ALTAY TAKIMI

MITRE ATT&CK FRAMEWORK RAPORU

Hazırlayan : Efe Körün

Tarih : 07.02.2025

GİRİŞ

Siber güvenlik dünyasında, saldırganların sürekli gelişen taktikleri karşısında savunma mekanizmalarını güçlendirmek ve tehditlere karşı proaktif bir duruş sergilemek kritik öneme sahiptir. Bu noktada, MITRE ATT&CK Framework, siber güvenlik uzmanları için vazgeçilmez bir kaynak ve rehber niteliği taşımaktadır.

Bu raporun amacı, siber güvenlik alanında yaygın olarak kullanılan MITRE ATT&CK Framework'ü kapsamlı bir şekilde incelemektir. Rapor, framework'ün ne olduğunu, neden önemli olduğunu, temel bileşenlerini ve siber güvenlik operasyonlarında nasıl kullanıldığını açıklamayı hedeflemektedir.

MITRE ATT&CK Framework Nedir?

MITRE ATT&CK Framework'ü, siber güvenlik alanında saldırganların kullandığı taktikleri, teknikleri ve ortak bilgiyi tanımlamak için kullanılan bir bilgi tabanıdır. MITRE Corporation tarafından geliştirilmiştir. Framework, savunma ve saldırı taraflarına, güvenlik uzmanlarına ve siber güvenlik araştırmacılarına yardımcı olmak için tasarlanmıştır.

MITRE ATT&CK Framework'un temel amacı, savunma taraflarının saldırganların kullanabileceği taktikleri ve teknikleri anlamalarına ve siber saldırılarla mücadele ederken daha etkili olmalarına yardımcı olmaktır. Bu şekilde, güvenlik uzmanları ve kurumlar, siber saldırılara karşı daha iyi savunma stratejileri geliştirebilir ve olası saldırıları tespit ve önleme konusunda daha proaktif bir tutum alabilirler.

MITRE ATT&CK Framework Neden Önemlidir?

Ortak Dil: Siber güvenlik uzmanları arasında ortak bir oluşturur. Tehditleri ve saldırı davranışlarını tanımlamak ve iletişim kurmak için standart bir referans sunar. Bu, farklı güvenlik ekipleri, organizasyonlar ve hatta ülkeler arasında işbirliğini kolaylaştırır.

Tehdit İstihbaratı Geliştirme: Tehdit istihbaratı çalışmalarını yapılandırır ve iyileştirir. Bilinen tehdit aktörlerinin (APT grupları, siber suç örgütleri vb.) kullandığı taktik ve teknikleri analiz etmek ve profillerini oluşturmak için kullanılır. Bu sayede, gelecekteki saldırıları tahmin etmeye ve önlemeye yardımcı olur.

Güvenlik Açığı Değerlendirmesi ve Red Team Operasyonları: Güvenlik açıklarını ve zayıflıklarını test etmek için kırmızı takım operasyonlarında ve güvenlik açığı değerlendirmelerinde rehberlik eder. Saldırganların gerçek dünyadaki taktik ve tekniklerini simüle ederek, savunma mekanizmalarının etkinliğini ölçmeye ve iyileştirmeye olanak tanır.

Savunma Geliştirme ve Saldırı Tespiti: Savunma stratejileri geliştirmek ve tespit yeteneklerini güçlendirmek için temel oluşturur. Hangi tekniklere karşı savunmasız olunduğunu belirleyerek, öncelikli güvenlik yatırımlarının yapılmasını ve etkili detection kurallarının oluşturulmasını sağlar.

Olay Müdahale ve Adli Bilişim: Olay müdahale süreçlerinde ve adli bilişim analizlerinde yol gösterir. Bir saldırı olayının hangi taktik ve tekniklerle gerçekleştirildiğini belirleyerek, olayın kapsamını anlamaya, etkilenen sistemleri tespit etmeye ve iyileştirme çalışmalarına yardımcı olur.

Risk Yönetimi: Kuruluşların risk yönetimi süreçlerine katkıda bulunur. Hangi tür saldırıların en olası ve en etkili olduğunu anlamak, riskleri önceliklendirmeye ve uygun güvenlik kontrollerini uygulamaya yardımcı olur.

MITRE ATT&CK Framework Taktik ve Tekniklerin Önemi

Mitre Atak Framework'de bulunan taktik ve teknikler, siber güvenlik savunmasının her aşamasında kritik bir rol oynar. Bunların önemini şu şekilde özetleyebiliriz:

Taktikler: Saldırı yaşam döngüsünün aşamalarını anlamamızı sağlar. Bir saldırının hangi aşamada olduğunu belirlemek, olayın ciddiyetini ve potansiyel etkisini anlamak için önemlidir. Örneğin, "Initial Access" taktiği, saldırının başlangıcında olduğunu gösterirken, "Data Exfiltration" taktiği, saldırının kritik bir aşamasında olduğunu ve hassas verilerin tehlikede olduğunu gösterir. Bu aşamaları bilmek, olay müdahale ekiplerinin hızlı ve etkili bir şekilde yanıt vermesine yardımcı olur.

