

MITRE & Pyramid of Pain



M. Barış Güven

17.02.2025

Giriş	3
Mitre ATT&CK Framework	4
Mitre ATT&CK Tablosu Nedir?	4
Mitre ATT&CK Tablosu neden önemlidir?	5
Mitre ATT&CK Framework’de bulunan taktik ve tekniklerin önemi.....	5
TTP nedir?.....	7
TTP-Based Threat Hunting ve Detection Engineering	8
TTP-Based	8
Threat Hunting (Tehdit Avcılığı)	8
Detection Engineering (Tespit Mühendisliği)	8
2022 Ukraine Electric Power Attack	8
Senaryo.....	11
Pyramid of Pain	13
Göstergelerin Anlamları.....	14
Hash Değerleri:.....	14
IP Adresleri:	15
Domain Names (Alan Adları):	15
Network/Host Artifacts.....	15
Tools.....	15
TTP’s (Taktikler, Teknikler ve Prosedürler)	15
Pyramid of Pain’nin Tehdit İstihbaratındaki Önemi	15
Pyramid of Pain Nasıl Çalışır?.....	16
Sonuç.....	17
Kaynakça.....	18

Giriş

Bu rapor Siber Vatan bünyesinde çalışan Altay Takımı için hazırlanmıştır. Raporda Mitre ATT&CK ve Pyramid of Pain Modeli araştırılıp incelenmiştir. Mitre, siber suçluların Taktik, Teknik ve Prosedürlerini inceleyip oluşturduğu matrisler ile bu saldırıların tanımını yapan bir platformdur. Bu saldırılarda kullanılan; taktik, teknik ve prosedürlere göre siber analistlerin, saldırı aşamalarında, hangi güvenlikleri almaları gerektiğine yardımcı olur. Pyramid of Pain'de Tehdit İstihbaratı alanında, analistlere yardımcı olan bir modüldür. Buna göre saldırganların sisteme yapabilecek saldırı aşamalarını inceliyoruz.

Mitre ATT&CK Framework

Siber dünyada saldırganların sisteme yapabileceği eylemleri gösteren teknik, taktik ve prosedürlerin yer aldığı bilgi tabanıdır. 2013 yılından itibaren Mitre firması tarafından geliştirilmektedir, ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) saldırganların davranışlarını sistematik olarak kategorize etme ihtiyacından doğmuştur. Gerçek dünya gözlemlerine dayanır, düşman taktikleri ve tekniklerini içeren küresel olarak erişilebilen bir tabandır. Özel sektörde, hükümette ve siber güvenlik ürün ve hizmet topluluğunda belirli tehdit modellerinin ve metodolojilerinin geliştirilmesi için bir temel olarak kullanılır.

Saldırganların mevcut sistemdeki faaliyetlerinin sınıflandırılması gerekmektedir. Saldırganlar, mevcut güvenlik önlemleriyle tespit edilmemesi için saldırı yöntemlerini değiştireceklerdir. Saldırganın hedefi doğrultusunda alabileceği aksiyonlara karşı risklerin belirlenmesi, gerekli iyileştirme ve planlamaların yapılması, alınan güvenlik önlemlerinin doğruluğunu kontrol etmek için kullanılmaktadır.

MITRE ATT&CK, birkaç farklı matristen oluşmaktadır.

- **Enterprise ATT&CK:** Windows, Linux veya MacOS sistemlerine uygulanan teknik ve taktiklerden oluşur.
- **Mobile ATT&CK:** Mobil cihazlara uygulanan taktik ve teknikleri içerir.
- **Pre-ATT&CK:** Saldırganların sisteme girmeden önceki çalışmalarını içeren taktik ve teknikleri içerir.

Mitre ATT&CK Tablosu Nedir?

Mitre ATT&CK tablosu, taktik ve tekniklerin belli aşamalar halinde kategorize edildiği yerdir. Bu kategoriler hiyerarşik bir sıralama içerisinde yer alırlar. Saldırganın bir hedefe saldırmadan önce yaptığı keşif (reconnaissance) aşamasından, saldırı sonrası hedefe vereceği kalıcı zarara (Impact) kadar olan süreci gösterir. Her taktiğin birden fazla farklı tekniği ve

bazı tekniklerinde bir veya birden fazla alt tekniği bulunur.

