MITRE ATT&CK FRAMEWORK

Rabia EKŞİ
17.02.2025

İçindekiler

GİRİŞ

Siber güvenlik, günümüzün dijital dünyasında giderek daha fazla önem kazanmaktadır. Tehdit aktörleri, gelişmiş teknikler ve taktikler kullanarak kurumların altyapılarına sızmakta ve büyük zararlara yol açmaktadır. Bu bağlamda, Mitre ATT&CK Framework, saldırganların davranışlarını ve saldırı tekniklerini anlamak, bu tehditlere karşı savunma stratejilerini geliştirmek için kritik bir araçtır. Bunun yanı sıra, "Pyramid of Pain" modeli, bir saldırının ne kadar etkili olabileceğini veya savunmanın ne kadar zor olabileceğini anlamaya yönelik güçlü bir araçtır. Bu model, tehdit aktörlerinin kullandığı araçların, tekniklerin ve altyapıların değiştirilebilme düzeyine bağlı olarak bir savunma stratejisinin ne kadar güçlü olduğunu gösterir. Yüksek seviyedeki tehditlerin veya saldırıların tespit edilmesi ve engellenmesi daha zorken, bu seviyeye yakın olan tehditler daha kolayca savunulabilir hale gelir. Pyramid of Pain, siber güvenlik uzmanlarının doğru stratejileri seçmeleri ve tehditleri ortadan kaldırmak için hangi seviyede müdahale etmeleri gerektiğini anlamalarına yardımcı olur.

Bu raporda, Mitre ATT&CK Framework'ün önemi, framework içindeki taktik ve tekniklerin nasıl kullanıldığı, TTP (Tactics, Techniques, Procedures) kavramı ve bu kavramın tehdit avcılığı ile güvenlik mühendisliği üzerine etkisi ve Pyramif Of Pain modelinin incelemesi ele alınacaktır. Ayrıca, 2022 Ukraine Electric Power Attack (C0034) örneği üzerinden saldırı teknikleri incelenecek ve bir saldırı senaryosu üzerinden Mitre ATT&CK tablosu oluşturulacaktır.

MITRE ATT&CK FRAMEWORK

Mitre Att&ck Framework Nedir ve Neden Önemlidir?

MITRE ATT&CK, tehdit aktörlerinin farklı saldırı tekniklerini sistematik bir şekilde açıklayan ve sınıflandıran bir çerçevedir. Çerçeve, saldırganların bir hedefe nasıl saldırdıklarını ve her aşamada hangi teknikleri kullandıklarını anlamaya yönelik kapsamlı bilgiler sunar. Bu çerçeve, genellikle aşağıdaki temel öğelere dayanır:

- **Taktikler**: Saldırganın hedeflerine ulaşırken kullandığı genel hedeflerdir. Bir saldırganın saldırı amacına göre seçtiği adımların bir yol haritasıdır. Taktikler, saldırının hangi aşamasında olduğumuzu anlamamıza yardımcı olur.
- **Teknikler**: Taktiklerin uygulanma yollarıdır. Teknikler, belirli bir hedefe ulaşmak için kullanılan pratik adımları ifade eder. Örneğin, "Hedef Sisteme Erişim Sağlama" (Initial Access) taktiği altında "Phishing" gibi bir teknik yer alabilir.
- **Alt Teknikler**: Tekniklerin daha detaylı alt başlıklarıdır ve daha spesifik saldırı yöntemlerini tanımlar.

MITRE ATT&CK, siber güvenlik uzmanlarının savunma stratejilerini ve saldırı tespit sistemlerini (IDS, IPS, SIEM) iyileştirmelerine yardımcı olmak için kullanılır. Öneminden bahsedecek olursak:

- **Saldırıları Anlamak ve Analiz Etmek**: ATT&CK çerçevesi, saldırganların nasıl hareket ettiğini ve hangi yolları kullandığını anlamamıza yardımcı olur. Bu, savunma stratejilerinin oluşturulmasında önemli bir adımdır.

- **Savunma Stratejileri Geliştirmek**: Saldırganların tekniklerini ve taktiklerini bilmek, savunma ekiplerine hangi önlemleri alacaklarını ve nasıl tepki vereceklerini öğretir. Saldırılarla ilgili bilgi, güvenlik duvarları, antivirüs yazılımları ve izleme araçları gibi sistemlerin daha etkili hale gelmesini sağlar.
- **Saldırı Tespit ve Yanıt**: ATT&CK, saldırıların tespit edilmesi ve engellenmesi için faydalıdır. Güvenlik araçları bu çerçeveye dayanarak saldırıların izlerini arar ve uyarılar üretir. Bu, organizasyonların potansiyel tehditleri hızlı bir şekilde tanımasına yardımcı olur.
- **Red Team ve Blue Team Çalışmaları**: Red Team (saldırı testleri) ve Blue Team (savunma) ekipleri, ATT&CK çerçevesini kullanarak saldırı senaryoları oluşturabilir ve bu senaryolar üzerinde testler yapabilirler. Bu, her iki tarafın da yeteneklerini geliştirmelerine yardımcı olur.
- **Güncel Tehditlere Uyum Sağlama**: Saldırganlar sürekli olarak yeni teknikler ve taktikler geliştirir. ATT&CK çerçevesi, bu gelişmeleri takip eder ve güncellemeler sağlar, böylece güvenlik profesyonelleri her zaman en son tehditlere karşı korunabilirler.