Teknikler: Saldırganların kullandığı spesifik yöntemleri ve araçları anlamamızı sağlar. Hangi tekniklerin kullanıldığını bilmek, saldırının nasıl gerçekleştiğini ve hangi güvenlik kontrollerinin aşıldığını anlamak için önemlidir. Örneğin, "Phishing" tekniğinin kullanıldığını bilmek, kullanıcı eğitimlerinin ve e-posta güvenlik önlemlerinin güçlendirilmesi gerektiğini gösterir. "Credential Dumping" tekniğinin kullanıldığını bilmek, kimlik yönetimi ve erişim kontrolü politikalarının gözden geçirilmesi gerektiğini gösterir. Bu teknikleri bilmek, daha spesifik ve etkili savunma önlemleri geliştirmeye olanak tanır.

Taktik ve tekniklerin sürekli olarak güncellenmesi ve yeni saldırı davranışlarının framework'e eklenmesi, Mitre Atak Framework'ü dinamik ve güncel bir kaynak haline getirir. Bu da siber güvenlik uzmanlarının en son tehditlere karşı hazırlıklı olmasına yardımcı olur.

TTP Nedir?

TTP, "Tactics, Techniques, and Procedures" kelimelerinin kısaltmasıdır. Siber güvenlik bağlamında, TTP'ler, belirli bir tehdit aktörünün veya saldırgan grubunun karakteristik davranışlarını tanımlamak için kullanılır.

Taktikler: Saldırganın genel stratejik hedeflerini (neden saldırıyor?)

Teknikler: Saldırganın taktik hedeflerine ulaşmak için kullandığı yöntemler (nasıl saldırıyor?)

Prosedürler: Saldırganın teknikleri uygularken izlediği adımlar, kullandığı araçlar ve belirli uygulamalar (nasıl uyguluyor?

TTP'ler, tehdit aktörlerini birbirinden ayırt etmek ve belirli saldırı kampanyalarını tanımlamak için de önemlidir. Örneğin, bir APT grubunun TTP'leri, kullandıkları özel taktikler, teknikler genellikle belirli kalıplar ve karakteristik özellikler gösterir.

TAKTİKLER

Initial Access (İlk Erişim): Bu taktik, saldırganların hedef ağa veya sistemlere ilk erişimi sağladıkları aşamayı ifade eder. Saldırganlar genellikle başlangıçta açıkları veya zayıflıkları kullanarak bu erişimi elde ederler.

Araçlar: Metasploit, Cobalt Strike, Social Engineering Toolkit (SET)
Örnekler: Spear phishing, Exploit Public-Facing Application

Execution (Yürütme): Bu aşama, saldırganların kötü niyetli kodları çalıştırmak veya sistemlerde işlem yapmak için kullanabilecekleri yöntemleri içerir. Saldırganlar genellikle komut satırı araçlarını veya betik dillerini kullanarak bu aşamada işlem yaparlar.

Araçlar: PowerShell, Command Prompt, Shell Scripting
Örnekler: Command-Line Interface, Scripting

Persistence (Kalıcılık): Saldırganlar, erişim sağladıkları sistemde kalıcı olmak için çeşitli teknikleri kullanır. Bu, sistem yeniden başlatıldığında veya güncellendiğinde erişimi sürdürmek için yapılan işlemleri içerir.

Araçlar: Windows Registry, Windows Task Scheduler, Cron
Örnekler: Registry Run Keys/Startup Folder, Scheduled Task

Privilege Escalation (Yetki Yükseltme): Saldırganlar, elde ettikleri düşük seviyeli erişim haklarını yüksek seviyeli erişim haklarına yükseltmek için yöntemler ararlar. Bu, genellikle sistem veya ağ üzerinde daha fazla kontrol sağlamak için yapılır.

Araçlar: Mimikatz, Windows Credential Editor, PowerUp
Örnekler: Exploitation of Vulnerability, Access Token Manipulation

Defense Evasion (Savunma Kaçınılması): Saldırganlar, algılanmayı veya engellenmeyi önlemek için savunma mekanizmalarını atlatmaya çalışırlar. Bu, izleme, tespit veya engelleme çabalarından kaçınmak için yapılan çeşitli teknikleri içerir.

