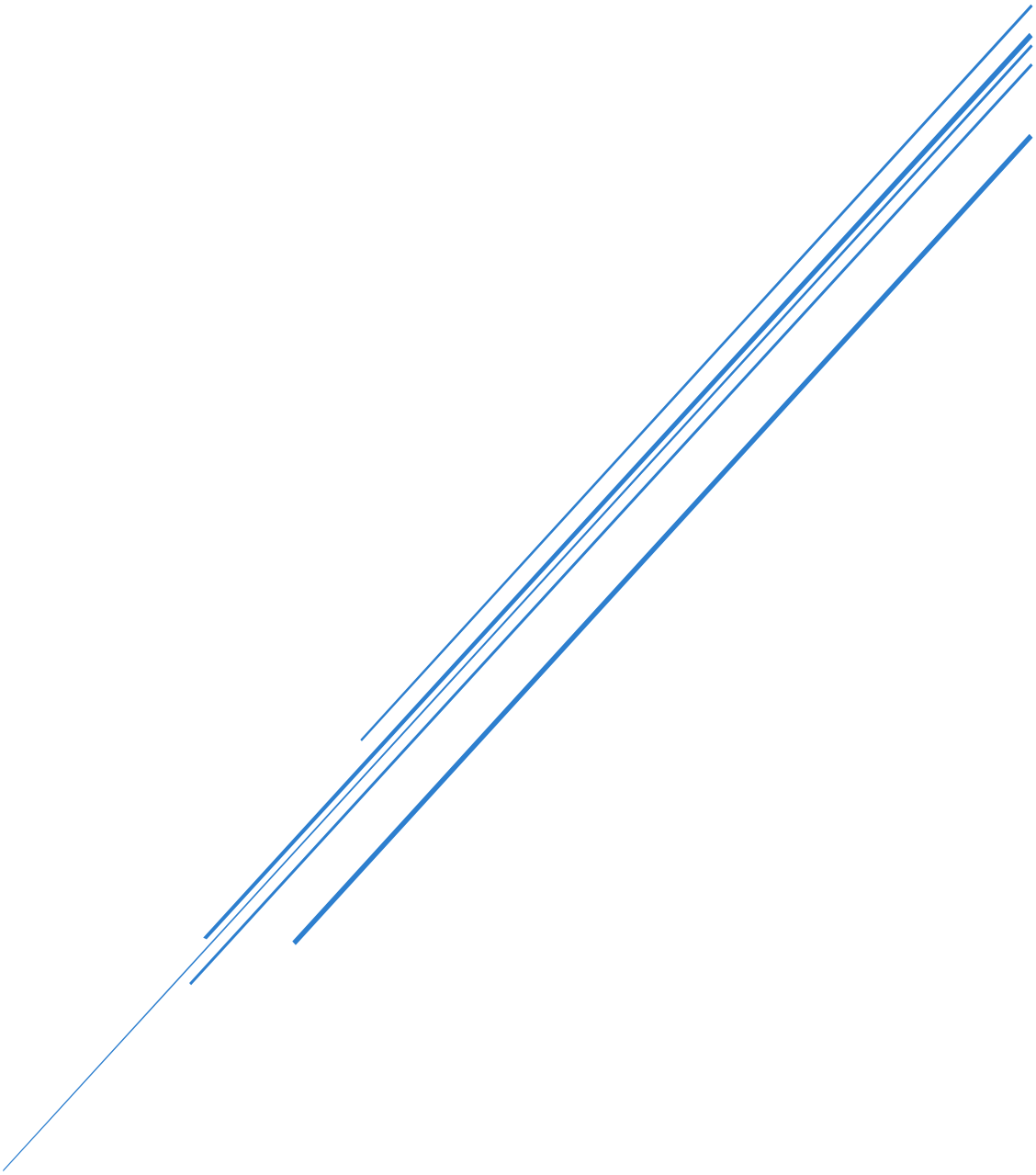
MITRE ATT&CK TTP VE PYRAMID OF PAIN

Hazırlayan: Emrecan Atlıhan

Tarih: 11.02.2025



İçindekiler

GİRİŞ

Günümüz siber güvenlik dünyasında yaşanılan gelişmeleri aynı anda takip etmek gerekiyor. Herhangi bir gelişmeden geri kalınma durumunda yaşanabilecek zafiyetler hem kendimizi hem de çalıştığımız şirketi risk altına alabilir. Saldırganlar her gün yeni bir teknik ile saldırı gerçekleştirebilirler. Bunun yanı sıra eski teknikleri de kullanabilirler. Bunları takip etmek amacıyla analistler belli birkaç standart belirlediler. Sadece takip etmek amacıyla da kalmadı yaratılan standartlar. Saldırıların açıklanmasında da etkili oldular. Ayrıca bu saldırıların açıklanmasında da kolaylık sağladılar. Bir saldırının keşif aşamasında kullanılan taktiği (nmap taraması vs.) belli bir teknik adı vererek raporlamada kolaylıklar sağlandı. Bu taktik ve tekniğin bir yerde toplanarak tam olarak yaratılan standart ise MITRE ATT&CK oldu. Giriş sayfasında da başlıkta gördüğünüz gibi raporun içeriğinde bugün bu standarttan bahsedip amacını anlatacağız. Bunlara ek olarak başlıkta bahsettiğimiz TTP ve Pyramid of Pain ile ilgili de kısa bir özet geçelim. TTP, taktik teknik ve prosedür olarak geçer. Pyramid of Pain ise saldırganın amacını ne kadar engelleyip ona vereceğimiz zorlukların bir sıralamasıdır. Daha detaylı bir şekilde aşağıda bunlardan bahsedeceğim. Bu raporda MITRE ATT&CK tablosunu öğrenmek, TTP ve Pyramid of Pain'in ne işe yaradığını okuyana aktarmayı amaçlıyoruz.

