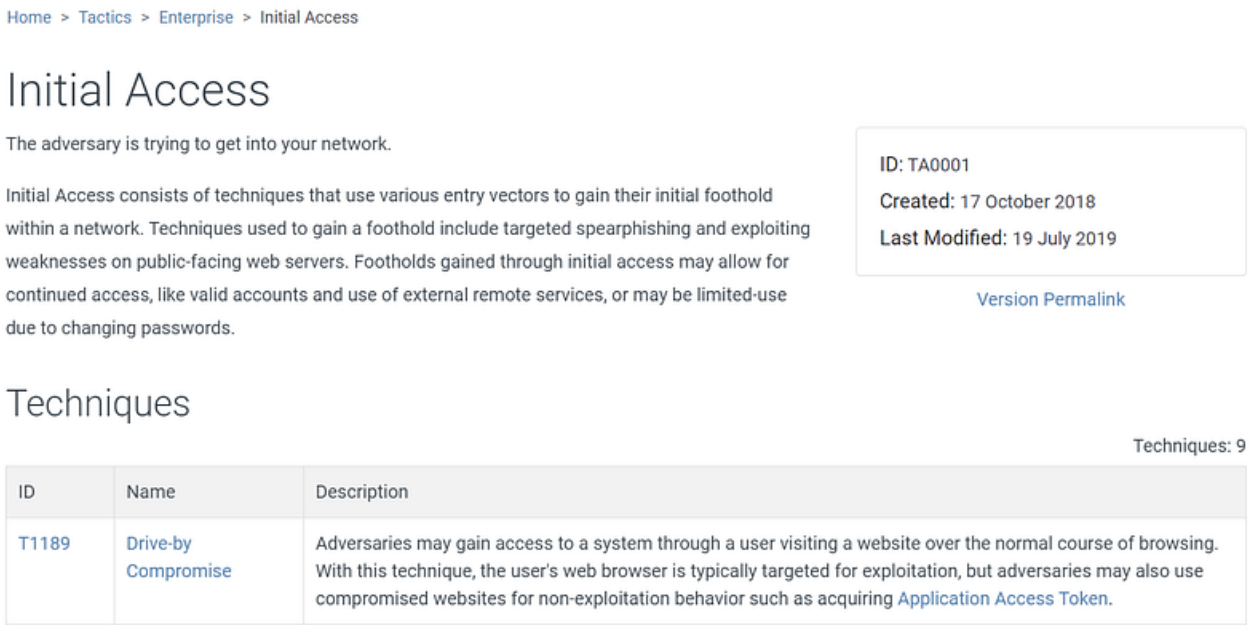
Örnek olarak, kurumsal matristeki taktikler aşağıdaki görüntüde gösterilmektedir:



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.