Araçlar: Process Hacker, ProcDump, Process Explorer
Örnekler: File Deletion, Process Injection

Credential Access (Kimlik Bilgisi Erişimi): Saldırganlar, kullanıcı kimlik bilgilerini (örneğin, şifreleri veya oturum açma verilerini) elde etmek için yöntemler kullanır. Bu, doğrudan kimlik bilgilerini çalmak veya depolanan kimlik bilgilerine erişmek olabilir.

Araçlar: Mimikatz, LaZagne, Keystroke Logging Software
Örnekler: Credential Dumping, Keylogging

Discovery (Keşif): Saldırganlar, hedef ağ veya sistemleri keşfetmek ve üzerinde çalışmak için bilgi toplama sürecine girerler. Bu, sistem yapılandırması, ağ topolojisi veya kullanıcı bilgileri gibi bilgilerin elde edilmesini içerir.

Araçlar: Nmap, Windows Management Instrumentation (WMI), Bloodhound
Örnekler: Network Scanning, System Information Discovery

Lateral Movement (Yanal Hareket): Saldırganlar, erişim elde ettikleri bir sistemden diğer sistemlere veya ağ içinde hareket etmeye çalışırlar. Bu, saldırganın eriştiği bir sistemden başka bir sisteme yayılma çabalarını ifade eder.

Araçlar: PsExec, Bloodhound, CrackMapExec (CME)
Örnekler: Remote Desktop Protocol, SMB/Windows Admin Shares

Collection (Toplama): Saldırganlar, hedef sistem veya ağdan veri veya bilgi toplamak için çeşitli yöntemleri kullanırlar. Bu, duyarlı verilerin veya kullanışlı bilgilerin toplanmasını içerir.

Araçlar: FTK Imager, Wireshark, Snort
Örnekler: Data from Local System, Data from Network Shared Drive

Exfiltration (Dışa Aktarma): Saldırganlar, hedef sistem veya ağdan topladıkları verileri dışarıya çıkarmak için yöntemler kullanır. Bu, çalınan verilerin bir dış sunucuya aktarılmasını içerir.

Araçlar: FTP, DNS Tunneling, HTTP/S
Örnekler: Exfiltration Over Command and Control Channel

Impact (Etki): Saldırganlar, sistemlere veya ağlara zarar vermek veya hizmetleri kesintiye uğratmak için çeşitli yöntemler kullanabilirler. Bu, genellikle kötü amaçlı yazılımın kullanılmasıyla gerçekleşir.

Araçlar: SDelete, Diskpart, rm (Unix/Linux)
Örnekler: Data Destruction, Disk Wipe

TEKNİKLER

Bir saldırı sırasında saldırganlar tek bir teknikle sınırlı kalmazlar. Genellikle, hedef sistemin veya ağın güvenlik önlemlerine bağlı olarak farklı teknikleri bir arada kullanarak saldırıyı daha etkili hale getirirler.

Her taktik altında birçok teknik yer almakta olup, saldırganlar saldırının gidişatına ve karşılaştıkları engellere göre farklı teknikleri kombine edebilirler. Bu yüzden siber güvenlik uzmanları, yalnızca saldırı taktiklerini değil, aynı zamanda bu taktikleri gerçekleştirmek için kullanılan teknikleri de detaylı bir şekilde incelemelidir.

TTP-Based Threat Hunting Nedir?

Tehdit avcılığı, kuruluşların ağlarında ve sistemlerinde gizlenen tehditleri proaktif olarak arama sürecidir . Geleneksel güvenlik önlemlerinin tespit edemediği saldırıları ortaya çıkarmayı ve saldırganların sistemlere sızmış olabileceğine dair işaretleri aramayı amaçlar . TTP tabanlı tehdit avcılığı ise, saldırganların bilinen TTP'lerini kullanarak tehditleri tespit etmeye odaklanır. Bu yaklaşım, saldırganların davranışlarını anlamaya ve saldırı yaşam döngüsünün erken aşamalarında tehditleri belirlemeye yardımcı olur.

MITRE ATT&CK Framework'ü, saldırganların kullandığı taktikleri ve teknikleri anlamak, hangi olayların araştırılması gerektiği ve hangi göstergelerin aranması gerektiği konusunda bilinçli kararlar almak konusunda yardımcı olur.

Örneğin, bir threat hunter, "Persistence" taktiği altında listelenen teknikleri inceleyerek saldırganların sistemlerde kalıcılık sağlamak için kullandığı yaygın yöntemleri öğrenebilir ve bu bilgilere dayanarak ağda ilgili olayları arayabilir.

TTP'lere dayalı Threat Hunting'in avantajları:

Proaktif Yaklaşım: Saldırganlar saldırılarına başlamadan önce tehditleri belirlemeyi sağlar.