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (2) Gather Victim Host Information (4) Gather Victim Identity Information (2) Gather Victim Network Information (2) Gather Victim Org Information (4) Pushing for Information (4) Search Closed Sources (2) Search Open Technical Databases (2) Search Open Websites/Domains (2) Search Victim-Owned Websites	Acquire Access (4) Acquire Infrastructure (4) Compromise Accounts (2) Compromise Infrastructure (4) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (2) Stage Capabilities (4) Valid Accounts (4)	Content Injection (4) Drive-by Compromise (4) Exploit Public-Facing Application (2) External Remote Services (4) Phishing (4) Replication Through Removable Media (4) Supply Chain Compromise (2) Trusted Relationship (4) Valid Accounts (4)	Cloud Administration Command (4) Command and Scripting Interpreter (11) Container Administration Command (4) Deploy Container (4) Exploitation for Client Execution (4) Inter-Process Communication (2) Native API (4) Scheduled Task/Job (2) Serverless Execution (4) Shared Modules (4) System Services (2) User Execution (2) Windows Management Instrumentation (4)	Account Manipulation (7) BITS Jobs (4) Boot or Logon Autostart Execution (4) Boot or Logon Initialization Scripts (2) Boot or Logon Initialization Scripts (2) Browser Extensions (4) Create Account (2) Create or Modify System Process (2) Domain or Tenant Policy Modification (2) Event Triggered Execution (17) External Remote Services (4) Hijack Execution Flow (2) Implant Internal Image (4) Modify Authentication Process (2) Office Application Startup (4) Power Settings (4) Pre-OS Boot (2) Scheduled Task/Job (2) Server Software Component (2) Traffic Signaling (2) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (2) Account Manipulation (2) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (2) Browser Extensions (4) Create Account (2) Create or Modify System Process (2) Domain or Tenant Policy Modification (2) Execution Guardrails (2) Escape to Host (4) Event Triggered Execution (17) Exploitation for Privilege Escalation (4) Hijack Execution Flow (13) Process Injection (2) Scheduled Task/Job (2) Valid Accounts (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (2) BITS Jobs (4) Build Image on Host (4) Debugger Evasion (4) Decfuscate/Decode Files or Information (4) Deploy Container (4) Direct Volume Access (4) Domain or Tenant Policy Modification (2) Execution Guardrails (2) Escape to Host (4) Exploitation for Defense Evasion (4) File and Directory Permissions Request Modification (2) Hide Artifacts (12) Hijack Execution Flow (13) Process Injection (2) Impair Defenses (11) Impersonation (4) Indicator Removal (10) Indirect Command Execution (4) Masquerading (10) Modify Authentication Process (2) Modify Cloud Compute Infrastructure (2) Modify Cloud	Adversary-in-the-Middle (4) Brute Force (4) Credentials from Password Stores (2) Exploitation for Credential Access (4) Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (4) Multi-Factor Authentication Interception (4) Multi-Factor Authentication Request Generation (4) Network Sniffing (4) OS Credential Dumping (2) Steal Application Access Token (4) Steal or Forge Authentication Certificates (4) Steal or Forge Cookies (4) Steal Web Session (4) Unsecured Credentials (4) Modify Cloud	Account Discovery (4) Application Window Discovery (4) Browser Information Discovery (4) Cloud Infrastructure Discovery (4) Cloud Service Dashboard (4) Cloud Service Discovery (4) Cloud Storage Object Discovery (4) Container and Resource Discovery (4) Debugger Evasion (4) Device Driver Discovery (4) Domain Trust Discovery (4) File and Directory Discovery (4) Group Policy Discovery (4) Log Enumeration (4) Network Service Discovery (4) Network Share Discovery (4) Network Sniffing (4) Password Policy Discovery (4) Peripheral Device Discovery (4)	Exploitation of Remote Services (4) Internal Spearphishing (4) Lateral Tool Transfer (4) Remote Service Session Hijacking (2) Remote Services (4) Application Through Removable Media (4) Software Deployment Tools (4) Taint Shared Content (4) Use Alternate Authentication Material (4)	Adversary-in-the-Middle (4) Archive Collected Data (2) Audio Capture (4) Automated Collection (4) Browser Session Hijacking (2) Clipboard Data (4) Data from Cloud Storage (4) Data from Configuration Repository (2) Data from Information Repositories (2) Data from Local System (4) Data from Network Shared Drive (4) Data from Removable Media (4) Data Staged (2) Email Collection (2) Input Capture (4) Screen Capture (4) Video Capture (4)	Application Layer Protocol (2) Communication Through Removable Media (4) Content Injection (4) Data Encoding (2) Data Obfuscation (2) Dynamic Resolution (2) Encrypted Channel (2) Fallback Channels (2) Hide Infrastructure (4) Ingress Tool Transfer (4) Multi-Stage Channels (4) Non-Application Layer Protocol (4) Non-Standard Port (4) Protocol Tunneling (4) Proxy (4) Remote Access Software (4) Traffic Signaling (2) Web Service (2)	Automated Exfiltration (2) Data Transfer Size Limits (4) Exfiltration Over Alternative Protocol (2) Exfiltration Over C2 Channel (4) Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (2) Exfiltration Over Web Service (4) Scheduled Transfer (4) Transfer Data to Cloud Account (4)	Account Access Removal (4) Data Destruction (1) Data Encrypted for Impact (4) Data Manipulation (2) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Financial Theft (4) Firmware Corruption (4) Inhibit System Recovery (4) Network Denial of Service (2) Resource Hijacking (4) Service Stop (4) System Shutdown/Reboot (4)

Mitre ATT&CK Tablosu neden önemlidir?

Mitre ATT&CK tablosu saldırı hakkında bir kılavuz özelliği taşır. Bu saldırıların hangi cihazlarda nerede ve ne zamanlarda kullanıldığı hakkında geniş bir bilgi sunar. Bu bilgileri kullanarak cihazlarımızı daha rahat sıkılaştırabilmemize olanak sağlar. Aynı zamanda bünyesinde saldırgan gruplar (APT) hakkında da bilgiler barındırmaktadır. APT gruplarının saldırırken kullandığı, taktik ve teknikleri örneklerle açıklamasıyla, bu grupların faaliyetlerini izleme açısından fikir verir. Bünyesinde barındırdığı veri kaynakları ile de saldırı tespit etmek ve önlem almak için kullanılabilir potansiyel izleme noktalarını içerir. Güvenlik ekiplerine saldırı tespit etme ve müdahale etme konusunda rehberlik eder.

Mitre ATT&CK Framework’de bulunan taktik ve tekniklerin önemi

Reconnaissance (Keşif)

Saldırganlar hedef sistem veya ağ hakkında aktif ve pasif bilgi toplamaya çalışır. Pasif bilgi toplama, hedef sistemle doğrudan etkileşime geçmeden açık kaynak üzerindeki servislerden veya web sitelerinden bilgi toplama yöntemidir. Aktif bilgi toplama, doğrudan sistem taraması veya erişimi ile yapılan bilgi toplama tekniğidir. Hedef sisteme doğrudan erişim yada tarama ile yapılan bilgi toplama tekniğidir. Sistem ile etkileşime geçildiğinden izin alınmadan yapılan bir bilgi toplama girişimi, aktif bilgi toplanan sistem bilgilerine; bilişim sisteminin altyapı ve personel bilgileri gibi hassas verilerini içerebilmektedir.

Resource Development (Kaynak Geliştirme)

Saldırganlar hedeflerini yapacakları saldırıyı desteklemek ve güçlendirmek için gerekli kaynakları oluşturur veya temin eder. Bu kaynaklar, saldırıyı desteklemek için altyapı, hesaplar veya özel yetenekler gibi çeşitli unsurları içerir. Saldırganlar, operasyonlarını desteklemek için stratejik olarak seçilen veya hazırlanan kaynakları kullanarak saldırılarını daha etkili hale getirmeye çalışırlar.

Initial Access (İlk Erişim)

Saldırganlar, hedef ağı veya sistemlere çeşitli giriş vektörlerini kullanarak ilk erişimi sağlar. Hedeflenen sistemlerdeki zafiyetlerden yararlanarak erişim elde edilebilir. Örneğin, güvenlik açıklarını sömürmek, halka açık sunucuları hedeflemek, kimlik avı saldırıları düzenlemek veya sosyal mühendislik yöntemlerini kullanmak gibi farklı taktiklerle saldırganlar, erişim sağlamak için çeşitli yolları arar. Sağladıkları zafiyetler ile de ilk erişimi elde etmiş olurlar.