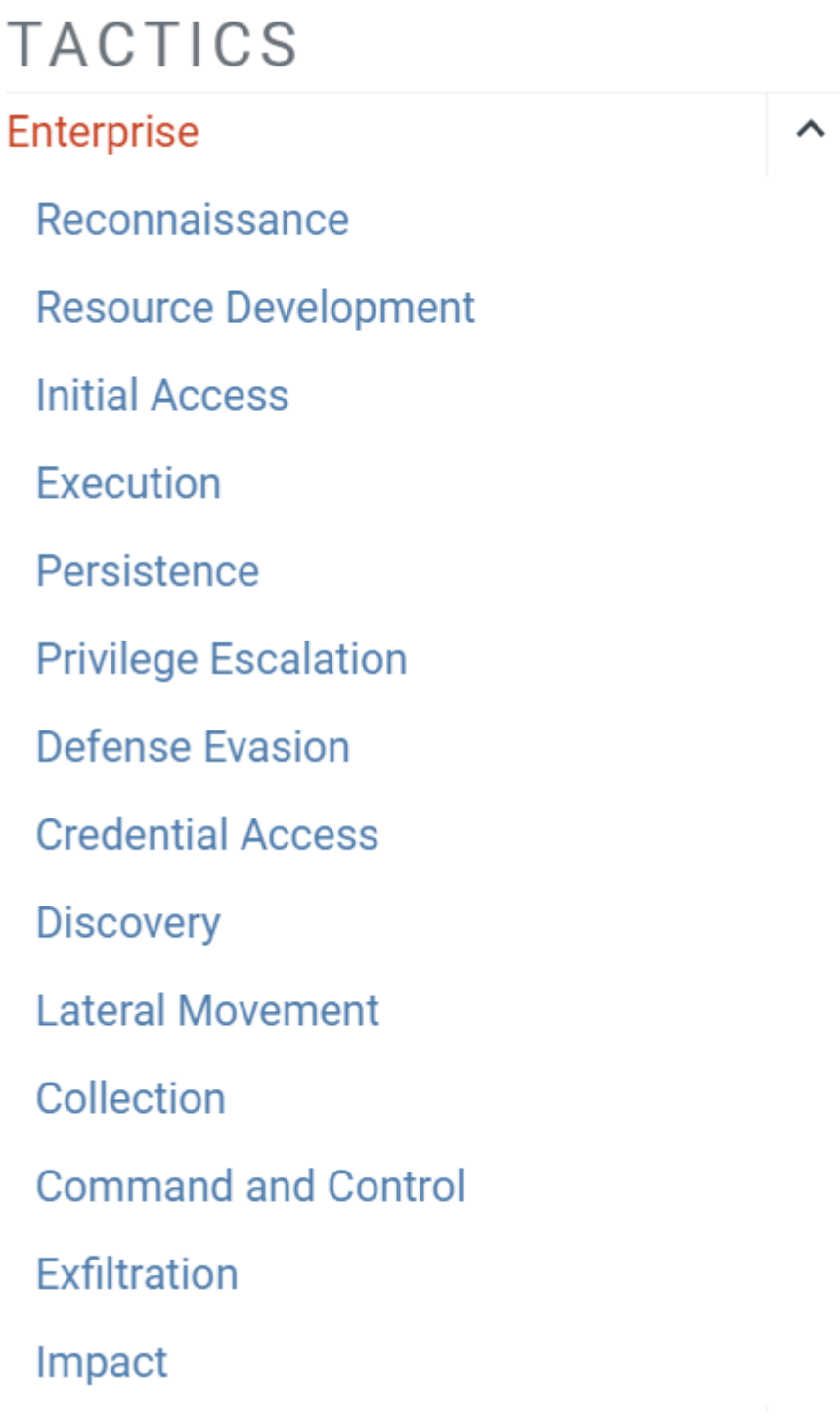
Enterprise Taktikleri

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	Privilige 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.



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	Privilige 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	aldırgan, uzaktan hizmetleri kullanarak cihazı kontrol etmeye veya izlemeye çalışıyor.

TACTICS

Mobile

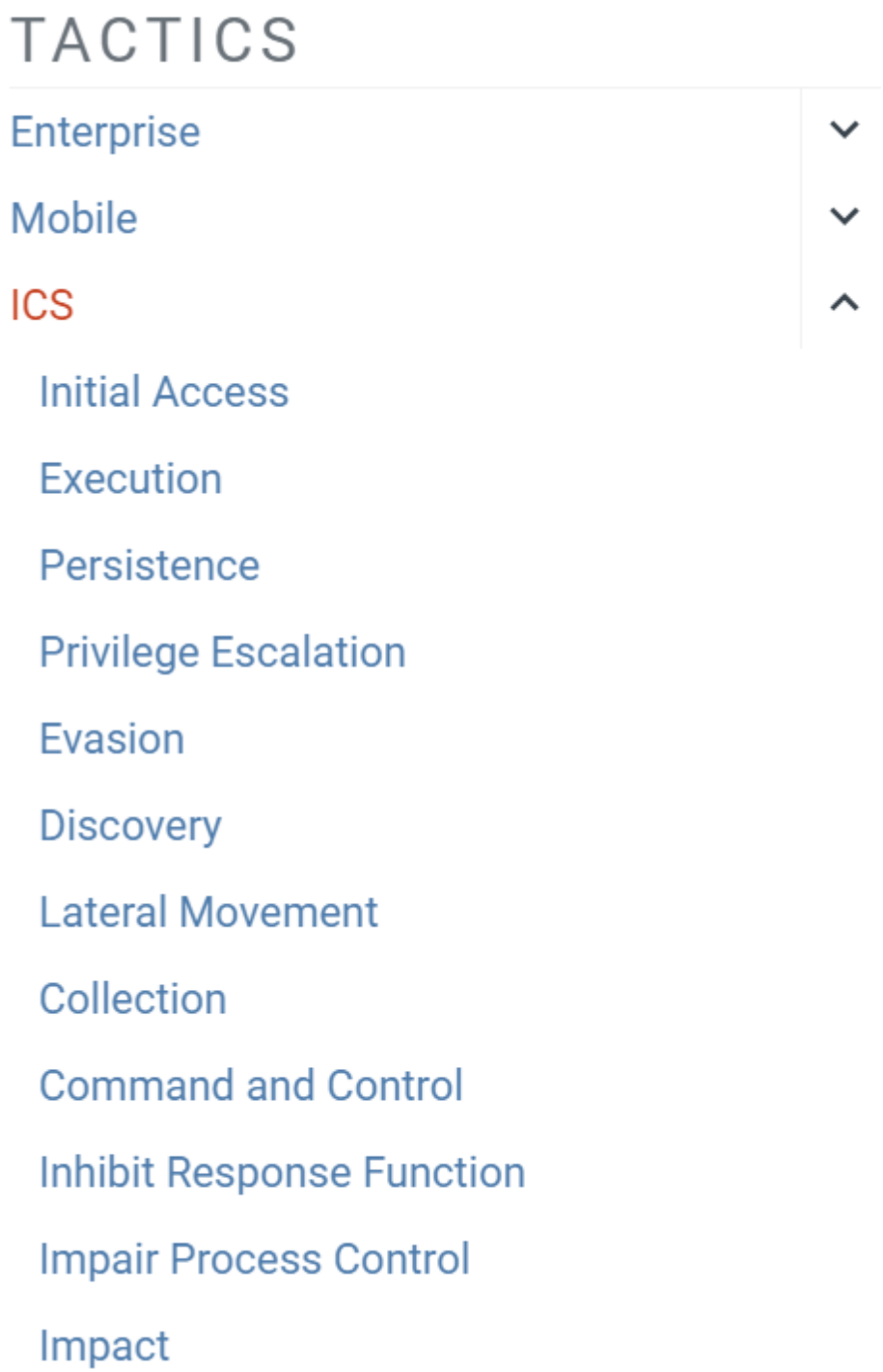
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact
- Network Effects
- Remote Service Effects

ICS Taktikleri

Aşağıdaki listede 12 farklı taktik sıralanmıştır.