MITRE ATT&CK

Öncelikle MITRE'den bahsedelim. Amerika'da 1958 yılından ulusal güvenliği ilertletmek amacıyla kamu yararına hizmet etmek ve bağımsız bir danışmanlık için yenilikçi çözümler üreten bir kuruluştur. Siber güvenlik, yapay zekâ ve makine öğrenmesi, sağlık, Telekom ve anayurt güvenliği gibi konularda da hizmet vermektedir.

MITRE ATT&CK Framework nedir?

Adversarial tactics, techniques ve Common Knowledge olarak açılımı olan MITRE ATT&CK, 2013 yılında kurulan ve sürekli gelişmeye devam eden bir saldırı teknikleri veri tabanıdır. Bu kaynak bize saldırıların sistemli bir şekilde analiz edilmesine kaynak sağlar. Aşama aşama yapılan saldırılarda kullanılan taktikleri detaylı bir şekilde kategorize etmemize olanak sunar.

SOC analistleri için bu tablo önemlidir. Bunun nedeni savunmayı bilmek için biraz da saldırı bilmeniz lazım. Bir siber saldırının her adımı burada detaylı bir şekilde anlatılıyor. Anlatmakla da kalmıyor önleme yollarından da bahsediyor. Hatta tekniğin kullanıldığı siber saldırılar hakkında da bilgiler veriyor.

MATRIX

Matriksler atak yollarının görselleştirilme metodu ile kategorize edilip anlaşılma konusunda kolaylık sağlanması amacıyla yapılmıştır.

Üç tane matriks vardır. Bunlar:

1- Enterprise Matris
2- Mobil Matris
3- ICS (Endüstriyel Kontrol Sistemleri) Matris

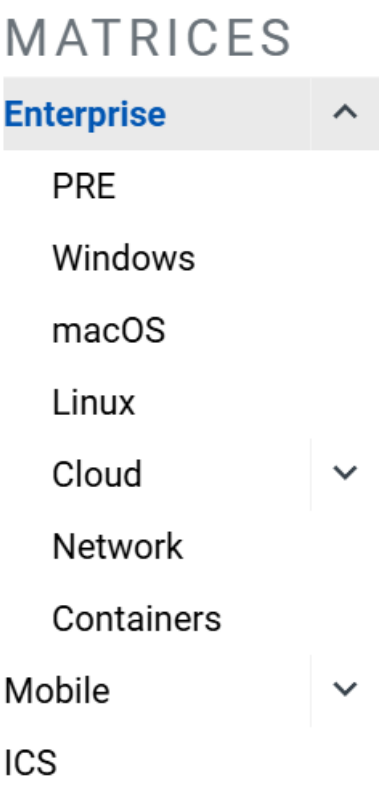
Bugün sadece Enterprise Matrise bakarak incelemelerde bulunacağız.

ENTERPRISE MATRİKS

Enterprise matriks MITRE tarafından yaratılan ilk matrikstir. İçinde daha çok dijital sistemler hakkında bilgi taşır. Diğer matrislere oranla içinde daha çok bilgi bulundururlar. Matriksin asıl kullanım amacı büyük organizasyonlara yapılan siber saldırıları anlamaya yöneliktir.

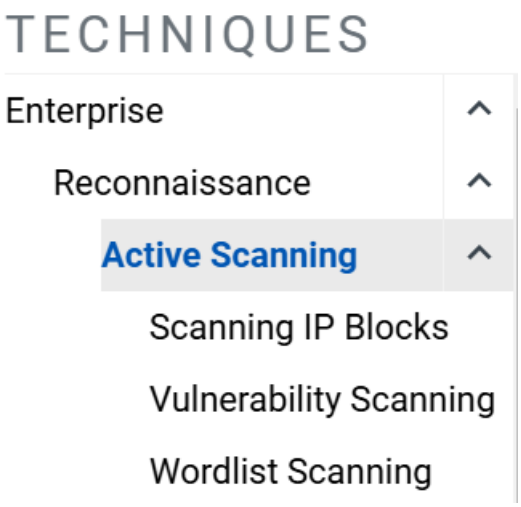
Bu matrisin altında sub-matricies olarak belirtilen 7 tane alt bulunur. Bunlar:

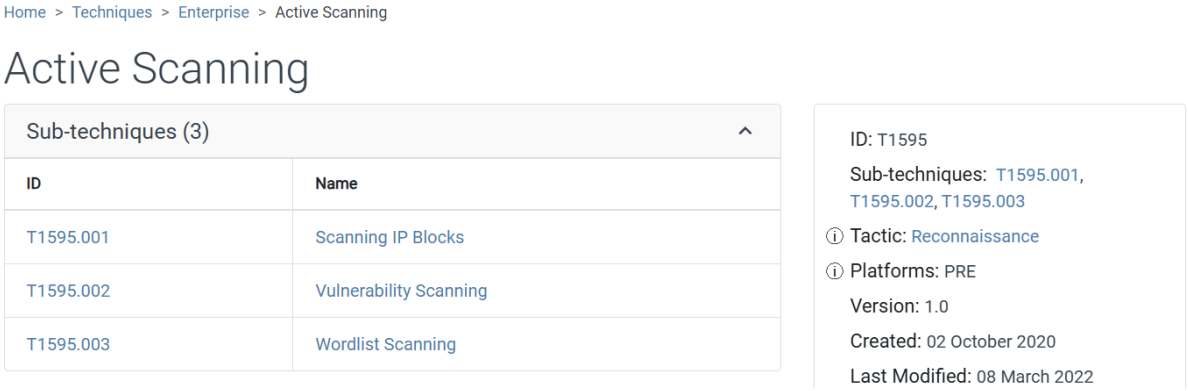
1. PRE
2. Windows
3. macOS
4. Linux
5. Cloud
6. Network
7. Containers



MITRE ATT&CK TEKNİKLERİ NEDİR VE NEDEN ÖNEMLİDİR?

Enterprise matrikse girdiğimizde karşımıza birkaç taktik ve teknikler çıkar. Bu taktikler en başta gözüken başlıktakilerdir altında kalan kısım ise sub-teknik olarak karşımıza çıkar. Örnek olarak verilmek istenilirse şudur:





Gördüğünüz gibi “Recoinassance” bölümünün altında kalan Active Scaninng tekniğinin 3 tane sub-tekniği olduğunu görürüz. Diğer bölümlerde de bunlara bakarak kendinizi geliştirebilirsiniz.

Kısaca teknik ve sub-tekniklerden bahsettik. Peki bu “Reconnaissance” gibi en başta görülen başlıklar ne için var? 14 tane olan bu başlıklara hızlıca göz gezdip ne anlama geldiğine bakalım.

- Reconnaissance

  Saldırganın saldırıyı başlatmadan yapacağı keşif aşaması.

- Resource Development

  Saldırganın saldırıyı yapabilmesi için bazı araç vb. satın alınması.

- Initial Access

  İlk dokunuş veya temas olarak adlandırdığımız burada saldırgan kurbanı ile ilk dokunuşu yapar. Buna oltalama e postaları örnek verilebilir.

- Execution

  Gönderilen zararlının ilk çalışması burada gerçekleşir.

- Persistence

  Kalıcılık olarak adlandırdığımız burada saldırgan görev zamanlayıcısı, servisler ya da kendine has bir kullanıcı yaratarak sistemde kalıcılık sağlamaya çalışır.

- Privilege Escalation

  Burada saldırgan daha yüksek yetkilere geçiş yapmaya çalışır.

- Defense Evasion

  Anti virüslerden kaçınmak için burada saldırgan kodlarını şifreleyebilirler. Ekstra olarak masum bir işlemin içine sızarak kendi işlemlerini de çalıştırabilirler.

- Credential Access

  Kullanıcı adı ve şifre çalmak gibi düşünülebilir.

- Discovery

  Sızdıktan sonra saldırganlar ağda kimlerin olduğunu öğrenmek için keşif yaparlar.

- Lateral Movement

  Ağdaki kişiler öğrenildikten sonra onlara erişim sağlamak diye adlandırılabilir.

- Collection

  Saldırganın sızdırmak istediği dosyaların toplamıdır. Bazen e postalar sesler videolar yer alır. 2 adım sonrası için kullanılmak istenilebilir.

- Command and Control

  Komuta ve Kontrol, düşmanların bir kurban ağı içinde kendi kontrolleri altındaki sistemlerle iletişim kurmak için kullanabilecekleri tekniklerden oluşur.

- Exfiltration

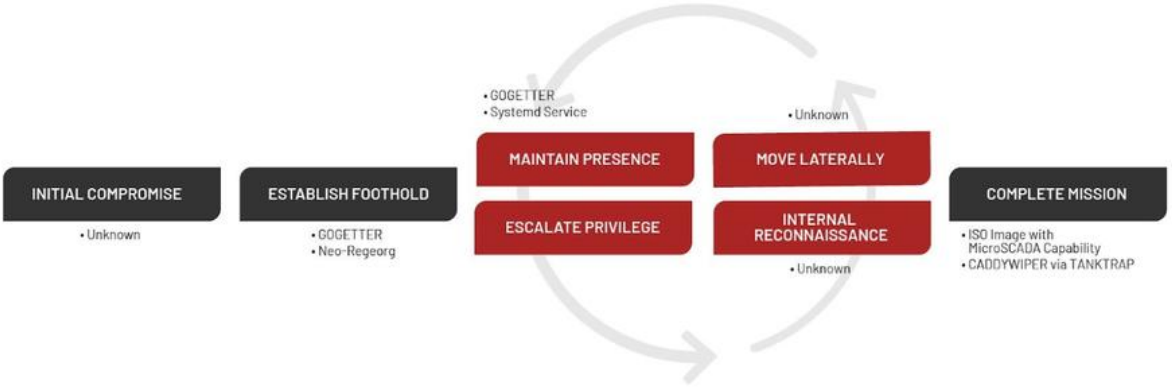
  Collection kısmında toplanan verinin dışarıya sızdırılması olayıdır.