Taktiklerin ve Tekniklerin Önemi

Taktikler: Saldırganların genel amaçlarını belirler. Bir saldırganın hangi aşamada olduğunu anlamak, savunma stratejisinin ne zaman ve nasıl devreye girmesi gerektiğini belirler. Örneğin, saldırgan "Persistence" (kalıcılık) sağlamak istiyorsa, bu onun sistemde daha uzun süre kalmayı amaçladığını gösterir. Bu aşamada kullanılan teknikler, saldırıyı durdurmak için önemlidir.

Teknikler: Saldırganların bu taktikleri uygularken kullandığı spesifik adımlar ve araçlardır. Teknikler, savunma ekiplerinin hangi araçlarla ve yöntemlerle karşılaştığını anlamalarını sağlar. Tekniklerin ne olduğunu bilmek, bu tekniklere karşı nasıl bir önlem alınacağına karar vermede kritik bir rol oynar. Örneğin, "Credential Dumping" tekniği altında, saldırganlar kimlik bilgilerini elde etmek için çeşitli araçlar kullanabilirler. Bu teknik, savunmanın şifreleme, kimlik doğrulama ve erişim denetimi gibi önlemler almasını gerektirir.

TTP Nedir?

TTP, "Tactics, Techniques, and Procedures" (Taktikler, Teknikler ve Prosedürler) ifadesinin kısaltmasıdır ve siber güvenlikte, özellikle tehdit aktörlerinin davranışlarını anlamak ve bu davranışları tespit etmek için kullanılan önemli bir kavramdır. TTP, bir saldırganın hedefe ulaşma yolundaki adımlarını tanımlar. Bu terimler şu şekilde açıklanabilir:

- **Taktikler (Tactics)**: Saldırganın saldırı amacı doğrultusunda kullandığı genel stratejilerdir. Bu, saldırganın siber saldırı sırasında başarmak istediği genel hedefleri ifade eder. Örneğin, hedef sistemde kalıcılık sağlamak, kimlik bilgilerini ele geçirmek, veri çalmak gibi hedefler birer taktiktir.

- **Teknikler (Techniques)**: Saldırganın taktikleri gerçekleştirmek için kullandığı belirli yöntemlerdir. Teknikler, daha somut ve spesifik adımlardır. Örneğin, **phishing (oltalama)**, **credential dumping (kimlik bilgilerini sızdırma)** veya **RAT (uzak erişim**

aracı) kullanma gibi teknikler, belirli taktikleri gerçekleştirmek için kullanılan yollardır.

- **Prosedürler (Procedures)**: Saldırganların belirli bir teknikle veya taktikle ilgili uyguladıkları somut adımlardır. Bu, saldırganın kullandığı araçlar, kullanılan kodlar ve saldırıların belirli bir yapıda nasıl gerçekleştirildiğini kapsar. Prosedürler, saldırıların "tekrarlanabilir" ve "standardize" hale gelmesini sağlayan belirli yolları içerir.
  TTP, MITRE ATT&CK çerçevesinde önemli bir yer tutar ve tehdit gruplarının davranışlarını modellemeye yönelik kapsamlı bilgiler sağlar. Bu sayede güvenlik ekipleri, saldırganların nasıl hareket ettiklerini ve hangi teknikleri kullandıklarını daha iyi anlayabilir.

TTP-Based Threat Hunting ve Detection Engineering Nedir?

1. TTP-Based Threat Hunting

TTP-Based Threat Hunting (TTP Tabanlı Tehdit Avcılığı), güvenlik uzmanlarının, belirli TTP'leri kullanarak proaktif bir şekilde potansiyel tehditleri ve saldırganları tespit etmeye yönelik gerçekleştirdiği bir yaklaşımdır. Bu, yalnızca bilinen tehditlere karşı değil, aynı zamanda saldırganların yeni ve bilinmeyen davranışlarını da tespit etmeye yönelik bir yöntemdir. TTP tabanlı tehdit avcılığı, genellikle aşağıdaki adımlarla yapılır:

- **Taktiklerin ve Tekniklerin Tanımlanması**: Tehdit avcıları, MITRE ATT&CK veya benzeri kaynaklardan belirli TTP'leri alır ve bu TTP'lerin hedef organizasyona nasıl uygulanabileceğini düşünür. Örneğin, kimlik bilgisi sızdırma (credential dumping) gibi bir tekniği, şirketin ağında nasıl işletebileceğini inceleyebilirler.
- **Veri Kaynaklarının Kullanılması**: Tehdit avcıları, organizasyonun ağını izlemek için mevcut loglardan, ağ trafiğinden, sistem davranışlarından ve diğer güvenlik verilerinden yararlanır. Bu veriler, belirli bir TTP'yi uygulamaya çalışan bir saldırganı tespit etmek için kullanılır.
- **Anomali Tespiti ve Korelasyonu**: TTP tabanlı avcılık sırasında, avcılar anormal etkinlikleri veya saldırganların izlediği örüntüleri tespit eder. Bu süreç, genellikle saldırganın daha önceki davranışlarını analiz ederek, benzer saldırıları önceden tahmin etmeye yönelik yapılan bir tür arama sürecidir.
- **Hedef Odaklı Yaklaşım**: Bu avcılık, genellikle saldırganın belirli bir hedefi gerçekleştirmek için kullandığı adımları izleyerek, daha önce gerçekleşmiş veya potansiyel bir saldırıyı bulmayı amaçlar. Yani, saldırganın izlediği yolu takip ederek tehdidi daha hızlı bulmaya çalışır.

2. TTP-Based Detection Engineering

TTP-Based Detection Engineering (TTP Tabanlı Algılama Mühendisliği), tehditlerin tespiti için yapılan mühendislik çalışmalarını ifade eder. Bu yaklaşım, tehdit avcılığında elde edilen bulgulara dayanarak güvenlik sistemlerini yapılandırmayı ve saldırıların erken tespitini sağlamayı amaçlar. TTP tabanlı algılama mühendisliği genellikle aşağıdaki adımları içerir:

- **Algılama Kurallarının Tasarlanması**: Algılama mühendisleri, TTP'lere dayalı olarak algılama kuralları oluşturur. Bu kurallar, belirli TTP'leri gerçekleştiren saldırganların davranışlarını tespit etmeyi amaçlar. Örneğin, credential dumping tekniğine karşı, şüpheli işlem ve dosya erişim davranışlarını tespit edebilecek kurallar yazılabilir.

- **Veri Kaynaklarının Entegrasyonu**: Güvenlik araçlarının, genellikle ağ ve sistem düzeyindeki verileri toplayarak, belirli TTP'lere karşı uyumlu hale gelmesi sağlanır. Bu, doğru veri toplama ve bu veriler üzerinden analiz yapma sürecini içerir. Loglar, ağ trafiği, sistem olayları gibi veriler kullanılabilir.
- **İzleme ve Korelasyon**: TTP tabanlı algılama mühendisliği, izleme sistemlerini ve analiz araçlarını optimize etmeye çalışır. Örneğin, bir güvenlik bilgi ve olay yönetimi (SIEM) sistemi, farklı logları ve verileri birleştirerek belirli bir TTP'yi gerçekleştiren tehditleri korelasyonlayabilir.

- **Yanıt ve İyileştirme**: Algılama mühendisliği sürecinin sonunda, güvenlik ekipleri saldırıyı tespit ederse, yanıt stratejilerini geliştirir ve ihlali engellemek için müdahalede bulunurlar. Ayrıca, algılama algoritmaları sürekli olarak iyileştirilir.

2022 Ukraine Electric Power Attack C0034

2022 Ukraine Electric Power Attack, **Sandworm Team** (APT28 olarak da bilinir) tarafından gerçekleştirilen ve Ukrayna'nın elektrik altyapısını hedef alan büyük bir siber saldırıdır. Bu saldırı, kritik altyapılara yönelik en büyük siber saldırılardan biri olarak tarihe geçmiştir. Sandworm Team, daha önce de birçok hükümet ve enerji sektörüne yönelik saldırılar gerçekleştirmiştir, ancak 2022'deki bu saldırı, belirli taktikler ve araçlar kullanılarak gerçekleştirilen daha karmaşık bir operasyondu.

Saldırının Amacı ve Hedefi

Saldırının amacı, Ukrayna'nın elektrik altyapısına siber saldırı yaparak elektrik şebekesini devre dışı bırakmaktı. Elektrik şebekesinin kontrolünü ele geçirmek ve kritik veri hatlarını yok etmek, aynı zamanda siber savaşın bir aracı olarak kullanıldı. Saldırı, özellikle **SCADA** (Supervisory Control and Data Acquisition) sistemleri ve **OT** (Operational Technology) altyapısı hedef alındı. Bu tür sistemler, endüstriyel süreçleri izlemek ve kontrol etmek için kullanılır ve doğrudan elektrik dağıtım şebekesi gibi kritik altyapılara bağlıdır.