Execution (Yürütme)

Saldırganlar kötü amaçlı kodları hedef sistemlerde çalıştırmak için “Exploits (Sömürüler), Phishing (Kimlik Avı), Uzaktan Komut ve Kontrol (RAT)” gibi teknikleri kullanırlar. Saldırganlar, erişim elde ettikleri yerel veya uzak sistemlerdeki kötü amaçlı yazılımları yürüterek genellikle hedeflerine daha fazla erişim sağlamak, sistemleri keşfetmek veya veri sızıntısı gibi daha geniş hedeflere ulaşmak için çeşitli yöntemleri kullanır. Bu aşama genellikle diğer taktiklerle birlikte kullanılır ve saldırganların operasyonlarını genişletmelerine olanak tanır.

Persistence (Kalıcılık)

Saldırganların, eriştiği sisteme olan erişiminin sona ermemesi ve sistemde olan ilerleyişini devam ettirebilmesi için kullandığı çeşitli tekniklerin uygulandığı evredir. Örnek olarak sisteme bulaştırdığı zararlı bir yazılım ile makinenin her başlangıcında sistemde saldırganın da yetki sahibi olmasını sağlayabilir, kimlik bilgilerini değiştirebilir ve mevcut erişimi engelleyici faaliyetlerde bulunabilir.

Privilege Escalation (Yetki Yükseltme)

Saldırganların erişim sağladığı sistemdeki hesabın mevcut yetkilerinin kısıtlı olması durumunda, sistemde daha özgür hareket edebilmek amacı ile daha geniş yetkilere sahip hesaplara erişmesi durumudur. Sistemdeki bazı güvenlik açıklarından yararlanarak sistemde admin yetkileri kullanılabilir. Bu yetkilerle sistem üzerinde vereceği zararın boyutunu artırabilir. Bu aşama, yetki yükseltme adına kullanılan teknikleri gösterir.

Defense Evasion (Savunmadan Kaçınma)

Sistem içerisinde saldırgan, algılanmayı önlemek için güvenlik önlemlerini atlatmak veya engellemek adına çeşitli teknikler kullanırlar. Bu aşama tespit edilmemek için izlerini gizlemeye çalışan saldırganların savunma mekanizmalarını atlatma çabalarını içerir.

Credential Access (Kimlik Bilgileri Erişimi)

Saldırganlar, kullanıcı hesaplarına ve kimlik bilgilerine erişmeye çalışır. Bu adımda saldırgan, hesap şifreleri, oturum açma bilgileri veya kimlik doğrulama verilerini ele geçirmeyi hedefler.

Discovery (Keşif)

İç ağ ve sistem hakkında daha geniş bilgi toplama aşamasında kullanılan teknikleri gösterir. Buradaki teknikler, saldırganın nasıl hareket edeceğine karar vermeden önce çevreyi gözlemlemelerine ve kendilerini yönlendirmelerine yardımcı olur.

Lateral Movement (Yanal Hareket)

Bir ağdaki uzak sistemlere girmek ve kontrol etmek için saldırganlar bu aşamadaki teknikleri kullanırlar. Öncelikli hedeflerini takip eder ve genellikle hedeflerini bulmak için ağ keşfetmeleri ve daha sonra ona erişmeleri gerekmektedir. Amaçları birden fazla sistem ve hesabın kontrolüne erişmektir. Saldırganlar bu taktiği kullanırken, kendi uzaktan erişim araçlarını veya yerel ağ ve işletim sistemi araçlarıyla, sömürü yaparken kullandıkları kimlik bilgileri ile anonim kalabilirler.

Collection (Toplama)

Saldırganların bilgi toplarken kullandığı tekniklerin yer aldığı taktik aşamasıdır. Amaçlarına göre farklı teknikler kullanırlar. Genelde, veri topladıktan sonra bir başka hedefteki verileri sızdırmak veya hedef ortam hakkında daha fazla bilgi edinmek için verileri kullanırlar. Yaygın olarak hedef aldıkları kaynaklar, çeşitli sürücü tipleri, tarayıcılar, ses, video ve e-postalardır. Yaygın toplanan veriler: ekran görüntüleri ve klavye girişleridir.

Command and Control (Komuta ve Kontrol)

Bir kurban ağ içindeki kontrol altında tutulan sistemlerle iletişim kurmak için kullanılabilecek tekniklerden oluşur. Saldırganlar genellikle tespit edilmekten kaçınmak için ağ trafiğini taklit etmeye çalışırlar. Hedef sistemin ağ yapısına ve savunmasına bağlı olarak çeşitli şekillerde sızdırılabilen bir yapıdır.

Exfiltration (Sızma)

Saldırganların ağdan veri çalmak için kullanabilecekleri tekniklerden oluşur. Verileri topladıktan sonra, toplanan verileri tespit edilmeden paketlerler. Hedef bir ağdan veri elde etme teknikleri tipik olarak komuta ve kontrol kanalları veya alternatif bir kanal üzerinden verileri sızdırma işlemidir.

Impact (Etki)

Saldırgan sistemlerinizi ve verilerinizi manipüle etmeye, kesintiye uğratmaya veya yok etmeye çalıştığı taktik aşamasıdır. Bu aşamada kullanılan tekniklerle iş ve operasyonel süreçlerin manipüle olması, kullanılabilirliğinin bozulması veya bütüncül olarak tehlikeye girmesi amaçlanır. Bazı durumlarda, iş süreçleri iyi görünebilir fakat saldırganların hedefleri doğrultusunda gizli kalabilmek için kurduğu bir manipülasyon tekniğidir.

TTP nedir?

TTP; Taktik, Teknik ve Prosedür olarak üç aşamadan meydana gelir. Aşamaları sırasıyla açıklamak gerekirse:

- **Taktik:** Saldırganların hedeflerine ulaşmak için kullandıkları belirli amaçları temsil eder. Örnek olarak keşif yaparak bilgi toplamak, ilk erişim sağlamak veya verileri sızdırmak gibi.
- **Teknik:** Taktiklerin gerçekleştirilebilmesi için kullanılan yöntemleri ayrıntıları ile açıklar. Örnek olarak kimlik avı saldırıları veya sistem açıklarından yararlanma gibi. Bazı tekniklerin mevcut olarak **alt teknikleri** de olur. Bu alt teknikler de daha düşük

seviyedeki saldırı davranışını tanımlar ve güvenlik ekiplerinin belirli riskleri azaltmak için ayrıntılı siber güvenlik taktikleri oluşturmalarına yardımcı olur. Bir kimlik avı saldırısı yaparken kötü amaçlı bir ek kullanma gibi.