Hedefli Arama: Bilinen TTP'lere odaklanarak daha verimli ve etkili tehdit avcılığı yapılmasını sağlar.

Erken Tespit: Saldırı yaşam döngüsünün erken aşamalarında tehditleri tespit ederek hasarı en aza indirir.

Sürekli İyileştirme: Tehdit avcılığı sürecinde elde edilen bilgiler, güvenlik duruşunu güçlendirmek ve gelecekteki saldırıları önlemek için kullanılabilir.

TTP-Based Detection Engineering Nedir?

TTP tabanlı tespit mühendisliği, saldırganların bilinen TTP'lerini kullanarak saldırıları tespit etmek için daha etkili ve verimli yöntemler geliştirmeyi amaçlar. MITRE ATT&CK çerçevesi, tespit mühendislerine saldırıların tespit edilmesini otomatikleştirmede ve iyileştirmede yardımcı olur.

Saldırganların kullandığı taktikleri ve teknikleri anlamak, tespit mühendislerinin daha doğru ve kapsamlı tespit kuralları oluşturmalarına olanak tanır.

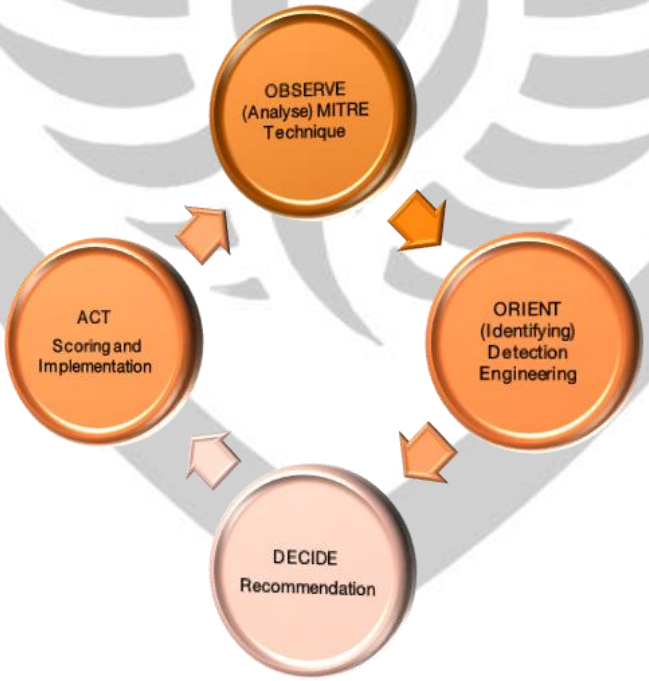
Örneğin, detection engineer, "Credentials Acces" taktiği altında listelenen teknikleri inceleyerek saldırganların kimlik bilgilerini çalmak için kullandığı yöntemleri öğrenebilir ve bu bilgilere dayanarak ilgili olayları tespit etmek için kurallar oluşturabilir.

TTP'lere dayalı Detection Engineering'in avantajları:

Gelişmiş Tespit: Saldırganların bilinen TTP'lerine odaklanarak daha doğru ve kapsamlı tespit kuralları oluşturulmasını sağlar.

Proaktif Savunma: Saldırıları erken aşamalarda tespit ederek yayılmasını ve hasarını önler.

Sürekli Geliştirme: Yeni tehditler ortaya çıktıkça tespit kuralları güncellenerek güvenlik duruşu sürekli olarak iyileştirilebilir.



Giriş

Bu rapor, 2022 yılında Ukrayna'nın elektrik dağıtım altyapısını hedef alan ve MITRE ATT&CK çerçevesinde C0034 olarak sınıflandırılan, Rusya ile bağlantılı olduğu bildirilen Sandworm adlı APT grubu tarafından gerçekleştirilen siber saldırıyı derinlemesine incelemektedir. Saldırının arka planı, amaçları, kullanılan teknikler, bu tekniklerin MITRE ATT&CK TID (Technique ID) karşılıkları, saldırının etkileri ve gelecekte benzer saldırılara karşı alınması gereken önlemler detaylı bir şekilde analiz edilmiştir.

Arka Planı Ve Olası Sebepleri

Ukrayna, 2014 yılında Kırım'ın ilhakı ve Donbass bölgesindeki çatışmaların başlamasından bu yana, Rusya ile hem fiziksel hem de siber alanda gergin bir ilişki içerisindedir. Siber alem, bu çatışmanın önemli bir cephesi haline gelmiş ve Ukrayna, Rusya kaynaklı olduğu değerlendirilen bir dizi siber saldırının hedefi olmuştur. Bu saldırılar, sadece devlet kurumlarını ve özel sektörü değil, aynı zamanda ülkenin kritik altyapılarını da hedef almıştır.