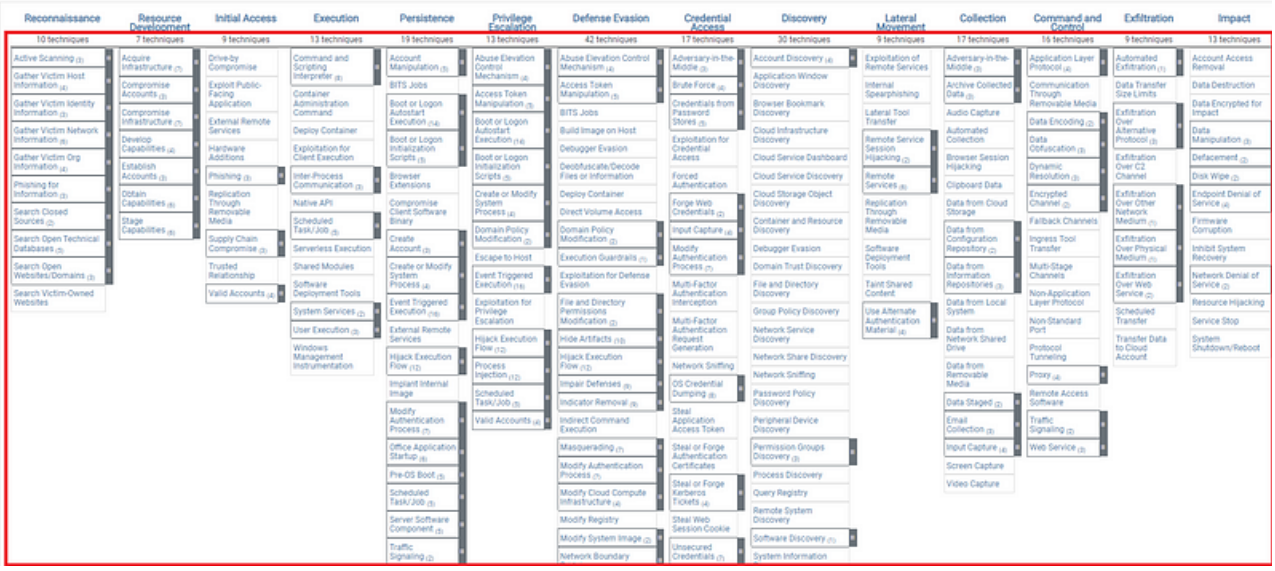
ICS Tactics: https://attack.mitre.org/tactics/ics/

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 ortamınızdaki yerini korumaya çalışıyor.
TA0111	Privilige Escalation	Saldırgan, daha yüksek düzeyde izinler elde etmeye çalışıyor.
TA0103	Evation	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 çevrelerini manipüle etmeye, kesintiye uğratmaya veya yok etmeye çalışıyor.



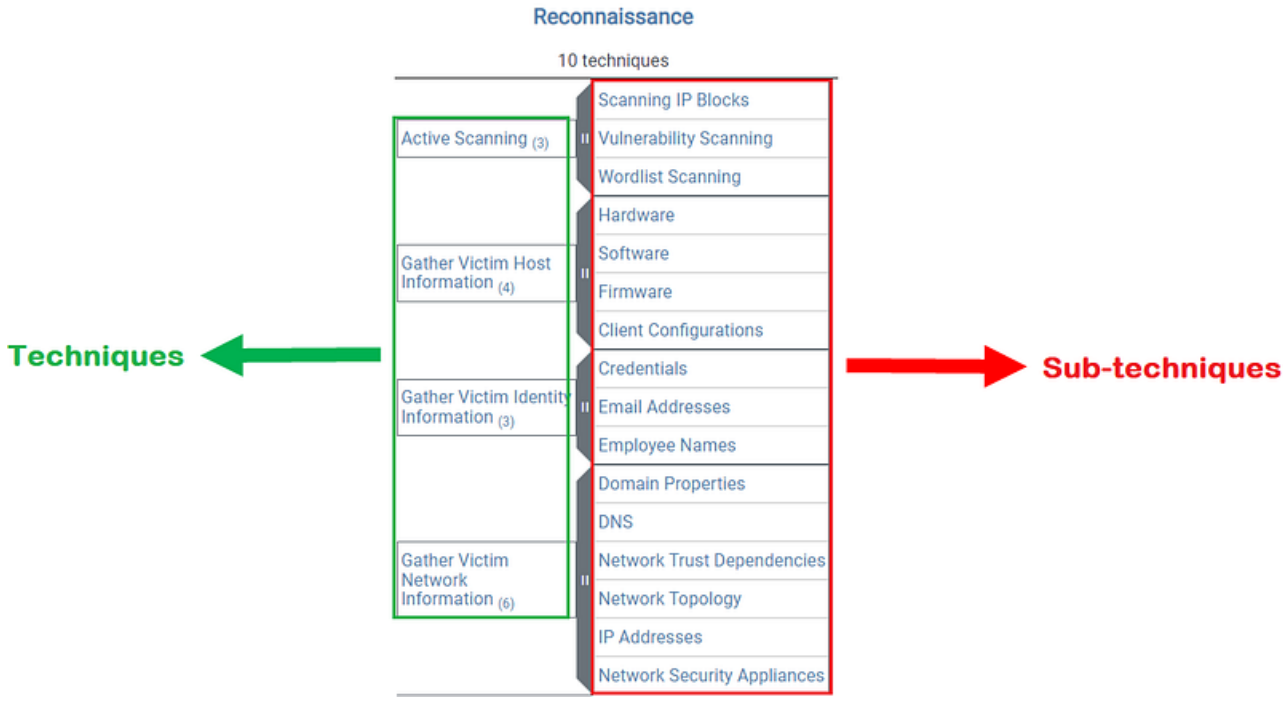
Techniques and Sub-Techniques (Teknikler ve Alt Teknikler)

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:



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

Yukarıdaki resimde gösterildiği gibi, matriste tekniklerin adlarının yazılı 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.