- Impact

  Kurban makinenin kullanılabilirliğini bozmak buna örnek verilebilir. Saldırgan alacağını aldıktan sonra kurbana ransom bırakırsa bu impac’te örnek olacaktır.

2022 Ukrayna Elektrik Santrali Saldırısı

Saldırının kısaca özetini vermeden de geçmek olmaz. Araştırmalara göre ilk adım hakkında bilgi sahibi değiliz. Web shell olarak Neo-regeorg kullanılıp GOGETTER adlı Go yazılımı ile de bunu Proxy kullanarak gizlediler.

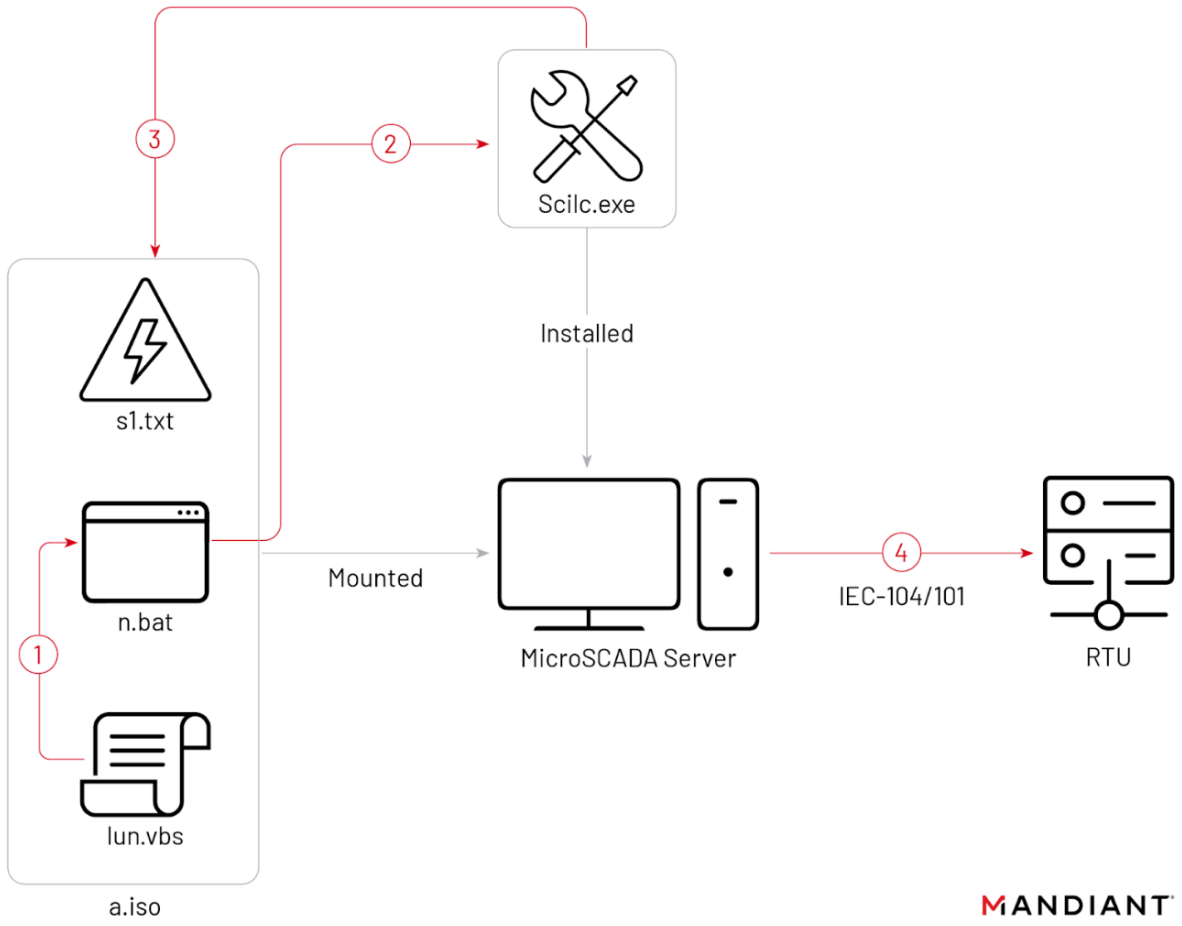


Sandworm tarafından kullanılan Systemd yapılandırma dosyası, grubun sistemlerde kalıcılığı sürdürmesini sağlamıştır. “WantedBy” değeri programın ne zaman çalıştırılması gerektiğini tanımladılar. Sandworm tarafından kullanılan yapılandırmada ‘multi-user.target’ ayarı, programın ana bilgisayarın kullanıcıların oturum açmasını kabul edecek bir duruma ulaştığında, örneğin başarılı bir şekilde açıldıktan sonra çalıştırılacağı anlamına geliyordu. Bu, GOGETTER'in yeniden başlatmalar arasında kalıcılığını korumasını sağladı. “ExecStart” değeri, çalıştırılacak programın yolunu belirtir, bu durumda bu yol GOGETTER'dir.

```
[Unit]
Description=Initial cloud-online job (metadata service crawler)
After=
Requires=
[Service]
RestartSec=240000s
Restart=always
TimeoutStartSec=30
ExecStart=/usr/bin/cloud-online
[Install]
WantedBy=multi-user.target
```

Bu kısma geldiğimizde saldırgan bir iso dosyası ile saldırıya devam ettiğini görüyoruz. SCADA sistemleri .iso uzantılı dosyaları sanal disk olarak otomatik bir şekilde çalıştırıyor. Saldırganlar bunu yaparak MicroSCADA yazılım paketinin bir parçası olan scilc.exe'yi çalıştırıyorlar. Bunu çalıştırmalarının sebebi "pack\scil\" dosya yoluna s1.txt'yi eklemek. Dosyanın içinde muhtemelen MicroSCADA'da çalıştırılmak istenen SCIL komutları var. Bu komutlara erişilebilirlik mümkün olmasa bile trafolara komut gönderdiği düşünülmektedir.

SCIL, MicroSCADA kontrol sistemleri için tasarlanmış yüksek seviyeli bir programlama dilidir ve sistemi ve özelliklerini çalıştırabilir. SCIL programları genellikle komutlar, nesneler, değişkenler, önceden tanımlanmış fonksiyonlara çağrılar ve ifadelerden oluşabilen metin tabanlı ifadelerdir.



2 gün süren aktivitelerin sonunda CADDYWİPER adında bir program yerleştiriliyor. Bu program birkaç farklı saldırıda da gözlemlenmiştir. CADDYWİPER C tabanlı çok güçlü bir silicidir. Domain kontrolcüsü tarafından TANKTRAP kullanılarak iki Grup İlkesi oluşturularak kuruluyor. CADDYWİPER'ın yanı sıra NEARMISS, SDELETE, PARTYTICKET gibi programlar da burada gözlemlenmiştir. Bu grup politikaları, bir dosyayı sunucudan yerel sabit diske kopyalamak ve kopyalanan dosyayı belirli bir zamanda çalıştıracak bir görevi zamanlamak için talimatlar içeriyordu.

2 grup ilkesi olarak oluşturulan CADDYWİPER'lar belli bir zamanda çalıştırılmak için msserver.exe olarak kuruldu.

Item	Value
Task Name	qAWZe
Legacy Task Name	QcWBX
Command to Run	C:\Windows\msserver.exe
Trigger	Run at 2022-10-12 16:50:40

Table 2: Sandworm TANKTRAP GPO 1 Scheduled Task

Item	Value
Task Name	QJKWt
Legacy Task Name	zJMwY
Command to Run	C:\Windows\msserver.exe
Trigger	Run at 2022-10-12 17:15:59

Table 3: Sandworm TANKTRAP GPO 2 Scheduled Task

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	During the 2022 Ukraine Electric Power Attack, Sandworm Team utilized a PowerShell utility called TANKTRAP to spread and launch a wiper using Windows Group Policy.[1]