Kullanılan Taktikler, Teknikler ve Prosedürler (TTP)

Saldırganlar, bu saldırıda birçok **TTP (Tactics, Techniques, and Procedures)** kullanmışlardır. Bunlar arasında, **data destruction (T1485)**, **command and control tunneling (T1572)**, **web shell deployment (T1505)**, **group policy modification (T1484)** ve **scheduled task execution (T1053)** gibi teknikler bulunmaktadır. Bu tekniklerin kullanımı, saldırganların hedef altyapılara kalıcı olarak yerleşmelerine ve izlerini gizlemelerine yardımcı olmuştur. 2022 Ukraine Electric Power Attack (C0034) sırasında **Sandworm Team** tarafından kullanılan çeşitli teknikler ve bunların TID (Technique ID) değerleri aşağıda ayrıntılı olarak incelenmiştir:

1. T1059.001 - Command and Scripting Interpreter: PowerShell

- **Açıklama**: Sandworm Team, **PowerShell** komutlarını kullanarak TANKTRAP adlı bir aracı yaymak ve bir **wiper** (silici yazılım) çalıştırmak için **Windows Group Policy**'i kullandı. Bu teknik, hedef sistemlerde uzaktan komut çalıştırmak için PowerShell'in nasıl kullanılabileceğini gösterir.
- **Uygulama**: Hedef sistemlere PowerShell komutları kullanarak, özellikle SCADA sistemlerinin çalıştığı ortamda zararlı yazılımın yayılmasını sağladılar.

2. T1543.002 - Create or Modify System Process: Systemd Service

- **Açıklama**: Sandworm Team, **Systemd**'yi kullanarak **GOGETTER** adlı zararlı yazılımın kalıcılığını sağladı. Bu işlem, GOGETTER'ın her sistem başlatıldığında çalışmaya başlamasını sağlamak için **WantedBy=multi-user.target** konfigürasyonu kullanılarak yapıldı.
- **Uygulama**: GOGETTER'ın hedef sistemde arka planda sürekli çalışmasını sağlamak amacıyla Systemd servisi oluşturuldu.

3. T1485 - Data Destruction

- **Açıklama**: **CaddyWiper** adlı zararlı yazılım, hedefin IT altyapısındaki dosyaları silmek ve OT (Operational Technology) sistemleriyle ilişkili dosyaları yok etmek için kullanıldı. Ayrıca, harici sürücüler ve fiziksel disk bölümleri de silindi.
- **Uygulama**: CaddyWiper, kritik verileri yok ederek sisteme zarar verdi.

4. T1484.001 - Domain or Tenant Policy Modification: Group Policy Modification

- **Açıklama**: **Group Policy Objects (GPO)** kullanılarak hedef sistemlere zararlı yazılımlar dağıtıldı. GPO'lar, Windows ortamlarında yapılandırmaların merkezi olarak yönetilmesini sağlar ve saldırganlar bu yapılandırmalarla kötü amaçlı yazılımları yayabilir.
- **Uygulama**: GPO'lar aracılığıyla hedef sistemlerde CaddyWiper'ın yüklenmesi ve çalıştırılması sağlandı.

5. T1570 - Lateral Tool Transfer

- **Açıklama**: **Group Policy Object (GPO)** kullanarak **CaddyWiper**'ın **msserver.exe** adlı dosyasının bir staging sunucusundan hedef makinelerine kopyalanması sağlandı. Bu, zararlı yazılımın yayılmasını ve çalıştırılmasını sağlayan bir teknik olarak kullanıldı.
- **Uygulama**: GPO'lar aracılığıyla zararlı dosyanın sistemler arası yayılması sağlandı.

6. T1036.004 - Masquerading: Masquerade Task or Service

- **Açıklama**: Sandworm Team, **Systemd service** birimi kullanarak **GOGETTER** malware'ını, normalde meşru görünen bir servis gibi gizledi. Bu, güvenlik algılamalarını atlatmak için kullanılan yaygın bir taktiktir.
- **Uygulama**: GOGETTER zararlı yazılımı, sahte bir sistem servisi olarak gizlenerek, tespit edilmesi zor hale getirildi.

7. T1095 - Non-Application Layer Protocol

- **Açıklama**: **GOGETTER** C2 (Command and Control) iletişimini, **TLS tabanlı tünelleme** kullanarak gerçekleştirdi. Bu, zararlı yazılımın dışarıya veri sızdırmasını gizler.

- **Uygulama**: C2 kanalının şifreli olması, saldırganların kötü amaçlı yazılımlarını daha gizli tutmalarını sağladı.

8. T1572 - Protocol Tunneling
- **Açıklama**: **GOGETTER**'ın **Yamux** protokolünü kullanan bir **TLS tabanlı C2 kanalı** kurdu. Bu, iletişimin tünellenmesi ve ağ güvenlik cihazları tarafından tespit edilmesinin zorlaştırılması anlamına gelir.
- **Uygulama**: Bu teknik, saldırganların hedef sistemle olan iletişimini güvenli hale getirdi.