- **Prosedürler:** Saldırganların bir tekniği veya alt tekniği yürütmek için kullandıkları belirli uygulamalardır. Örneğin bir saldırıdan LSASS belleğini kazıyarak kimlik bilgisi elde etmesi.

TTP-Based Threat Hunting ve Detection Engineering

TTP-Based

Saldırganların hedeflerine ulaşmak için kullanmaları gereken teknikleri tanımlamak ve aramak, saldırıların kullandığı araçları ve açıkları aramaktan daha oturaklı bir yaklaşımdır. Bu teknikler sık sık değişmediği gibi hedef teknolojinin kısıtlamaları nedeniyle saldırıların arasında yaygın olarak görülür. Mitre ATT&CK çerçevesi, bu teknikleri tanımlamak için etkili bir yöntemdir. ATT&CK, kamuya açık siber tehdit istihbaratından bildirilen düşman TTP'lerini taktik kategorilere göre sınıflandırır ve bunları Cyber Attack Lifecycle aşamaları içerisinde hizalar.

Cyber Attack Lifecycle (Siber Saldırı Yaşam Döngüsü):

Bir saldırının, yaptığı başarılı saldırının, aşamalarını özetleyen bir çerçevedir.

Threat Hunting (Tehdit Avcılığı)

Tehdit avcılığı, siber tehdit avcılığı olarak da bilinir; bir organizasyonun ağı içinde daha önce tespit edilmemiş veya halen devam eden siber tehditleri belirlemeye yönelik proaktif bir yaklaşımdır.

Tehdit avcılığı, içerden kaynaklanan tehditler ve aksi halde fark edilmeyecek diğer siber saldırılara karşı kuruluşların güvenlik duruşlarını güçlendirmeye yardımcı olduğu için önemlidir. Otomatik güvenlik araçları ve dikkatli SOC (Güvenlik Operasyon Merkezi) analistleri, çoğu siber güvenlik tehdidini büyük zararlar vermeden önce tespit edebilse de, bazı sofistike tehditler bu savunmaları aşabilir.

Detection Engineering (Tespit Mühendisliği)

Kötü amaçlı etkinlikleri belirlemek için belirli kalıpları, davranışları ve ihlal göstergelerini (Indicators of Compromise | IoCs) tanıyan tespit kuralları setlerini tasarlama, uygulama ve sürekli olarak iyileştirme uygulamasıdır. Bu, birçok SIEM sisteminde kutudan çıkar çıkmaz hazır gelen kurallara yalnızca güvenmekten öteye geçer; verilerinizi derinlemesine incelemeyi, log davranışlarını anlamayı ve ileri düzey bir saldırının neler yapabileceğini öngörmeyi gerektirir.

2022 Ukraine Electric Power Attack

Rus hacker grubu Sandworm, Ukrayna hükümet yetkilileri ve slovak siber güvenlik firması ESET'e göre, 2 milyon kişinin etkileneceği bir kesintiye yol açmayı hedefleyerek Ukrayna enerji şebekesine saldırdı. Bu saldırının Mitre ATT&CK platformunda yayınlanan teknikleri şu şekilde paylaşılmıştır:

Enterprise		
ID	İsim	Kullanım
T1059.001	Command and Scripting Interpreter: PowerShell	Windows Grup İlke'sini kullanarak bir silme aracını yaymak ve başlatmak için TANKTRAP adlı bir PowerShell yardımcı programı kullanıldı.
T1543.002	Create or Modify System Process: Systemd Service	GOGETTER isimli araçlarının kalıcılığını koruması için systemd'yi yapılandırıp sistem kullanıcı oturum açmalarını kabul etmeye başladığında GOGETTER'ı çalıştırmak için <i>WantedBy=multi-user.target</i> yapılandırmasını belirtti.
T1485	Data Destruction	Sandworm Ekibi, OT (Operational Technology) yetenekleri ile, eşlenen sürücüler ve fiziksel sürücü bölümlerini silmek için kurbanın BT ortam sistemlerine CaddyWiper'ı yerleştirdi.
T1484.001	Domain or tenant Policy Modifaciton: Group Policy Modification	Kötü amaçlı yazılımları dağıtmak ve yürütmek için Grup İlkesi Nesnelerini (GPO) kullandı.
T1570	Lateral Tool Transfer	CaddyWiper'ın yürütülebilir msserver.exe dosyasını bir hazırlama sunucusundan yerel bir sabit sürücüye koplayamak için Grup İlkesi Nesnesi (GPO) kullandı.
T1036.004	Masquerading: Masquerade Task or Service	GOGETTER kötü amaçlı yazılımını meşru veya meşru görünen hizmetler olarak maskelemek için Systemd hizmet birimlerinden yararlandı.
T1095	Non-Application Layer Protocol	TLS tabanlı bir tünel içinde C2 iletişimlerini proxy'ledi.
T1572	Protocol Tunneling	Harici sunucu veya sunucular ile "Yamux" TLS tabanlı bir C2 kanalı kurmak için GOGETTER tünelleme yazılımını konuşturdu.
T1053.005	Scheduled Task/Job: Scheduled Task	CaddyWiper'ı önceden belirlenmiş bir zamanda yürütmek için bir Grup İlkesi Nesnesi (GPO) arac
T1505.003	Server Software Component: Web Shell	Neo-REGEORGwebshell'i internete bakan bir sunucuya yerleştirdiler.

Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 4 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Cloud Administration Command	Account Manipulation (0-7)	Abuse Elevation Control Mechanism (0-1)	Abuse Elevation Control Mechanism (0-1)	Adversary-in-the-Middle (0-4)	Account Discovery (0-4)	Exploitation of Remote Services (0-4)	Adversary-in-the-Middle (0-4)	Application Layer Protocol (0-1)	Automated Exfiltration (0-1)	Account Access Removal (0-1)
AppleScript	BITS Jobs	Access Token Manipulation (0-3)	Access Token Manipulation (0-3)	Brute Force (0-4)	Application Window Discovery (0-4)	Internal Spearphishing (0-4)	Archive Collected Data (0-4)	Communication Through Removable Media (0-1)	Data Transfer Size Limits (0-1)	Data Destruction (0-1)
AutoHotkey & AutoIT	Boot or Logon Autostart Execution (0-1)	Account Manipulation (0-3)	Account Manipulation (0-3)	Credentials from Password Stores (0-1)	Browser Information Discovery (0-1)	Remote Service Session Hijacking (0-1)	Audio Capture (0-1)	Content Injection (0-1)	Exfiltration Over Alternative Protocol (0-1)	Data Encrypted for Impact (0-1)
Cloud API	Boot or Logon Initialization Scripts (0-1)	Build Image on Host (0-1)	Build Image on Host (0-1)	Exploitation for Credential Access (0-1)	Cloud Infrastructure Discovery (0-1)	Cloud Service Dashboard (0-1)	Automated Collection (0-1)	Data Encoding (0-1)	Exfiltration Over C2 Channel (0-1)	Data Manipulation (0-1)
JavaScript	Boot or Logon Autostart Execution (0-1)	Debugger Evasion (0-1)	Debugger Evasion (0-1)	Forged Authentication (0-1)	Cloud Service Dashboard (0-1)	Cloud Service Dashboard (0-1)	Remote Services (0-1)	Data Obfuscation (0-1)	Exfiltration Over C2 Channel (0-1)	Defacement (0-1)
Java	Boot or Logon Initialization Scripts (0-1)	Desktops/Decode Files or Information (0-1)	Desktops/Decode Files or Information (0-1)	Forge Web Credentials (0-1)	Cloud Service Dashboard (0-1)	Cloud Service Dashboard (0-1)	Replication Through Removable Media (0-1)	Clipboard Data (0-1)	Exfiltration Over Other Network Medium (0-1)	Disk Wipe (0-1)
Network Device CLI	Browser Extensions (0-1)	Deploy Container (0-1)	Deploy Container (0-1)	Input Capture (0-1)	Cloud Storage Object Discovery (0-1)	Cloud Storage Object Discovery (0-1)	Software Deployment Tools (0-1)	Encrypted Channel (0-1)	Exfiltration Over Physical Medium (0-1)	Endpoint Denial of Service (0-1)
PowerShell	Create Account (0-1)	Container Service (0-1)	Container Service (0-1)	Modify Authentication Process (0-1)	Container and Resource Discovery (0-1)	Container and Resource Discovery (0-1)	Taint Shared Content (0-1)	Fallback Channels (0-1)	Exfiltration Over Web Service (0-1)	Financial Theft (0-1)
Python	Create or Modify System Process (0-1)	Launch Agent (0-1)	Launch Agent (0-1)	Trust Modification (0-1)	Use Alternate Authentication Material (0-1)	Use Alternate Authentication Material (0-1)	Hide Infrastructure (0-1)	Hide Infrastructure (0-1)	Exfiltration Over Web Service (0-1)	Firmware Corruption (0-1)
Unix Shell	Launch Daemon (0-1)	Systemd Service (0-1)	Systemd Service (0-1)	Multi-Factor Authentication Interception (0-1)	Debugger Evasion (0-1)	Debugger Evasion (0-1)	Ingress Tool Transfer (0-1)	Scheduled Transfer (0-1)	Inhibit System Recovery (0-1)	Resource Hijacking (0-1)
Visual Basic	Create or Modify System Process (0-1)	Windows Service (0-1)	Windows Service (0-1)	Multi-Factor Authentication Request Generation (0-1)	Device Driver Discovery (0-1)	Device Driver Discovery (0-1)	Multi-Stage Channels (0-1)	Transfer Data to Cloud Account (0-1)	Network Denial of Service (0-1)	Service Stop (0-1)
Windows Command Shell	Event Triggered Execution (0-1)	Domain or Tenant Policy Modification (0-1)	Domain or Tenant Policy Modification (0-1)	Network Stalling (0-1)	File and Directory Discovery (0-1)	File and Directory Discovery (0-1)	Non-Application Layer Protocol (0-1)	Transfer Data to Cloud Account (0-1)	System Shutdown/Reboot (0-1)	
Container Administration Command	External Remote Services (0-1)	Escape to Host (0-1)	Escape to Host (0-1)	OS Credential Dumping (0-1)	Data from Network Shared Drive (0-1)	Data from Network Shared Drive (0-1)	Protocol Tunneling (0-1)			
Deploy Container	Hijack Execution Flow (0-1)	Event Triggered Execution (0-1)	Event Triggered Execution (0-1)	Hide Artifacts (0-1)	Data from Removable Media (0-1)	Data from Removable Media (0-1)	Proxy (0-1)			
Exploitation for Client Execution	Hijack Execution Flow (0-1)	Hijack Execution Flow (0-1)	Hijack Execution Flow (0-1)	Hide Artifacts (0-1)	Data Staged (0-1)	Data Staged (0-1)	Remote Access Software (0-1)			
Inter-Process Communication (0-1)	Implant Internal Image (0-1)	Process Injection (0-1)	Process Injection (0-1)	Impersonation (0-1)	Email Collection (0-1)	Email Collection (0-1)	Traffic Signaling (0-1)			
Native API	At (0-1)	Scheduled Task/Job (0-1)	Scheduled Task/Job (0-1)	Indicator Removal (0-1)	Input Capture (0-1)	Input Capture (0-1)	Web Service (0-1)			
Scheduled Task/Job (0-1)	Modify Authentication Process (0-1)	At (0-1)	At (0-1)	Indirect Command Execution (0-1)	Screen Capture (0-1)	Screen Capture (0-1)				
Systemd Timers	Office Application Startup (0-1)	Scheduled Task/Job (0-1)	Scheduled Task/Job (0-1)	Maneuvering (0-1)	Video Capture (0-1)	Video Capture (0-1)				
Serverless Execution	Power Settings (0-1)	Scheduled Task/Job (0-1)	Scheduled Task/Job (0-1)							
Shared Modules	Pre-OS Boot (0-1)	At (0-1)	At (0-1)							
Software Deployment Tools	Scheduled Task/Job (0-1)	Container Orchestration Job (0-1)	Container Orchestration Job (0-1)							
System Services (0-1)	Systemd Timers (0-1)	Valid Accounts (0-1)	Valid Accounts (0-1)							
User Execution (0-1)	At (0-1)	Scheduled Task/Job (0-1)	Scheduled Task/Job (0-1)							
Windows Management Instrumentation	Windows Components (0-1)	Systemd Timers (0-1)	Systemd Timers (0-1)							
	SQL Stored Procedures (0-1)	At (0-1)	At (0-1)							
	Terminal Services DLL (0-1)	Container Orchestration Job (0-1)	Container Orchestration Job (0-1)							
	Transport Agent (0-1)	Valid Accounts (0-1)	Valid Accounts (0-1)							
	Web Shell (0-1)	Scheduled Task/Job (0-1)	Scheduled Task/Job (0-1)							