Enterprise	T1543	.002	Create or Modify System Process: Systemd Service	During the 2022 Ukraine Electric Power Attack, Sandworm Team configured Systemd to maintain persistence of GOGETTER, specifying the `WantedBy=multi-user.target` configuration to run GOGETTER when the system begins accepting user logins.[1]
Enterprise	T1485		Data Destruction	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed CaddyWiper on the victim's IT environment systems to wipe files related to the OT capabilities, along with mapped drives, and physical drive partitions.[1]
Enterprise	T1484	.001	Domain or Tenant Policy Modification: Group Policy Modification	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Group Policy Objects (GPOs) to deploy and execute malware.[1]
Enterprise	T1570		Lateral Tool Transfer	During the 2022 Ukraine Electric Power Attack, Sandworm Team used a Group Policy Object (GPO) to copy CaddyWiper's executable `msserver.exe` from a staging server to a local hard drive before deployment.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Systemd service units to masquerade GOGETTER malware as legitimate or seemingly legitimate services.[1]
Enterprise	T1095		Non-Application Layer Protocol	During the 2022 Ukraine Electric Power Attack, Sandworm Team proxied C2 communications within a TLS-based tunnel.[1]
Enterprise	T1572		Protocol Tunneling	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the GOGETTER tunneler software to establish a "Yamux" TLS-based C2 channel with an external server(s).[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged Scheduled Tasks through a Group Policy Object (GPO) to execute CaddyWiper at a predetermined time.[1]
Enterprise	T1505	.003	Server Software Component: Web Shell	During the 2022 Ukraine Electric Power Attack, Sandworm Team deployed the Neo-REGEORG webshell on an internet-facing server.[1]
ICS	T0895		Autorun Image	During the 2022 Ukraine Electric Power Attack, Sandworm Team used existing hypervisor access to map an ISO image named `a.iso` to a virtual machine running a SCADA server. The SCADA server's operating system was configured to autorun CD-ROM images, and as a result, a malicious VBS script on the ISO image was automatically executed.[1]
ICS	T0807		Command-Line Interface	During the 2022 Ukraine Electric Power Attack, Sandworm Team leveraged the SCIL-API on the MicroSCADA platform to execute commands through the `scilc.exe` binary.[1]
ICS	T0853		Scripting	During the 2022 Ukraine Electric Power Attack, Sandworm Team utilizes a Visual Basic script `lun.vbs` to execute `n.bat` which then executed the MicroSCADA `scilc.exe` command.[1]
ICS	T0894		System Binary Proxy Execution	During the 2022 Ukraine Electric Power Attack, Sandworm Team executed a MicroSCADA application binary `scilc.exe` to send a predefined list of SCADA instructions specified in a file defined by the adversary, `s1.txt`. The executed command `C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt` leverages the SCADA software to send unauthorized command messages to remote substations.[1]
ICS	T0855		Unauthorized Command Message	During the 2022 Ukraine Electric Power Attack, Sandworm Team used the MicroSCADA SCIL-API to specify a set of SCADA instructions, including the sending of unauthorized commands to substation devices.[1]