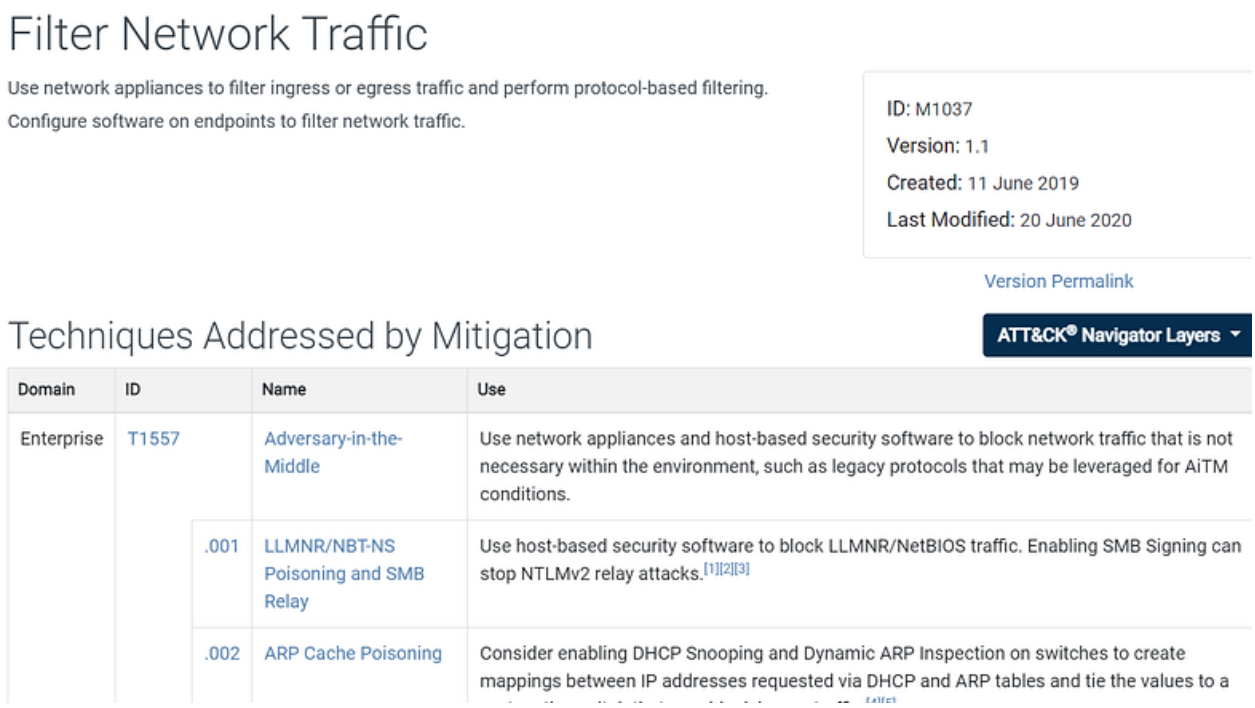
Prosedürlere tekniklerin bulunduğu sayfa üzerinden de erişilebilir.