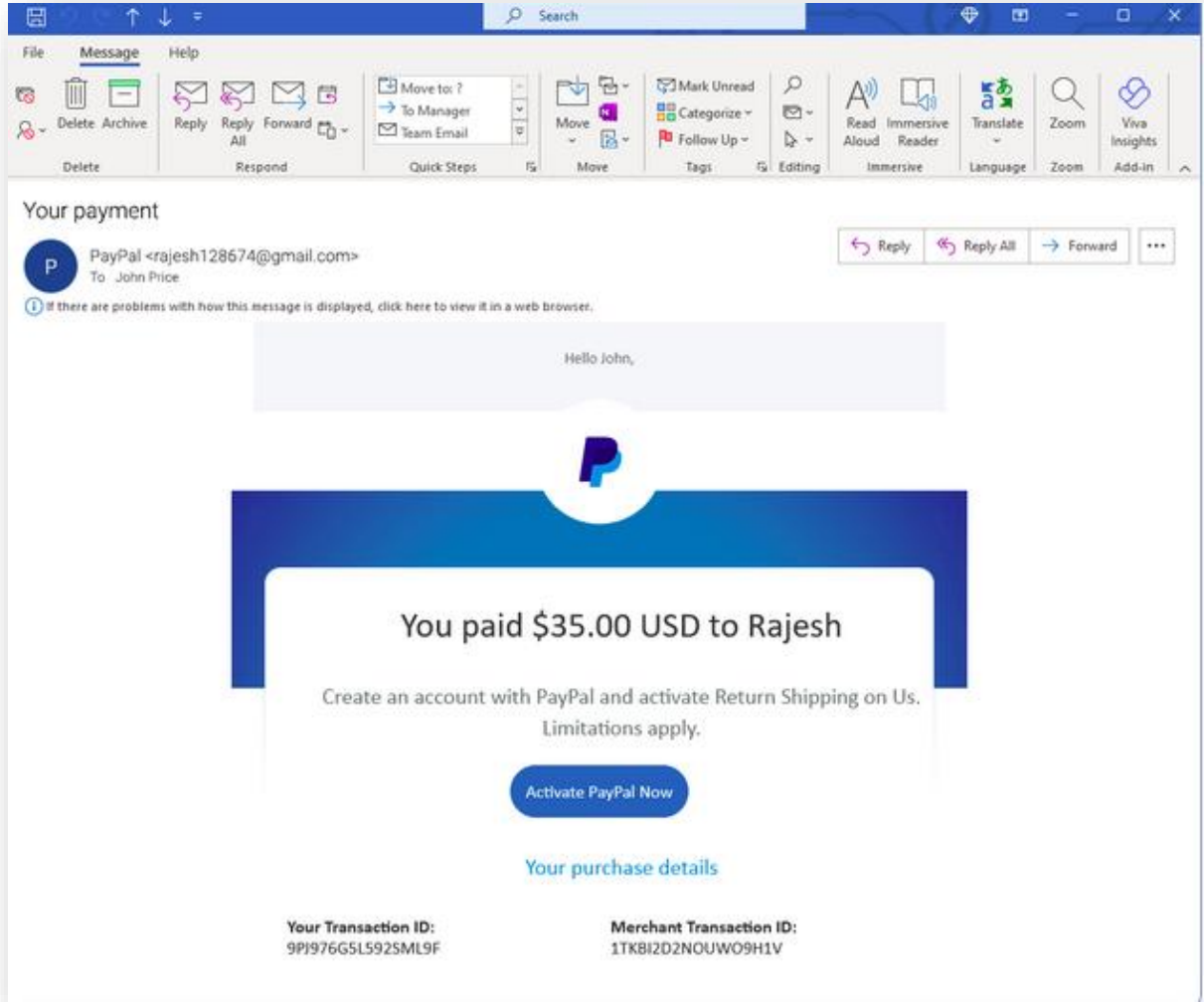
ICS		
ID	İsim	Kullanım
T0895	Autorun Image	Sandworm Ekibi, a.iso adlı bir ISO görüntüsünü bir SCADA sunucusu çalıştıran sanal bir makineye eşlemek için mevcut hipervizör erişimini kullandı. SCADA sunucusunun işletim sistemi, CD-ROM görüntülerini otomatik olarak çalıştıracak şekilde yapılandırıldı ve sonuç olarak, ISO görüntüsünde kötü amaçlı bir VBS betiği otomatik olarak yürütüldü.
T0807	Command-Line Interface	Sandworm Ekibi, scilc.exe ikili dosyası aracılığıyla komutları yürütmek için MicroSCADA platformundaki SCIL-API'yi kullandı.
T0853	Scripting	Sandworm Ekibi, n.bat'ı yürütmek için bir Visual Basic betiği olan lun.vbs'yi kullandı ve ardından MicroSCADA scilc.exe komutunu yürüttü.
T0894	System Binary Proxy Execution	Saldırgan tarafından tanımlanan bir dosyada belirtilen SCADA talimatlarının önceden tanımlanmış bir listesini göndermek için bir MicroSCADA uygulama ikili dosyası scilc.exe'yi çalıştırdı, s1.txt çalıştırılan komut; <C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt>

		SCADA yazılımını kullanarak yetkisiz komut mesajlarını uzak trafo merkezlerine gönderir.
T0855	Unauthorized Command Message	Trafo merkezlerine yetkisiz komutların gönderilmesi de dahil olmak üzere bir dizi SCADA talimatını belirtmek için MicroSCADA SCIL-API'yi kullandı.