Yukarıda gördüğünüz gibi matrisleri ve TID'leri verilmiştir. Şimdi hepsine teker teker bakıp ne anlama geldiğini ve saldırıda nasıl kullanıldığını öğrenelim.

T1059.001 Command Scripting Interpereter:Powershell

Saldırganlar yürütme için PowerShell komutlarını ve betiklerini kötüye kullanabilirler. PowerShell, Windows işletim sistemine dahil olan güçlü bir etkileşimli komut satırıdır.

Sandworm Ekibi, Windows Grup İlkesi'ni kullanarak bir silme aracı yaymak ve başlatmak için TANKTRAP adlı bir PowerShell yardımcı programını kullandı.

T1543.002 Create or Modify System Process: Systemd Service

Saldırganlar, kalıcılığın bir parçası olarak kötü amaçlı yükleri tekrar tekrar çalıştırmak için systemd hizmetleri oluşturabilir veya değiştirebilir. Systemd, arka plan arka plan işlemlerini ve diğer sistem kaynaklarını yönetmek için yaygın olarak kullanılan bir sistem ve hizmet yöneticisidir.

Sandworm Ekibi, GOGETTER'ın kalıcılığını korumak için Systemd'yi yapılandırdı ve sistem kullanıcı oturum açmalarını kabul etmeye başladığında GOGETTER'ı çalıştırmak için WantedBy=multi-user.target yapılandırmasını yaparak kalıcılık sağladı.

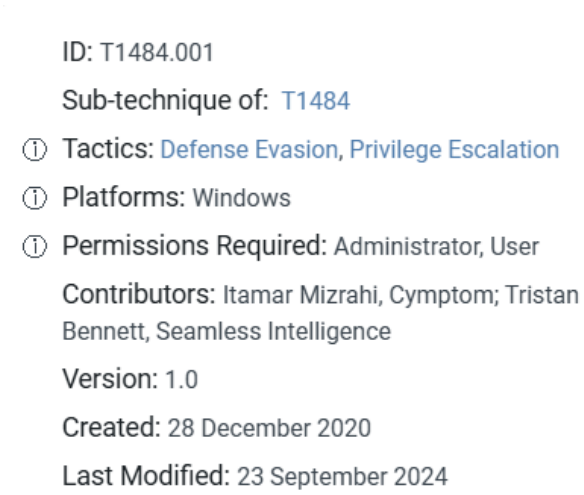
T1485 Data Destruction

Saldırganlar, sistemlerin, hizmetlerin ve ağ kaynaklarının kullanılabilirliğini kesintiye uğratmak için belirli sistemlerdeki veya bir ağdaki çok sayıda veriyi ve dosyayı yok edebilir. Verinin silinmesi, yerel ve uzak sürücülerdeki dosyaların veya verilerin üzerine yazılması yoluyla saklanan verileri adli tıp teknikleriyle kurtarılamaz hale getirebilir.

Sandworm Ekibi, eşlenen sürücüler ve fiziksel sürücü bölümleriyle birlikte OT yetenekleriyle ilgili dosyaları silmek için kurbanın sistemlerine CaddyWiper'ı yerleştirdi.