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

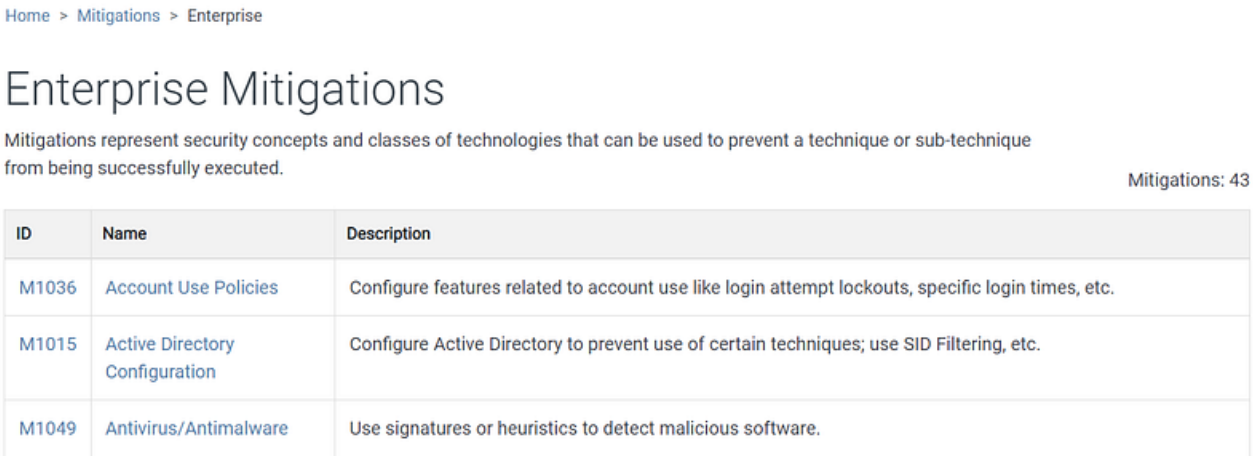
ATT&CK® Navigator Layers

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**



Home > Mitigations > Enterprise

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

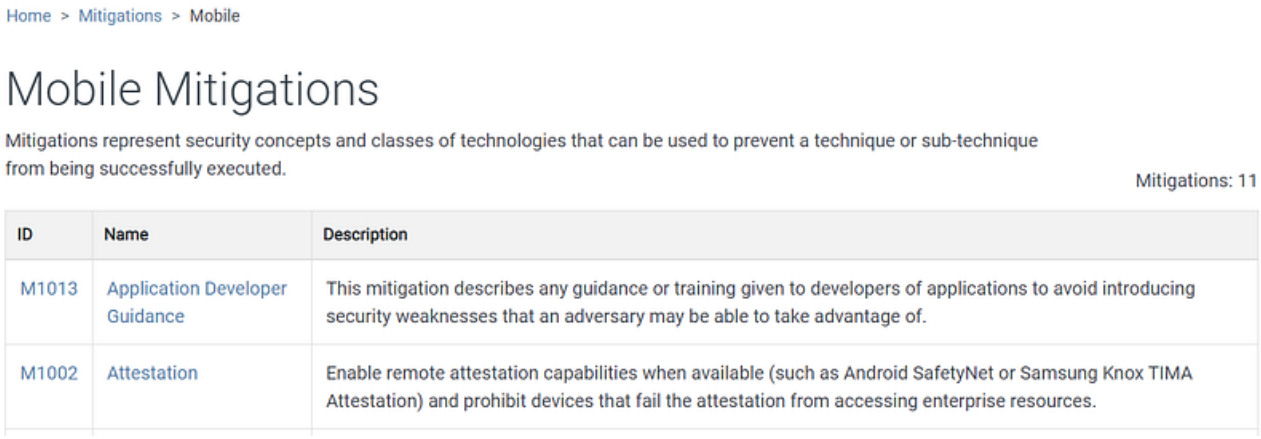
ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use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



Home > Mitigations > Mobile

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.

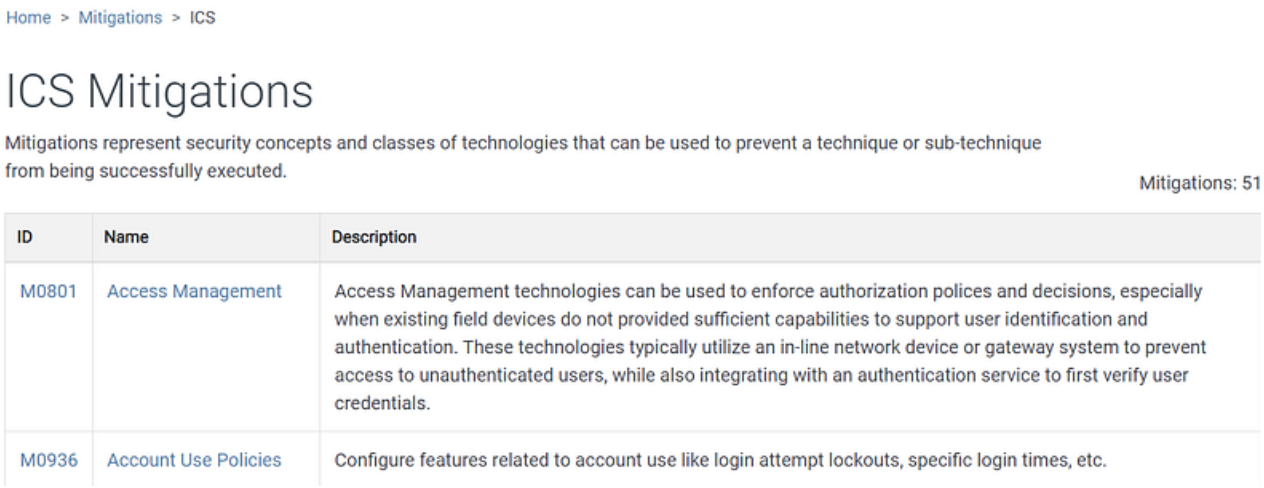
Bu tarihte güncel olarak mobil mitigasyonlarının sayısı aşağıdaki gibidir:

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 polices and decisions, especially when existing field devices do not provided 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.