Execution 10 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 7 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques
Autorun Image	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
Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter
Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware
Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message
Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message
Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential	
Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction	
Native API						Point & Tag Identification		Denial of Service	
Scripting						Program Upload		Device Restart/Shutdown	
User Execution						Screen Capture		Manipulate I/O Image	
						Wireless Sniffing		Modify Alarm Settings	
								Rootkit	
								Service Stop	
								System Firmware	

Senaryo

A isminde bir şirket düşünelim. A şirketi, ürün tedarikçilerine internet ortamında bir pazar oluşturuyor. Bu pazarı yönetmek adına arkaplanda çok sayıda siber güvenlik analisti ve yazılımcı çalışmakta. Bu şirketteki verileri çalmak isteyen kötü niyetli saldırganımız, şirket hakkında **Reconnaissance** aşamasında **T1593.001** Sosyal Medya tekniğini kullanarak bilgi topluyor. Bulduğu verilerle bu şirketin çağrı merkezinde çalışan X kullanıcısının sosyal medya hesabını bulup, ona phishing mail gönderiyor.



Gelen maili inceleyen çalışanın sorgusuz bir şekilde maili onayladığını varsayarsak, (T1566.002 Spearphishing Link) mail linkine bağlı olarak çalışan (T1204.001) Malicious File (kötü amaçlı dosya) kurbanımızın sistemine yüklenir. Bu şekilde saldırgan, kurbanın sistemi üzerinde çalıştırılabilir dosya ile **Execution** işlemi yapar. Execution işlemi yapan saldırgan, sistem içerisinde kalıcılık sağlamak isteyecektir, Burada da kurbanın sisteminin Windows olduğunu varsayarsak, kullanmak isteyeceği teknik T1543.003 Create or Modify System Process: Windows Service olacaktır. Saldırgan sistemde kalıcı olmak için yeni bir hizmet yükleyebilir yada mevcut bir hizmeti başlangıçta çalışacak şekilde değiştirebilir. Sistem yardımcı programları (sc.exe gibi) kullanılarak, Kayıt Defteri doğrudan değiştirilerek veya doğrudan Windows API ile etkileşime girilerek ayarlanabilir veya değiştirilebilir. Saldırganlar, bir sistemdeki kötü niyetli faaliyetlerin varlığını gizlemek için bu sürücülerini Rootkit olarak kullanabilir. Sisteme erişen saldırgan kalıcılığını koruduktan sonra aynı teknik ile **Privilege Escalation** (yetki yükseltme) taktiğini de kullanarak artık sistemde söz sahibidir. Bu şekilde A şirketinin çağrı merkezi sistemine bağlı olarak çalışan uygulamasının T1040 Network Sniffing tekniği ile ağ trafiğini dinleyebilir. Uygulama geniş bir ağ kullanacağı için geniş miktarda veri yakalanacaktır. Sonraki aşama ise ağ üzerinde aktif olarak şirketin çağrı merkezinden sorumlu kişileri tespit etmek (**discovery** taktiği) ve uygulama üzerinden onlara yanal hareket yapmayı denemek olacaktır. Burada da T1563

Remote Service Session Hijacking tekniđi devreye girer. Uzak bađlantıları kabul etmek üzere özel tasarlanmış bir hizmet kullanan çağrı merkezi sisteminde oturumu ele geçirmek için kollarını sıvar. Muhtemel RDP kullanan merkez uygulaması için *T1563.002* subtekniki (*RDP Hijacking*) kullanılacaktır. Akabinde ise *T1123 Audio Capture & T1125 Video Capture* teknikleri ile, çağrı merkezi kullanıcısının ve müşterinin arasında geçen kişisel bilgiler, kimlik bilgileri gibi kritik veriler toplanacaktır. Ve tabi saldırganımız bu sistemde kalıcılıđını sağladığı gibi, yetki yükseltme işlemini de başardığı için buraya bir **Command and Control** taktiki ile kanal oluşturmak isteyecektir. Bu kanalı oluşturmak için kullanmak isteyeceđi en güzel teknikte, *T1219 Remote Access Software* tekniđi olacaktır. Bu teknik Uzaktan erişim yazılımlarının kullandığı uzaktan izleme ve yönetim (RMM) araçları, yasal teknik destek yazılımı olarak kullanıldığından sistemde meşru bir komuta ve kontrol kanalı oluşturulabilir. Saldırganımız hedef aldığı A şirketinin çağrı merkezi sayesinde birçok müşteriyle olan iletişimi kullanarak **Impact** Taktiki altında bulunan, *T1657 Financial Theft* tekniđini kullanarak şirkete farketirmeden birçok müşterinin bilgilerini sızdırılabilir.

Pyramid of Pain

2013 yılında ortaya çıkan güvenlik uzmanı David J Bianco'nun icadıdır. Tehdit İstihbaratı alanında kullanılan model olan Pyramid of Pain, saldırıların; saldırı yaptıktan sonra verdikleri zararı basitten karmaşıđa doğru sıralayan bir hiyerarşik yapısı vardır. Bu katmanları anlamak, saldırıların hangi kategoride ne kadar çaba sarf edeceklerini öngörmemiz açısından önemlidir. Aşağıdaki görsel hiyerarşik yapıyı daha iyi anlamamızı

sağlayacaktır.



Göstergelerin Anlamları

Hash Değerleri:

Hash değeri, bir uygulamanın kimliğini temsil eder, verileri benzersiz bir şekilde tanımlayan sabit bir uzunluğun sayısal değeri olarak oluşturulmuşlardır. Bu değerlerin farklı algoritmaları mevcuttur, SHA1, MD5 vb. Bu SHA1, MD5 şüpheli veya zararlı dosyalara karşılık gelir. Genellikle kötü amaçlı yazılım örneklerine veya bir ihlalde yer alan dosyalara benzersiz referanslar sağlamak için kullanılır.

MD5 (Message Digest): 1992’de Ron Rivest tarafından tasarlandı ve 128-bit hash değerine sahip yaygın olarak kullanılan bir kriptografik hash işlevidir.

SHA-1 (Secure Hash Algorithm 1): 1995 yılında ABD Ulusal Güvenlik Ajansı tarafından icat edilmiştir. Veriler SHA-1; bir girdi alır ve 40 basamaklı bir altıgen sayı olarak 160-bit hash değer üretir. NIST, 2011 yılında SHA-1 kullanımını ortadan kaldırdı ve 2013 sonunda bruteforce saldırılarına duyarlı olmasına dayanarak dijital imzalar için kullanımını yasakladı.

SHA-2 (Secure Hash Algorithm 2): SHA-2 Hash Algoritması, 2001 yılında Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ve Ulusal Güvenlik Ajansı (NSA) tarafından SHA-1’in yerini almak için tasarlanmıştır. SHA-2’nin birçok varyantı var ve tartışmasız en yaygın

olanı SHA-256'dır. SHA-256 algoritması, 64 haneli altı eksenel sayı olarak 256 bitlik bir hash değeri döndürür.