Ukrayna’nın Kritik Altyapılarına Yönelik Bazı Siber Saldırılar

2015 Ukrayna Elektrik Kesintisi: Bilinen ilk siber saldırı kaynaklı elektrik kesintisi, Ukrayna'da 230.000 kişiyi etkiledi. Saldırganlar, BlackEnergy zararlı yazılımını kullanarak elektrik dağıtım sistemlerine sızdı. Amaç, sistemleri devre dışı bırakarak geniş çaplı bir kesintiye yol açmaktı.

2016 Ukrayna Elektrik Kesintisi: Kiev'de yaşanan bu kesintide, Industroyer/CrashOverride adlı özel bir zararlı yazılım kullanıldı. Bu yazılım, endüstriyel kontrol sistemleriyle doğrudan etkileşime geçebiliyordu. Bu durum, kritik altyapıların siber saldırılara karşı ne kadar savunmasız olduğunu gösterdi.

2017 NotPetya Saldırısı: NotPetya, fidye yazılımı gibi görünse de, aslında verileri silmeyi hedefleyen yıkıcı bir saldırıydı. Ukrayna'daki bankalar, havaalanları ve enerji şirketleri başta olmak üzere dünya çapında birçok sektörü etkiledi. Bu saldırı, siber saldırıların küresel çapta yol açabileceği zararları gözler önüne serdi.

2022 Saldırısının Bağlamı

2022'deki elektrik santrali saldırısı, Rusya'nın Ukrayna'yı işgalinin hemen öncesinde ve işgalin ilk günlerinde gerçekleşti. Bu zamanlama, saldırının sadece teknik bir siber saldırı olmadığını, aynı zamanda daha geniş bir askeri ve siyasi stratejinin parçası olduğunu göstermektedir. Saldırı, Ukrayna'nın direncini kırmayı, altyapısını felç etmeyi ve halk arasında kaos yaratmayı amaçlayan bir güç gösterisi olarak değerlendirilebilir.

Saldırının Zaman Çizelgesi

Saldırı, Sandworm Ekibi'nin Haziran 2022'de veya daha önce kurbanın ağına sızmasıyla başladı. Ekip, internet erişimli bir sunucuya Neo-REGEORG web kabuğunu yerleştirerek ağda kalıcılık sağladı. Saldırganlar, muhtemelen üç aya kadar SCADA sistemine erişim sağladı. 10 Ekim 2022'de saldırganlar, trafo merkezlerini kapatmak için kötü amaçlı kontrol komutları çalıştırmak amacıyla "a.iso" adlı bir optik disk görüntüsünü kullanarak yerel bir MicroSCADA ikili dosyasını çalıştırdı. 12 Ekim 2022'de saldırganlar, CaddyWiper kötü amaçlı yazılımını dağıtarak ve çalıştırarak BT sistemlerinde veri imhası gerçekleştirdi.

Tanktrap	Windows Grup İlkesi'ni kullanarak CaddyWiper'ı dağıtan ve başlatan bir PowerShell yardımcı programı.
CaddyWiper	Sürücüleri ve dosyaları silen bir kötü amaçlı yazılım . CaddyWiper, bulaştığı sistemin boot yapısını bozarak sistemin yeniden başlatılmasını engeller, bazı dosyaların üzerine yazarak bozar, kritik altyapılarda kullanılan bazı paket programların sistemde çalışan servislerini silmeye çalışır ve bulaştığı sistemde izini yok etmeye çalışır. Ayrıca, CaddyWiper'ın içinde sisteme daha sonra tekrar arka kapıdan giriş sağlayabilecek SSH servisi bulunur .
GOGETTER	Harici sunucularla TLS tabanlı bir "Yamux" C2 kanalı kurmak için kullanılan bir tünelleyici yazılımı.
Neo-REGEORG	İnternet erişimli bir sunucuda dağıtılan bir web kabuğu.
SCIL-API	SCADA komutlarını yürütmek için kullanılan bir API.
MicroSCADA	Saldırıda hedef alınan SCADA sistemi.

Saldırıda Kullanılan Teknikler

2022 Ukrayna Elektrik Gücü Saldırısı'nda Sandworm Ekibi, sisteme erişim sağlamak ve SCADA sistemlerinden yetkisiz komutlar göndermek için gelişmiş bir dizi TTP'ler kullanmıştır.

T1059.001 Command and Scripting Interpreter: PowerShell

Sandworm Ekibi, TANKTRAP adlı bir PowerShell aracını kullanarak, Windows Grup İlkesi aracılığıyla bir veri silme(data wiper) yazılımı yaydı ve çalıştırdı.