9. T1053.005 - Scheduled Task/Job: Scheduled Task
- **Açıklama**: **GPO** kullanılarak **CaddyWiper**'ın belirli bir zaman diliminde otomatik olarak çalışması için **Scheduled Task** (zamanlanmış görev) oluşturuldu. Bu görev, belirli bir zamanda malware'ın etkinleşmesini sağladı.
- **Uygulama**: CaddyWiper'ın bir zamanlanmış görevle, otomatik olarak yüklenmesi ve çalışması sağlandı.

10. T1505.003 - Server Software Component: Web Shell
- **Açıklama**: Sandworm Team, internet üzerinden erişilebilen bir sunucuya **Neo-REGEORG** adlı web shell'ini kurdu. Bu, hedef sunucu üzerinde uzaktan kontrol elde etmelerini sağladı.
- **Uygulama**: Web shell, saldırganların hedef sisteme uzaktan erişim sağlamalarına olanak tanıdı.

11. T0895 - Autorun Image
- **Açıklama**: Sandworm Team, **ISO görüntüsünü** bir **SCADA sunucusu** üzerinde çalıştırılacak şekilde yapılandırarak zararlı bir **VBS script**'ini otomatik olarak çalıştırdı. Bu, ISO görüntüsünü bir sanal makineye bağlayarak yapılmıştır.
- **Uygulama**: ISO görüntüsündeki zararlı yazılım, SCADA sistemine zarar vermek için çalıştırıldı.

12. T0807 - Command-Line Interface
- **Açıklama**: **MicroSCADA** platformunun **SCIL-API**'sını kullanarak, **scilc.exe** komut dosyasını çalıştırarak sistem üzerinde komutlar yürütüldü.
- **Uygulama**: SCADA sistemi üzerinde komut yürütme amacıyla **scilc.exe** kullanıldı.

13. T0853 - Scripting
- **Açıklama**: Sandworm Team, **Visual Basic** scripti **lun.vbs**'yi kullanarak **n.bat** dosyasını çalıştırdı. Ardından **scilc.exe** komut dosyasını çalıştırarak SCADA sistemine zarar verdi.
- **Uygulama**: **lun.vbs** ve **n.bat** zararlı betikleri, SCADA platformunun çalışmasına zarar vermek için kullanıldı.

14. T0894 - System Binary Proxy Execution
- **Açıklama**: **scilc.exe** binarisini kullanarak, **s1.txt** dosyasındaki önceden belirlenmiş SCADA komutları çalıştırıldı. Bu, SCADA sistemine yetkisiz komutlar göndermek için yapıldı.

- **Uygulama**: SCADA sistemi üzerinden istenmeyen komutlar göndermek için bu komut dosyası kullanıldı.

15. T0855 - Unauthorized Command Message

- **Açıklama**: Sandworm Team, **MicroSCADA SCIL-API** aracılığıyla, **substation cihazlarına** yetkisiz komutlar göndermek için SCADA talimatlarını belirledi.
- **Uygulama**: SCADA altyapısındaki cihazlara zarar vermek amacıyla yetkisiz komutlar gönderildi.

Kullanılan Yazılımlar:

- **S0693 - CaddyWiper**: Bu, hedefin dosyalarını yok etmek için kullanılan bir silici yazılımdır. SCADA sistemlerine zarar vermek amacıyla kullanıldı.

Bu saldırı, özellikle **SCADA sistemleri** üzerindeki zararlı yazılım ve tehdit tekniklerinin ne kadar güçlü ve tahrip edici olabileceğini gösteriyor. Sandworm Team, hedeflerine ciddi zararlar vermek için bir dizi sofistike teknik ve araç kullanmıştır.