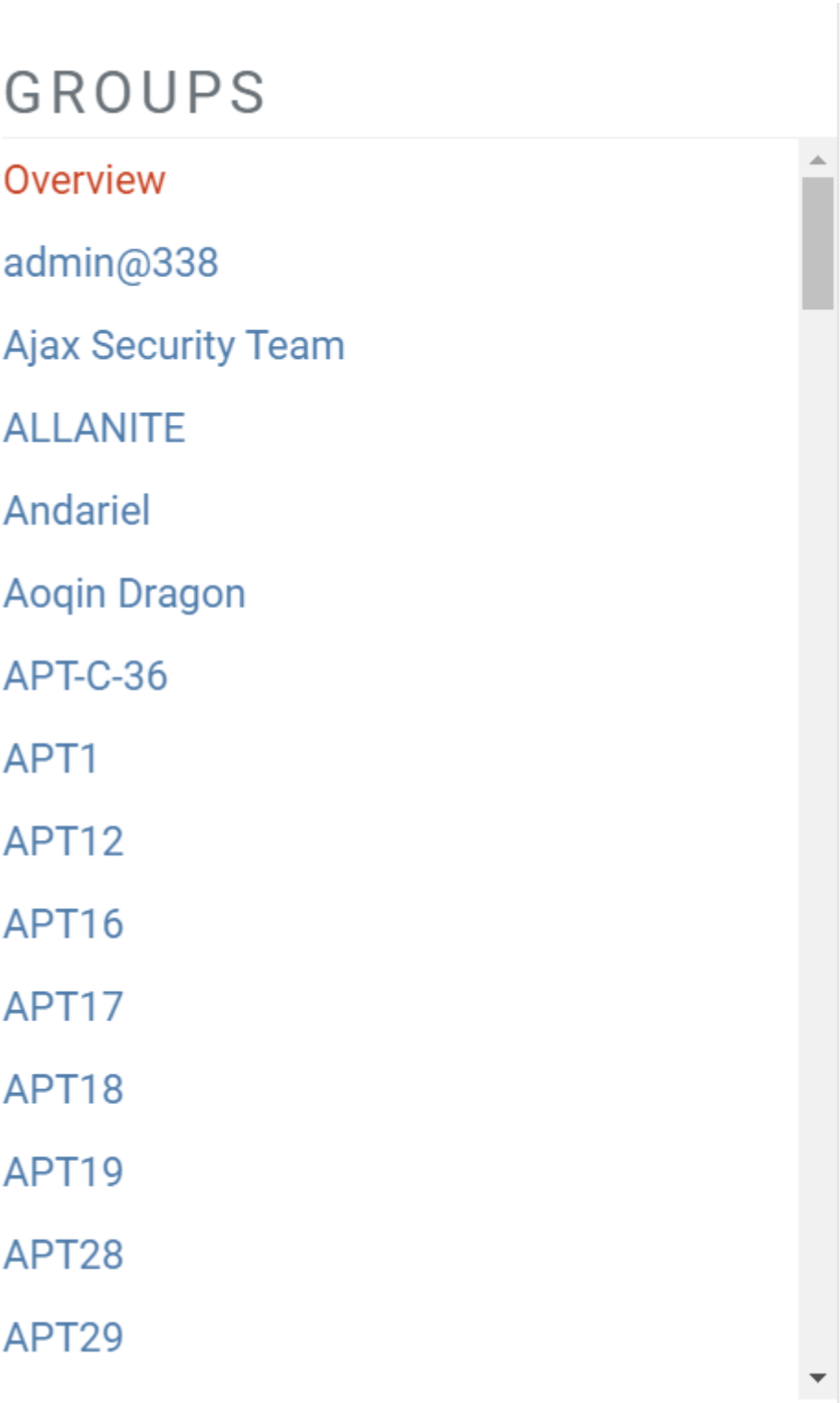
MITRE ATT&CK Framework içerisinde APT gruplarıyla ilgili bilgiler toplanır ve hangi APT grubunun hangi sistemlere yönelik hedef aldığı ve hangi siber saldırı tekniklerini uyguladığı belirlenmeye yardımcı olur.

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

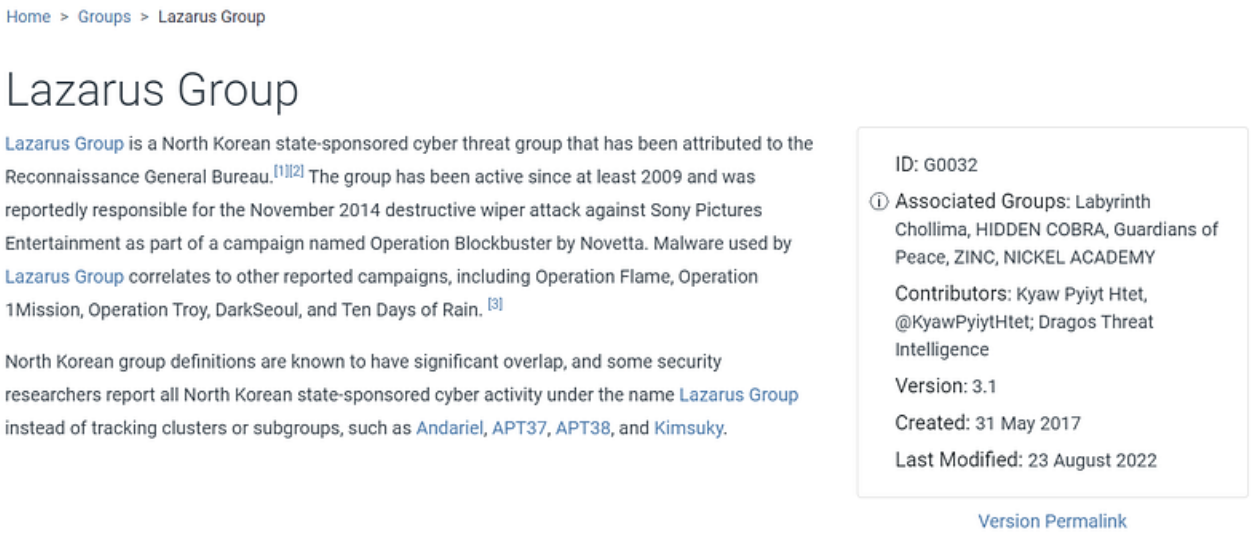
Gruplar: 135

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:



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



Grup Adı: Lazarus Group

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

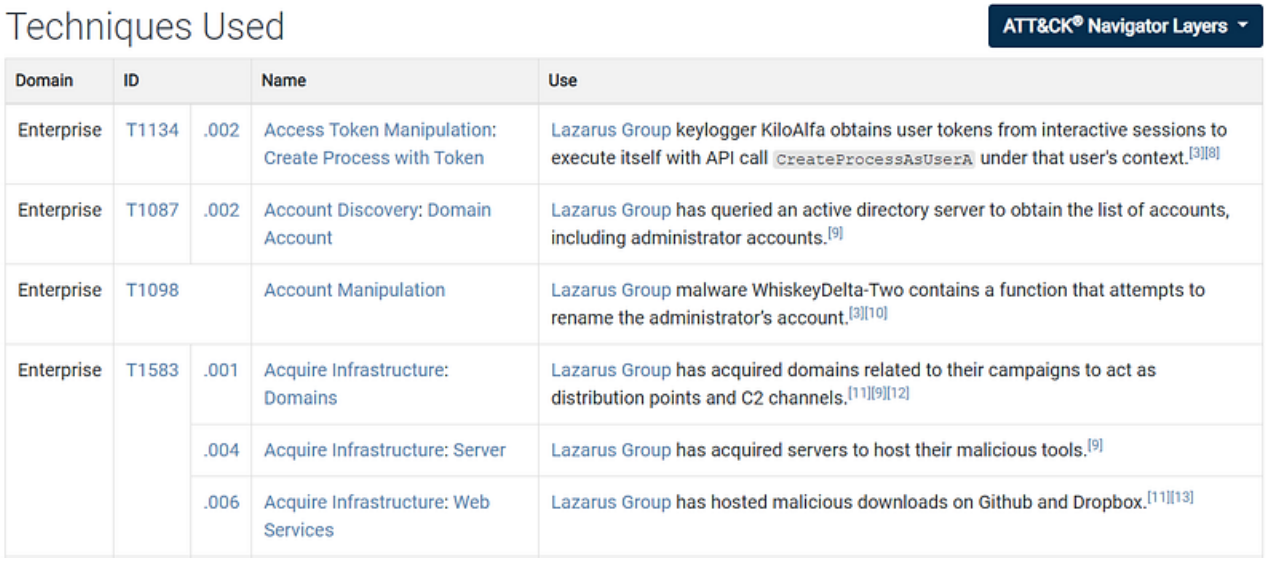
Açıklama: Lazarus Group, Kuzey Kore ile ilişkilendirilen bir APT grubudur. Finansal hırsızlık, casusluk ve siber sabotaj gibi çeşitli amaçlarla faaliyet gösterir. Grup, banka hırsızlıkları, fidye yazılımları saldırıları ve cryptocurrency hırsızlığı gibi çeşitli saldırılar gerçekleştirmiştir.

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.

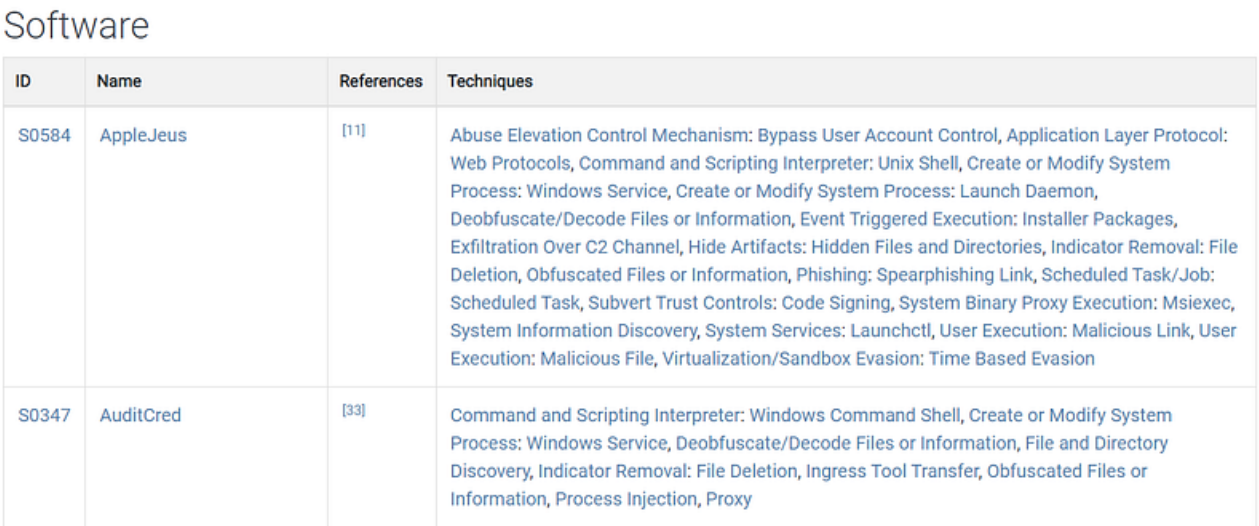


Techniques Used

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 `CreateProcessAsUserA` 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