T1543.002 Create or Modify System Process

Sandworm Ekibi, GOGETTER adlı zararlı yazılımın sistemde kalıcı olmasını sağlamak için Systemd'i yapılandırdı. Bunu yaparken, "WantedBy=multi-user.target" ayarını kullanarak GOGETTER'ın *giriş ekranından hemen önce* otomatik çalışmasını sağladı.

T1485 Data Destruction

Sandworm Ekibi, kurbanın BT ortamındaki sistemlerine CaddyWiper adlı zararlı yazılımı yerleştirdi ve bu yazılım endüstriyel kontrol sistemleri ile ilgili dosyaları, ayrıca ağ üzerindeki ve fiziksel sürücüdeki bölümleri silmek için kullanıldı.

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

Sandworm Ekibi, Windows'un Grup İlkesi özelliğini suistimal etti. Normalde yöneticilerin kullandığı bu özellik, hackerlar tarafından virüsleri ağdaki birçok bilgisayara hızla yaymak için kullanıldı. Bu, saldırının etkisini büyüterek sistemlere zarar verme veya kontrolü ele geçirme amacı taşıyordu.

T1570 Lateral Tool Transfer

Sandworm Ekibi, Ukrayna elektrik şebekesi saldırısında, CaddyWiper virüsünü (sahte msserver.exe adıyla) önce kendi sunucularında hazırladı. Sonra, Windows'un Grup İlkesi (GPO) özelliğini kullanarak, bu virüsü ağdaki birçok bilgisayarın sabit diskine kopyaladı. Bu sayede, virüsü merkezi bir noktadan birçok bilgisayara aynı anda yayarak, daha sonra çalıştırıp büyük hasar verdiler. GPO kullanmaları, saldırının etkisini artırdı.

T1036.004 Masquerading: Masquerade Task or Service

Sandworm Ekibi, Ukrayna elektrik şebekesi saldırısında GOGETTER virüsünü, Linux sistemlerdeki Systemd'i kullanarak, zararsız bir sistem hizmeti gibi göstererek gizledi. Bu, virüsün fark edilmeden çalışmasını sağladı.

T1095 Non-Application Layer Protocol

Sandworm Ekibi, ele geçirdiği bilgisayarlarla C2 erişimini normal internet trafiği gibi göstermek için TLS şifrelemesi ve proxy sunucular kullanmıştır. Böylece güvenlik sistemlerini atlatıp, arka planda virüslü bilgisayarlarla haberleşmiştir.

T1572 Protocol Tunneling

Sandworm Ekibi, ele geçirdikleri bilgisayarlarla gizlice ve güvenli bir şekilde iletişim kurmak için GOGETTER adlı yazılımla, normalde güvenli web sitelerinin de kullandığı TLS şifrelemesiyle korunan bir "tünel" oluşturdular. Bu tünel, "Yamux" adı verilen özel bir protokolü kullanıyordu. Bu tünel, internetteki kendi sunucularıyla gizli iletişim kurmalarını ve güvenlik sistemlerini atlatmalarını sağladı.

T1053.005 Scheduled Task/Job: Scheduled Task

Sandworm Ekibi, CaddyWiper adlı silici virüsü belirli bir anda çalıştırmak için akıllıca bir yöntem kullandı. Windows'un "Zamanlanmış Görevler" özelliğini, Grup İlkesi Nesneleri (GPO'lar) aracılığıyla kullandılar. Yani, virüsün hemen değil, önceden belirledikleri bir zamanda otomatik olarak çalışmasını sağladılar. GPO'ları kullanmaları ise bu zamanlamayı ağdaki birçok bilgisayara aynı anda uygulamalarına olanak tanıdı.

T1505.003 Server Software Component: Web Shell

Sandworm Ekibi, santraldaki internete açık bir sunucuya sızdı ve bu sunucuya, Neo-REGEORG adında bir *web shell* yerleştirdiler. Bu web shell, saldırganlara sanki sunucunun başındaymış gibi uzaktan komut çalıştırma, dosyalara bakma ve diğer işlemleri yapma imkanı verdi. Bu, saldırganların sunucu üzerinde tam kontrol sahibi olmasını ve oradan ağın diğer kısımlarına sızmasını sağlayan kritik bir adımdı.

T0895 Autorun Image

Sandworm Ekibi, SCADA sunucularını kontrol eden bir sanal makineye sızdı. Bunu, zaten sahip oldukları hipervizör erişimini (sanal makineleri yönetme yetkisini) kullanarak yaptılar. a.iso adında, içinde kötü amaçlı bir VBS scripti bulunan özel bir ISO dosyası oluşturdular. Bu ISO dosyasını, sanki sanal makineye bir CD takmışlar gibi, sanal makineye bağladılar. Elektrik Santarlinin SCADA sunucusunun işletim sistemi, CD-ROM'ları otomatik olarak çalıştıracak şekilde ayarlandığı için ISO dosyası, bağlanır bağlanmaz içindeki kötü amaçlı VBS scriptini *otomatik olarak* çalıştırdı ve saldırganların sisteme sızmasını sağladı.