Saldırı Senaryosu

İlk erişim vektörü olarak, phishing aracılığıyla hedefe gönderilen bir zip dosyası kullanılmıştır. Bu zip dosyasının içinde, zararlı bir JavaScript dosyası yer alır. Kullanıcı tarafından çalıştırıldığında, bu dosya IcedID adlı zararlı yazılımı indirip çalıştırmıştır. İlk olarak 2017 yılında tespit edilen IcedID, başlangıçta genel bir zararlı yazılım olarak kullanılsa da, son yıllarda fidye yazılımı aktörleri için bir "ilk erişim aracı" haline gelmiştir. IcedID, çalıştırıldıktan kısa bir süre sonra bazı temel keşif aktiviteleri gerçekleştirmiş, ancak sonrasında C2 sunucusuna düzenli olarak sinyal göndermek dışında herhangi bir faaliyet göstermemiştir. İki günlük bir bekleyişin ardından, saldırganlar IcedID aracılığıyla sisteme Cobalt Strike Beacon yükleyip çalıştırmıştır. Bu noktadan sonra saldırganlar, nltest.exe, whoami.exe ve net.exe gibi Windows yerel araçlarını kullanarak hedef sistemde ikinci bir keşif dalgası gerçekleştirmiş ve Cobalt Strike'ın "named pipe impersonation" (GetSystem) özelliğini kullanarak SYSTEM yetkilerini ele geçirmiştir. Saldırganlar, ağ içinde lateral hareket kabiliyeti kazanarak, SMB protokolü üzerinden Cobalt Strike Beacon dosyasını ağdaki diğer sistemlere taşımış ve çalıştırmıştır. Bu süreçte, bir domain controller üzerinden gerçekleştirilen port taramaları, SSH, SMB, MSSQL, RDP ve WinRM gibi hizmetleri hedeflemiştir. Kısa bir ara verdikten sonra saldırganlar, PsExec aracıyla ağdaki birçok sisteme Cobalt Strike Beacon DLL dosyasını kopyalamış ve çalıştırmıştır. Saldırının ilerleyen safhalarında, saldırganların RDP bağlantıları kurarak domain controller ve diğer sistemlere erişim sağladığı gözlemlenmiştir. Bu bağlantılar, IcedID tarafından işletilen bir proxy üzerinden yönlendirilerek 8080 numaralı port kullanılmıştır. Ayrıca, saldırganlar bir domain controller üzerinde yeni bir yerel kullanıcı hesabı oluşturmuş ve bu hesabı Administrator
grubuna ekleyerek kalıcılık sağlamıştır. Bununla birlikte, Windows Defender'ı devre dışı
bırakmak için grup politikalarını manipüle etmişlerdir. Saldırının son aşamasında, Cobalt Strike Beacons yardımıyla Conti fidye yazılımı bellek üzerinden tüm sistemlerde çalıştırılmıştır. Fidye yazılımı tüm sistemleri şifrelemiş ve kurbanlara bir fidye notu bırakmıştır. Saldırı sonrası yapılan incelemelerde, bir domain controller da dahil olmak üzere birçok sistemin erişilemez hale geldiği ve fidyenin ödense dahi bu sistemlerin geri yüklenemeyeceği anlaşılmıştır.

Kullanılan Taktik ve Teknikler

TAKTİK	TID	Açıklama
Initial Access	T1566.001 - Phishing: Spear Phishing Attachment	Hedef kullanıcılara zararlı içerik içeren bir zip dosyası gönderildi.
Initial Access	T1105 - Ingress Tool Transfer	Zararlı dosyalar, saldırgan kontrolündeki sunuculardan hedef sisteme indirildi.
Execution	T1203 - Exploitation for Client Execution	Zararlı dosyalar, kullanıcı etkileşimiyle çalıştırıldı.
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell	Saldırı senaryosunda kullanılan betikler PowerShell komutlarıyla oluşturuldu.
Execution	T1203 - Exploitation for Client Execution	Zararlı dosyalar ve DLL'ler hedef sisteme yüklendi.
Persistence	T1055 - Process Injection	Zararlı kodlar, sistemdeki çalıştırılabilir süreçlere enjekte edildi.
Persistence	T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder	Windows kayıt defterine yapılan düzenlemelerle zararlı yazılımlar her oturum açıldığında çalışacak şekilde ayarlandı.
Persistence	T1136.001 - Create Account: Local Account	Yeni kullanıcı hesapları oluşturularak kalıcı erişim sağlandı.
Persistence	T1078 - Valid Accounts	Sistemde mevcut kullanıcı kimlik bilgileri kullanılarak zararlı yazılımların çalıştırılması sağlandı.
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols	HTTP/HTTPS protokolleri üzerinden komuta ve kontrol iletişimi gerçekleştirildi.
Command and Control	T1105 - Ingress Tool Transfer	Zararlı yükler, komuta ve kontrol sunucularından hedef sistemlere aktarıldı.
Command and Control	T1090.001 - Proxy: Internal Proxy	RDP trafiği, IcedID süreci üzerinden saldırgan altyapısına yönlendirilerek izleme ve engelleme önlendi.
Discovery	T1482 - Domain Trust Discovery	nltest komutuyla domain ilişkileri ve güven ilişkileri sorgulandı.
Discovery	T1016 - System Network Configuration Discovery	ipconfig gibi komutlarla ağ konfigürasyonu keşfedildi.
Discovery	T1082 - System Information Discovery	Hedef sistemin işletim sistemi ve yapılandırmaları belirlendi.
Discovery	T1135 - Network Share Discovery	Ağ paylaşım noktaları ve erişilebilir kaynaklar belirlendi.

Defense Evasion	T1027- Obfuscated Files or Information	Kodlar, obfuscation teknikleriyle gizlenerek algılama önlendi.
Exfiltration	T1048.002 - Exfiltration Over Alternative Protocol: Exfiltration Over C2 Channel	Hassas veriler, Cobalt Strike yapılandırmaları üzerinden dış sunuculara aktarıldı.
Impact	T1486 - Data Encrypted for Impact	Sistemlerdeki dosyalar, Conti zararlısı ile şifrelenerek erişilemez hale getirildi.
Impact	T1490 - Inhibit System Recovery	Shadow Copy'ler silindi ve sistem kurtarma mekanizmaları devre dışı bırakıldı.