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

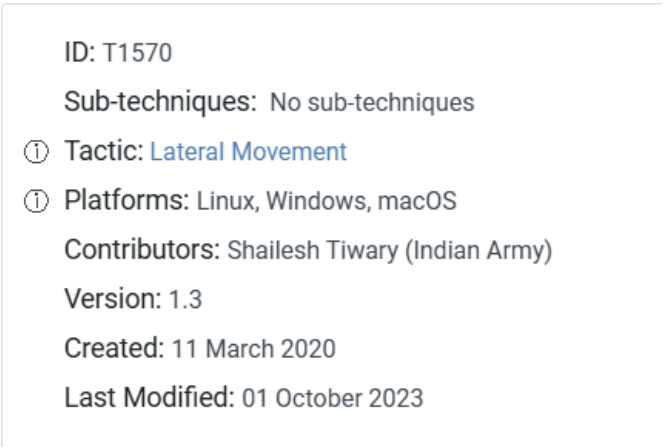
Saldırganlar Grup İlkesi Nesnelerini (GPO'lar), genellikle etki alanındaki ayrıcalıkları artırmak amacıyla, bir etki alanı için amaçlanan isteğe bağlı erişim denetimlerini yıkmak için değiştirebilir. Kötü amaçlı GPO değişiklikleri, Zamanlanmış Görev/İş, Araçları Devre Dışı Bırakma veya Değiştirme, Giriş Aracı Transferi, Hesap Oluşturma, Hizmet Yürütme ve daha fazlası gibi birçok başka kötü amaçlı davranışı uygulamak için kullanılabilir.



Sandworm Ekibi, kötü amaçlı yazılımları dağıtmak ve yürütmek için Grup İlkesi Nesnelerini (GPO'lar) kullandı.

T1570 Leteral Tool Transfer

Saldırganlar, ele geçirilmiş bir ortamdaki sistemler arasında araçları veya diğer dosyaları aktarabilir. Mağdur ortama bir kez sokulduktan dosyalar bir sistemden diğerine kopyalanarak bir operasyon süresince düşman araçları veya diğer dosyalar gözükebilir.



Sandworm Ekibi, dağıtım öncesinde CaddyWiper'ın yürütülebilir msserver.exe dosyasını bir hazırlama sunucusundan yerel bir sabit sürücüye kopyalamak için bir Grup İlkesi Nesnesi (GPO) kullandı.

T1036.004 Masquerading: Masquerade Task or Service

Saldırganlar, meşru veya zararsız görünmesini sağlamak için bir görevin veya hizmetin adını manipüle etmeye çalışabilirler.

Sandworm Ekibi, GOGETTER kötü amaçlı yazılımını meşru veya meşru görünen hizmetler gibi göstermek için Systemd hizmet birimlerinden yararlandı.

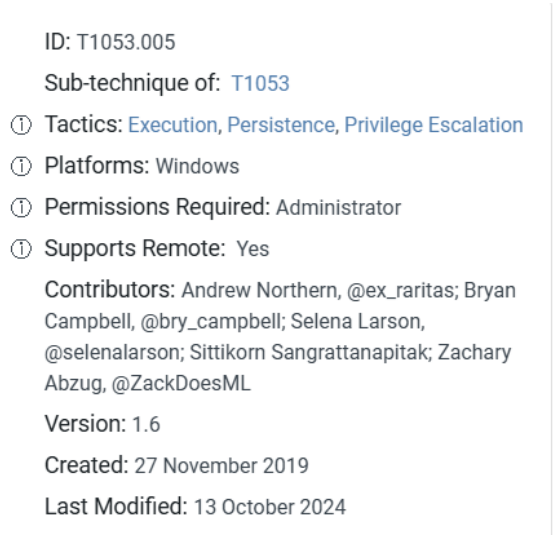
T1572 Protocol Tunneling

Saldırganlar, tespit edilmekten/ağ filtrelemesinden kaçınmak ve/veya başka türlü erişilemeyen sistemlere erişim sağlamak için, ayrı bir protokol içerisinde kurban sisteme ve sistemden ağ iletişimlerini tünelleyebilir.

Sandworm Ekibi, harici bir sunucu ile "Yamux" TLS tabanlı bir C2 kanalı kurmak için GOGETTER tünelleme yazılımını konuşlandırdı.

T1053.005 Scheduled Task/Job: Scheduled Task

Saldırganlar, kötü amaçlı kodun ilk veya tekrarlayan yürütülmesi için görev zamanlaması yapmak üzere Windows Görev Zamanlayıcısını kötüye kullanabilir.



Sandworm Ekibi, CaddyWiper'ı önceden belirlenmiş bir zamanda yürütmek için bir Grup İlkesi Nesnesi (GPO) aracılığıyla Zamanlanmış Görevlerden yararlanmıştır.

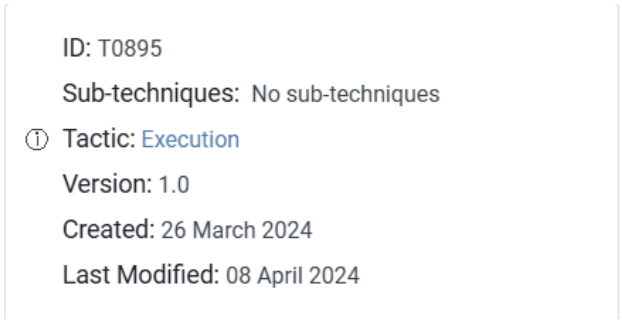
T1505.003 Server Software Component: Web Shell

Saldırganlar, sistemlere kalıcı erişim sağlamak için web kabuklarıyla web sunucularının arka kapısını açabilirler. Bir Web kabuğu, saldırganın bir ağa bir ağ geçidi olarak Web sunucusuna erişmesine izin vermek için açıkça erişilebilir bir Web sunucusuna yerleştirilen bir Web yazılımıdır.