T0807 Command-Line Interface

Sandworm Ekibi, MicroSCADA platformunu kontrol etmek için bu platformun kendi komut satırı arayüzünü (CLI) kullandı. scilc.exe adlı bir exe aracılığıyla, SCIL-API'yi kullanarak komutlar gönderdiler. Bu, sanki MicroSCADA'nın kendi kontrol panelini kullanıyormuş gibi, sisteme doğrudan müdahale etmelerini sağladı. Yani, normal kullanıcıların grafik arayüzle yaptığı işlemleri hackerlar komut satırından yazılı komutlarla yaptılar.

T0853 Scripting

Sandworm Ekibi, MicroSCADA sistemine komut göndermek için dolambaçlı bir yol izledi ve birden fazla script kullandı. Önce, lun.vbs adlı bir Visual Basic scripti çalıştırdılar. Bu script ise, n.bat adlı bir batch dosyasını çalıştırdı. n.bat dosyası ise, *asıl* işi yapan, yani MicroSCADA'yı kontrol eden scilc.exe komutunu çalıştırdı. Bu karmaşık yapı, muhtemelen güvenlik sistemlerini atlatmak ve izlerini gizlemek için kullanıldı. Yani, tek bir büyük ve şüpheli program yerine, birbirini çağıran küçük ve daha az dikkat çekici script kullandılar.

T0894 System Binary Proxy Execution

Sandworm Ekibi, Hazırladıkları s1.txt adlı bir dosyaya, MicroSCADA'ya göndermek istedikleri komutları (örneğin, "şu kesiciyi aç", "bu kesiciyi kapat") yazdılar. Sonra, scilc.exe programına bu dosyayı okumasını ve içindeki komutları MicroSCADA'ya göndermesini söyleyen bir komut çalıştırdılar (C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt). Böylece, MicroSCADA'nın *kendi aracını* kullanarak, uzak trafo merkezlerine yetkisiz komutlar gönderdiler ve elektrik kesintisine neden oldular.

Wazuh-i Splunk Kardeşler Firması Siber Saldırı Senaryosu

İstanbul'un hareketli siber güvenlik dünyasında, Wazuh-i Splunk Kardeşler, adından söz ettiren bir firma haline gelmişti. Özellikle büyük ölçekli şirketlere ve kamu kurumlarına sundukları SIEM çözümleriyle tanınıyorlardı. Ancak bu başarı, siber alemin karanlık köşelerinde pusuda bekleyenlerin dikkatini çekmekten de geri kalmamıştı.

“1.5 İskender” olarak bilinen sinsi bir grup, siber casusluk ve bilgi hırsızlığı konusunda kötü bir şöhrete sahipti. Liderleri, kod adı "Şekerpare" olan gizemli bir figürdü. "Şekerpare", siber casusluk ve bilgi hırsızlığındaki acımasızlığıyla tanınırdı. Hedeflerinde ise, ironik bir şekilde, eski iş arkadaşının kurduğu siber güvenlik devi Wazuh-i Splunk Kardeşler vardı. Şekerpare, yıllar önce "Çatlak Kase" adlı küçük bir siber güvenlik şirketinden, etik sınırları zorlayan hırsları yüzünden kovulmuştu. Bu kovulma, içindeki intikam ateşini körüklemişti.

Wazuh-i Splunk Kardeşler’e sızmak, Şekerpare için sadece bir siber saldırı değil, kişisel bir hesaplaşmaydı. Aylar süren titiz bir keşif çalışması sonucunda, Wazuh-i Splunk Kardeşler’in dijital zırhındaki çatlağı buldular. Wazuh-i Splunk Kardeşler’in sistemlerine sızıp, hem bilgi çalacak hem de şirketi siber alemde küçük düşüreceklerdi. Şekerpare'nin intikamı, Wazuh-i Splunk Kardeşler için hiç de tatlı olmayacaktı.

Saldırı Aşamaları

Keşif (Reconnaissance):

Active Scanning - T1595: "Dürümcü" ekibi, Wazuh-i Splunk Kardeşler’in sistemlerini Nmap, Shodan ve benzeri araçlarla tarar. "Pide" v2.3 adlı eski bir eklentiyi tespit ederler.

Gather Victim Host Information - T1592: Wazuh-i Splunk Kardeşler çalışanlarının LinkedIn profilleri, sosyal medya hesapları incelenir. Sistem yöneticisinin kişisel e-postası ve "Kebap Severler" forumundaki paylaşımları belirlenir.