PYRAMID OF PAIN

MITRE'nin "Pyramid of Pain" (Ağrı Piramidi) modeli, siber savunma stratejilerinde daha etkin bir yaklaşım sunan bir çerçeve olarak oldukça önemlidir. Bu model, savunmacıların saldırganların kullandığı teknikleri, araçları ve prosedürleri anlamalarına ve bu tehditleri daha etkili bir şekilde tespit etmelerine yardımcı olur. "Pyramid of Pain" terimi, savunmanın ne kadar zorlu hale geldiğini ve saldırganların güvenlik önlemlerini atlatmaya yönelik yaptıkları çabaların maliyetini simgeler. Bu yazıda, MITRE'nin Pyramid of Pain çerçevesi hakkında ayrıntılı bir inceleme yapacak ve modelin her bir seviyesinin nasıl savunma stratejilerine katkı sağladığını açıklayacağız.

Pyramid of Pain Nedir?

Pyramid of Pain, savunma stratejilerinin ve tespit yöntemlerinin, saldırganların davranışlarını analiz etmek ve bu davranışları hedef almak için kullanılan bir modeldir. Model, saldırganların araç, teknik ve prosedürlerini sınıflandırarak her bir seviyede savunma yapmak için hangi tür verilerin ve gözlemlerin en faydalı olduğunu belirler. Modeldeki her seviye, saldırganın değiştirmesi veya manipüle etmesi daha zor olan göstergelerle ilgilidir. Bu seviyeler, "Ağrı Piramidi" olarak adlandırılmasının nedeni, her bir seviyedeki artan "ağrının" (yani, savunmaların zorluk derecesinin) saldırganlar için giderek daha maliyetli hale gelmesidir.

Pyramid of Pain Seviyeleri

MITRE'nin Pyramid of Pain modeli beş ana seviyeden oluşur. Her seviyedeki göstergeler, saldırganların tespit edilmesini engellemek amacıyla manipüle etmeleri daha zor olan verilerden seçilir.

Seviye 1: Geçici (Ephemeral)

Bu seviye, kısa süreli ve kolayca değiştirilebilen göstergeleri temsil eder. Bu tür göstergeler genellikle saldırganlar tarafından hızla değiştirilip silinebilir. Örnekler arasında IP adresleri, dosya adları veya URL'ler bulunur. Savunma için bu göstergelerin takibi genellikle kısa vadeli ve sınırlıdır, çünkü saldırganlar bu tür göstergeleri hızla değiştirebilir. Ancak, bunlar yine de anlık saldırıların tespiti için önemlidir.

Seviye 2: Saldırgan Tarafından Taşınan Araçlar (Adversary-Brought Tools)

Bu seviye, saldırganların kendi kullandıkları özel araçları içerir. Bu araçlar, genellikle saldırganlar tarafından dışarıdan getirilir ve genellikle daha izole, belirgin araçlardır. Cobalt Strike, Metasploit veya diğer ticari saldırı araçları bu kategoriye girer. Bu araçlar, saldırganların sistemlere erişim sağlamak için kullandığı araçlar olup, savunmalar için genellikle daha kolay tespit edilirler çünkü bu araçlar sistemde nadiren bulunur. Ancak, bazı durumlarda saldırganlar bu araçları gizlemek için değişiklikler yapabilir.

Seviye 3: Mevcut Araçlar (Core to Pre-Existing Tools)

Bu seviye, sistemde zaten bulunan ve normalde zararsız olarak kabul edilen araçları içerir. Saldırganlar bu araçları, genellikle "Living off the Land" (LotL) stratejisiyle kötüye kullanarak meşru sistem araçlarını kendi saldırılarına dahil ederler. Örneğin, Windows'taki WMIC veya PowerShell gibi araçlar bu seviyeye örnek verilebilir. Bu tür araçlar, savunma için daha zordur çünkü genellikle meşru olarak kullanılırlar ve bunların kötüye kullanıldığını fark etmek daha karmaşıktır. Savunmanın bu seviyede başarılı olabilmesi için, bu araçların normalden sapma gösteren kullanımlarını tespit etmek gerekir.

Seviye 4: (Alt) Tekniğin Uygulamalarına Temel (Core to Some Implementations of (Sub-)Technique)

Bu seviye, belirli bir tekniğin veya alt-teknüğün belirli uygulamalarına işaret eder. Bu, genellikle bir teknik veya alt-teknikteki belirli bir davranışa dayalı gözlemleri içerir. Saldırganlar, bu tekniklerin her uygulamasında benzer izler bırakırlar, ancak yine de bazı varyasyonlar gösterebilirler. Bu seviyede saldırganlar, örneğin dosya silme veya başka bir iz silme tekniğini kullanırken, belirli gözlemlerle tespit edilebilirler. Bu tür gözlemler, saldırganın hangi alt-teknikleri kullandığını anlamak için kullanılır.