Hashlerin zararlı olup olmadığını açık kaynak araçlarının yardımı ile öğrenebiliriz: Virustotal, Metadefender Cloud gibi. Tabi, saldırganlar, kötü amaçlı yazılımı küçük değişikliklerle yeniden paketleyerek yeni hash değerleri de oluşturabilir.

IP Adresleri:

Belirli IP adreslerini içerir, aynı zamanda netblockları da kapsar. Bir ağa bağlı herhangi bir cihazı tanımlamak için bir IP adresi kullanılır. Masüstü bilgisayarlardan, sunuculara kadar uzanır. Zararlı aktörlerin IP adresleri engellenebilir. Ancak saldırganlar yeni sunucular veya proxyler kullanarak bu engeli aşabilirler.

Domain Names (Alan Adları):

Zararlı alan adlarını engellemek, saldırganların Command and Control (C2) sunucularını bozabilir. Alan adlarını değiştirmek, IP adreslerine göre daha zor olsa da, sofistike saldırganlar savunmaları aşmak için hızla yeni alan adları oluşturabilirler.

Network/Host Artifacts

Network: Saldırganların ağ üzerindeki gözlemlenebilir faaliyetleridir. Örnekler arasında URL desenleri, ağ protokollerine gömülü Command and Control (C2) bilgileri, belirgin HTTP User-Agent veya SMTP Mailer değerleri yer alır.

Host: Saldırganların sistemlerde bıraktığı izlerdir, Örneğin, belirli bir kötü amaçlı yazılım tarafından oluşturulduğu bilinen kayıt defteri anahtarları veya değerleri, dosyalar ve izinler gibi gözlemlenebilir kalıntılar dahildir.

Tools

Saldırganların amaçlarına ulaşmak için kullandığı yazılımlar. Örneğin hedefli oltalama (spear phishing) saldırıları için kötü amaçlı belgeler oluşturan araçlar, C2 bağlantısı kurmak için kullanılan arka kapılar (backdoor'lar), şifre kırıcılar ve diğer ana makine tabanlı araçlar bu kategoriye girer.

TTP's (Taktikler, Teknikler ve Prosedürler)

Saldırganların hedeflerine ulaşmak için izlediği yöntemlerdir. Keşif (reconnaissance) aşamasından veri sızdırmaya kadar tüm süreçleri kapsayan saldırı teknikleri ve uygulamalarını içerir.

Pyramid of Pain'nin Tehdit İstihbaratındaki Önemi

Tehdit İstihbaratını etkin şekilde kullanmanın nasıl mümkün olduğunu anlamada hayati öneme sahiptir. Hash değerleri ve IP adresleri gibi göstergeler otomatik olarak tespit edilip engellenebilir; ancak bunlar yalnızca kısa vadeli fayda sağlar. TTP'lerin belirlenmesi ve etkisiz hale getirilmesi, saldırgan davranışlarını derinlemesine anlamayı gerektirir fakat daha uzun süreli ve anlamlı koruma sağlar.

Pyramid of Pain Nasıl Çalışır?

Piramidin tepe noktalarına doğru tırmanıldığında durum bir her iki taraf için bir miktar daha fazla karmaşıklaşır. Saldırgan tarafın savunmayı geçmesi noktasında özel çaba sarfetmesi ve saldırısını özelleştirmesi gerekiyor. Piramidin tepesinde yer alan Tools ve TTP (Tactics, Techniques and Procedures) katmanlarındaysa savunma tarafının işi giderek zorlaşır.

Savunmanın ilk hatlarının saldırganlar tarafından geçildiği varsayımı altında saldırganların kullandığı araç veya dosyaların tespiti önem kazanır. Yara kuralları yardımıyla belirli zararlı yazılım karakteristiğine sahip araçların tespiti mümkün kılınabilmekte.

```
1 rule malware_detect
2 {
3     strings:
4         $m = "malware"
5         $z = "zararli"
6         $hex = { E2 34 A1 C8 23 FB }
7     condition:
8         any of them
9 }
```

Yukarıda gördüğümüz gibi basit bir yara kuralı ile text içeriği veya bir hex içeriği tespit edildiğinde alarm oluşabilmesi için basit bir kural kemiği yazdık. Yara kuralı bu şekilde zararlı aktiviteleri tespit edip alarmlar üretmek için kullanılır. Daha detaylı bilgi için [buraya tıklayınız](#).

Sonuç

Mitre ATT&CK matrislerini kullanarak saldırganlar gibi düşünebiliriz. Bu matrisler yolu ile bir saldırganın bir sisteme, sunucuya girdiği zaman amaçladığı hedefi az çok tahmin edebilir ve yapacağı hareketleri önceden kestirebiliriz. Bu şekilde oluşturacağımız sıkılaştırma yöntemleri ile sisteme sızma girişiminde bulunan saldırganın işini zorlaştıracak adımlarla sıkı güvenlik politikaları ile düzenli eğitilmiş şirket çalışanları ile güvenliğini koruyabiliriz. Güvenlik önlemimizi sıkı alamadığımız senaryo için Pyramid of Pain modülü ile bir saldırganın verebileceği zararları tespit edip, sistemi veya sunucuyu tahrip ederken hangi aşamada olduğunu anlayabilir ve müdahale süreçlerini bu anlamlara göre yapabiliriz.

Kaynakça

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

<https://medium.com/@dusiber/mitre-att-ck-9c8a66d9b46f>

<https://cyberartspro.com/mitre-attack-framework-nedir/>

<https://www.securefors.com/mitre-attack-framework-nedir/>

<https://attack.mitre.org/resources/learn-more-about-attack/training/threat-hunting/>

<https://www.mitre.org/sites/default/files/2021-11/prs-19-3892-ttp-based-hunting.pdf>

<https://www.ibm.com/think/topics/threat-hunting>

<https://www.geeksforgeeks.org/cyber-attack-life-cycle/>

<https://quzara.com/blog/pyramid-of-pain-threat-intelligence>

<https://medium.com/@kofrathur/pyramid-of-pain-updated-tryhackme-walkthrough-ee0782b98273>

<https://www.attackiq.com/glossary/pyramid-of-pain/>

<https://github.com/Yara-Rules/rules>

<https://ciroglu.org/2021/06/23/olay-mudahalesi-sureclerinde-ioc-tespiti-the-pyramid-of-pain-yara-rules-loki/>