Kaynak Geliştirme (Resource Development):

Obtain Capabilities: Tool - T1588.002: "Pide" v2.3'teki zafiyeti (CVE-2025-12414) kullanmak için "Lahmacun" adlı exploit geliştirilir.

Develop Capabilities - T1587.001: "Lahmacun" Wazuh-i Splunk Kardeşler’in web sunucusuna sızıp yetki yükseltmeyi hedefler.

İlk Erişim (Initial Access):

Exploit Public-Facing - T1190: "Lahmacun" ile Pide zafiyeti tetiklenir, Wazuh-i Splunk Kardeşler’in web sunucusuna sızılır.

Spearphishing Attachment - T1193: Sistem yöneticisine " Wazuh-i Splunk Kardeşler Güvenlik Bülteni - Acil Güncelleme (Adana Kebap Hediye Kuponlu)" başlıklı, "Adana.doc" (kötü amaçlı makro içerir) e-postası gönderilir.

Yürütme (Execution):

Execution - T1204: Sistem yöneticisi eki açar ve makroyu etkinleştirir.

Command and Scripting Interpreter - T1059.001: "Ciğer" adlı PowerShell betiği çalışır.

Kalıcılık (Persistence):

Scheduled Task/Job - T1053.005: "Ciğer" kendini her gün belirli saatte çalışacak şekilde zamanlar.

Boot or Logon Initialization Scripts- T1547.001: "Ciğer" kendisinin bir kopyasını Windows başlangıç klasörüne atar.

Savunmadan Kaçınma (Defense Evasion):

System Binary Proxy Execution: Mshta T1218.010: "Ciğer" betiği Mshta.exe ile gizlenir.

Obfuscated Files or Information - T1027: "Ciğer" betiğinin kodu gizlenir.

Kimlik Bilgisi Erişimi (Credential Access):

OS Credential Dumping - T1003.001: "Tantuni" (Mimikatz benzeri) ile parola özetleri (hash'ler) ele geçirilmeye çalışılır.

Credentials In Files- T1081: Sunucu/geliştirici bilgisayarlarında parola/API anahtarı arama.

Keşif (Discovery):

System Information Discovery - T1082: systeminfo ile sistem bilgileri toplanır.

System Network Configuration Discovery - T1016: ipconfig /all ve netstat -ano ile ağ bilgileri toplanır.

Yanal Hareket (Lateral Movement):

Remote Services - T1021.002: RDP veya SSH ile diğer sistemlere erişim denemesi.

Lateral Tool Transfer - T1570: Tantuni aracı ve diğer yardımcı araçların ağ paylaşım alanları vasıtasıyla başka makinelere kopyalanması.

Toplama (Collection):

Automated Collection - T1119: "Ezme" adlı araçla dosyalar otomatik taranır ve kopyalanır.

Data from Local System - T1005: Hassas veriler doğrudan kopyalanır.

Komuta ve Kontrol (Command and Control):

Application Layer Protocol - T1071.001: "Şiş" adlı arka kapı HTTPS üzerinden C2 ile iletişim kurar.

Encrypted Channel: Asymmetric Cryptography - T1573.002: C2 iletişimi asimetrik şifreleme ile korunur.

Veri Sızdırma (Exfiltration):

Exfiltration Over C2 Channel - T1041: Veriler "Şiş" üzerinden C2 sunucusuna gönderilir.

Exfiltration Over Web Service: Exfiltration to Cloud Storage- T1567.002: Veriler bulut depolama servislerine yüklenir.

Etki (Impact):

Data Encrypted for Impact - T1486: "Urfa" fidye yazılımı dosyaları şifreler.

Defacement - T1491.001: 1.5 İSKENDER'in website içeriğini kendi mesajları ile değiştirmesi.

SONUÇ

Bu raporda, MITRE ATT&CK Framework'ün siber güvenlik alanındaki önemini, bileşenlerini ve kullanım senaryolarını detaylı bir şekilde inceledik. Framework'ün, tehdit aktörlerinin taktik ve tekniklerini analiz etmek, tehdit istihbaratını geliştirmek, güvenlik açıklarını değerlendirmek ve olay müdahale süreçlerini iyileştirmek gibi birçok alanda kritik bir rol oynadığı görülmüştür.
Araştırma sürecinde kazanılan bilgiler, MITRE ATT&CK'ün sadece bir bilgi tabanı olmanın ötesinde, siber güvenlik ekipleri için stratejik bir rehber niteliği taşıdığını göstermektedir. Bu framework'ün etkin bir şekilde kullanılması, kuruluşların siber tehditlere karşı daha hazırlıklı ve dirençli olmasını sağlayacaktır.