Seviye 5: Teknik veya Alt-Tekniğe Temel (Core to Sub-Technique or Technique)

En yüksek seviye, genellikle saldırganın değiştirmekte zorlandığı en temel teknikleri ve alt-teknikleri içerir. Bu seviyedeki gözlemler, saldırganların kullandığı tekniklerin ve prosedürlerin zorla değiştirilmesini engeller. Örneğin, zamanlanmış görevlerin manipülasyonu gibi teknikler, belirli bir teknik uygulandığında her zaman belirli gözlemler bırakır. Bu tür gözlemler, saldırganın ne yaptığına dair çok sağlam ipuçları sağlar ve bu seviyedeki tespitler, saldırganları genellikle izlemekten alıkoyacak kadar etkili olabilir.

Pyramid of Pain'de Araçların ve Tekniklerin Yeri

Pyramid of Pain, MITRE'nin "Summiting the Pyramid" adlı bir güncellemesiyle daha da geliştirilmiştir. Bu güncelleme ile "Araçlar" kavramı iki farklı seviyeye bölünmüştür:

- **Seviye 2:** Saldırganlar tarafından taşınan ve genellikle kolayca değiştirilebilen araçlar.
- **Seviye 3:** Zaten sistemde mevcut olan araçlar, ki bu araçlar saldırganlar tarafından kötüye kullanılabilir.

Pyramid of Pain ve Ransomware Örnekleri

Ransomware saldırıları, özellikle Snatch Ransomware gibi sofistike örneklerle, Pyramid of Pain modelini nasıl kullandığını ve savunmaların nasıl şekillendirilebileceğini gösterir. Örneğin, Snatch ransomware, Windows Safe Mode'da çalışan bir arka kapıyı açmak için kayıt defteri anahtarlarını değiştirir ve bu değişiklikler Event ID 4657 ve 7045 ile tespit edilebilir. Bu tür gözlemler, savunma ekiplerinin yüksek seviyeli verilerle saldırıları daha etkin bir şekilde tespit etmelerini sağlar.

MITRE'nin Pyramid of Pain Projesinin Faydaları

MITRE'nin Pyramid of Pain modelinin uygulanması, savunma ekiplerine daha hedeflenmiş ve güçlü tespit yöntemleri sağlar. Yüksek seviyedeki tekniklerin ve gözlemlerin izlenmesi, saldırganların daha fazla maliyetle karşılaşmasına ve savunmaların daha güçlü hale gelmesine yol açar. Ayrıca, bu modelin kullanımıyla, daha sofistike ve evrimleşen tehditlere karşı savunma stratejileri oluşturulabilir, bu da siber güvenlik tehditlerinin daha etkin bir şekilde yönetilmesine olanak tanır.

Pyramid of Pain, savunma stratejilerini daha verimli hale getiren güçlü bir modeldir. Her seviyedeki göstergelerin doğru bir şekilde izlenmesi, saldırganların faaliyetlerini tespit etmek ve bunları engellemek için kritik önem taşır. Savunma ekiplerinin bu modeli uygulayarak daha sağlam, dirençli ve proaktif güvenlik stratejileri geliştirmesi mümkündür.

SONUÇ

Bu rapor, Mitre ATT&CK Framework'ün siber güvenlik alanındaki önemini vurgulamaktadır. Framework, tehdit aktörlerinin kullandığı yöntemleri anlamada ve savunma stratejileri geliştirmede kritik bir rol oynamaktadır. Ayrıca, TTP tabanlı tehdit avcılığı ve güvenlik mühendisliği, siber güvenlikte daha proaktif bir yaklaşım sergilemeye yardımcı olmaktadır. 2022 Ukraine Electric Power Attack örneği üzerinden yapılan analiz, Mitre ATT&CK framework'ünün gerçek dünyadaki saldırı senaryolarını anlamadaki gücünü ortaya koymuştur. Senaryoda, tehdit aktörlerinin keşif aşamasından başlayarak nasıl ilerlediği ve hangi teknikleri kullandığı Mitre ATT&CK tablosunda detaylı bir şekilde gösterilmiştir. Ayrıca, Pyramid of Pain modeli de siber tehditleri daha iyi anlamak ve savunma stratejilerini daha etkili hale getirmek için önemli bir araç olarak raporda yerini almıştır. Bu rapor, Mitre ATT&CK framework ile ilgili derinlemesine bilgi sahibi olmayı ve bu bilgilerin siber tehditlerle mücadelede nasıl uygulanabileceğini ortaya koymayı hedeflemiştir.

KAYNAKÇA

[1] https://attack.mitre.org

[2] https://www.picussecurity.com

[3] https://github.com

[4] https://thedfirreport.com

[5] https://chatgpt.com