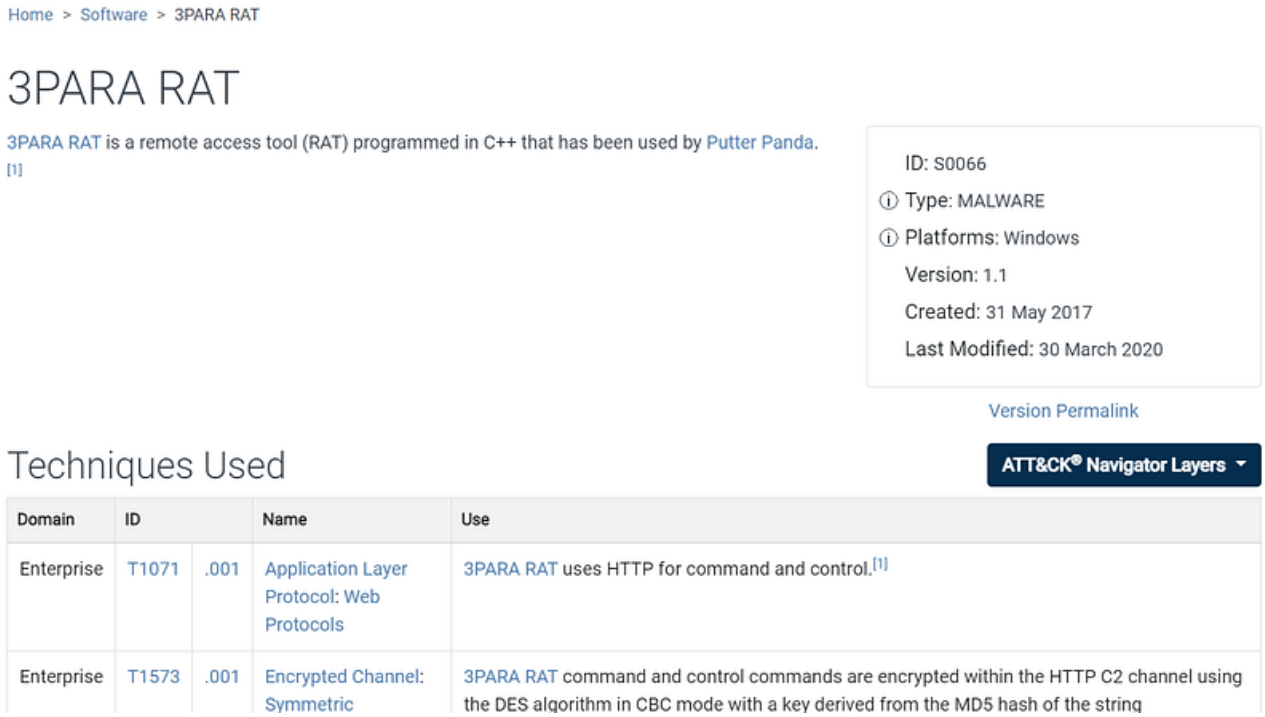
Software

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:



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.

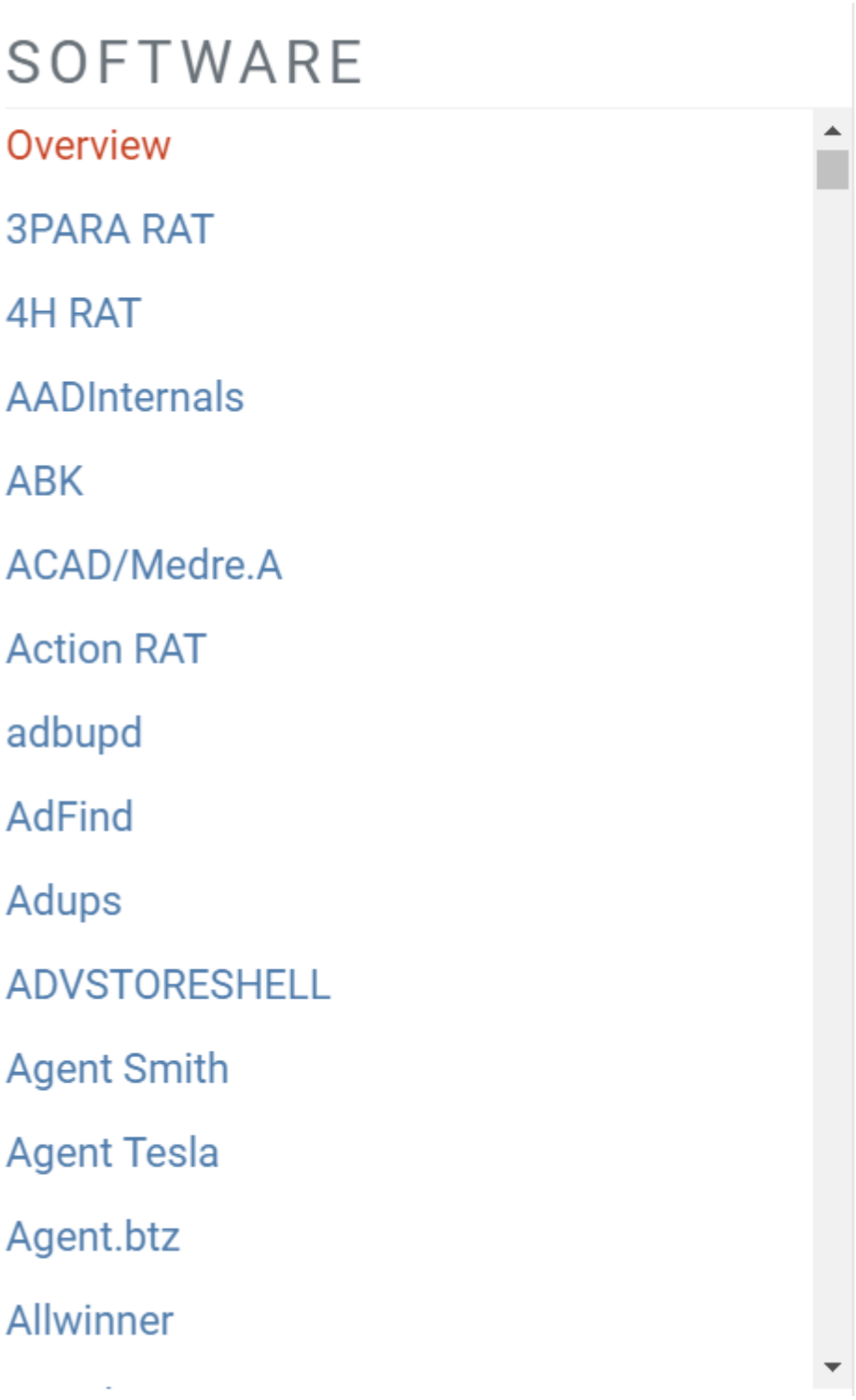
MITRE ATT&CK Framework’e birçok yazılım dahil edilmiş olup, isimler/ID’ler/Açıklamalar zaman içinde sürekli güncellenir ve yeni eklenen yazılımlarla birlikte artar. Bu eğitimin hazırlandığı dönemdeki yazılım sayısı aşağıdaki gibidir:

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.



By Doğukan Kaya on May 25, 2023.

Canonical link

Exported from Medium on June 1, 2023.