Sandworm Ekibi, Neo-REGEORGwebshell'i internete açık bir sunucuya yerleştirdi.

T0895 Autorun Image

Saldırganlar, kötü amaçlı kod çalıştırmak için AutoRun işlevselliğinden veya komut dosyalarından yararlanabilir. AutoRun işlevselliğini veya eski işletim sistemlerini etkinleştirmek üzere yapılandırılan cihazlar, çeşitli çıkarılabilir medya biçimlerinde (örn. USB, Disk Görüntüleri [.ISO]) depolanan kötü amaçlı kodları çalıştırmak için bu özelliklerin kötüye kullanılmasına açık olabilir. Genellikle, AutoRun veya AutoPlay, bu tekniğe karşı hafifletmek için birçok işletim sistemi yapılandırmasında devre dışı bırakılır.



Sandworm Ekibi, a.iso adlı bir ISO görüntüsünü SCADA sunucusu çalıştıran bir sanal makineye eşlemek için mevcut hiper yönetici erişimini kullandı. SCADA sunucusunun işletim sistemi CD-ROM görüntülerini otomatik olarak çalıştıracak şekilde yapılandırılmıştı ve sonuç olarak ISO görüntüsündeki kötü amaçlı bir VBS betiği otomatik olarak çalıştırıldı.

T0807 Command-Line Interface

Saldırganlar sistemlerle etkileşime geçmek ve komutları yürütmek için komut satırı arayüzlerini (CLI'ler) kullanabilir. CLI'lar bilgisayar sistemleriyle etkileşim için bir araç sağlar ve kontrol sistemleri ortamlarındaki birçok platform ve cihaz türünde ortak bir özelliktir.

Sandworm Ekibi, scilc.exe ikili dosyası aracılığıyla komutları yürütmek için MicroSCADA platformundaki SCIL-API'den yararlandı.

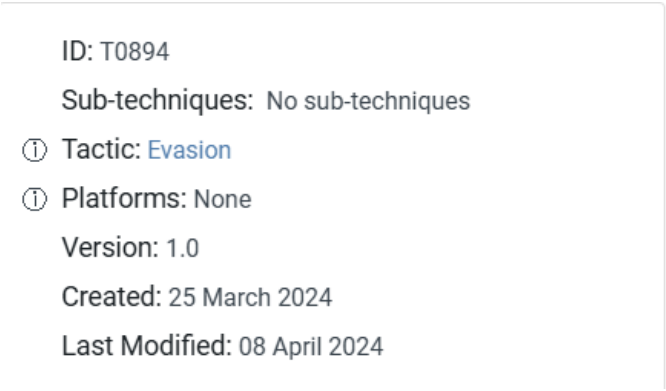
T0853 Scripting

Saldırganlar, önceden yazılmış bir komut dosyası biçiminde veya bir yorumlayıcıya kullanıcı tarafından sağlanan kod biçiminde rastgele kod çalıştırmak için komut dosyası dillerini kullanabilir.

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

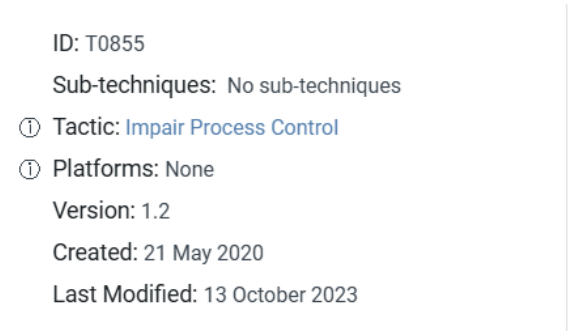
Saldırganlar, sistemde zaten mevcut olan ve genellikle güvenilir olarak kabul edilen ikili dosyaları (örneğin, işletim sistemi tarafından sağlanan uygulamalar) kullanarak kendi zararlı kodlarını çalıştırabilirler. Bu yaklaşım, zararlı yazılımın tespit edilmesini zorlaştırır çünkü faaliyetler meşru uygulamalar üzerinden gerçekleştirilir.



Sandworm Ekibi, düşman tarafından tanımlanan s1.txt dosyasında belirtilen SCADA talimatlarının önceden tanımlanmış bir listesini göndermek için bir MicroSCADA uygulama ikili scilc.exe çalıştırmıştır. Yürütülen C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt komutu, uzak trafo merkezlerine yetkisiz komut mesajları göndermek için SCADA yazılımından yararlanmaktadır.

T0855 Unauthorized Command Message

Saldırganlar, kontrol sistemi varlıklarına amaçlanan işlevlerinin dışında veya beklenen işlevlerini tetikleyecek mantıksal ön koşullar olmadan eylemler gerçekleştirmeleri talimatını vermek için yetkisiz komut mesajları gönderebilir. Komut mesajları ICS ağlarında kontrol sistemleri cihazlarına doğrudan talimatlar vermek için kullanılır.

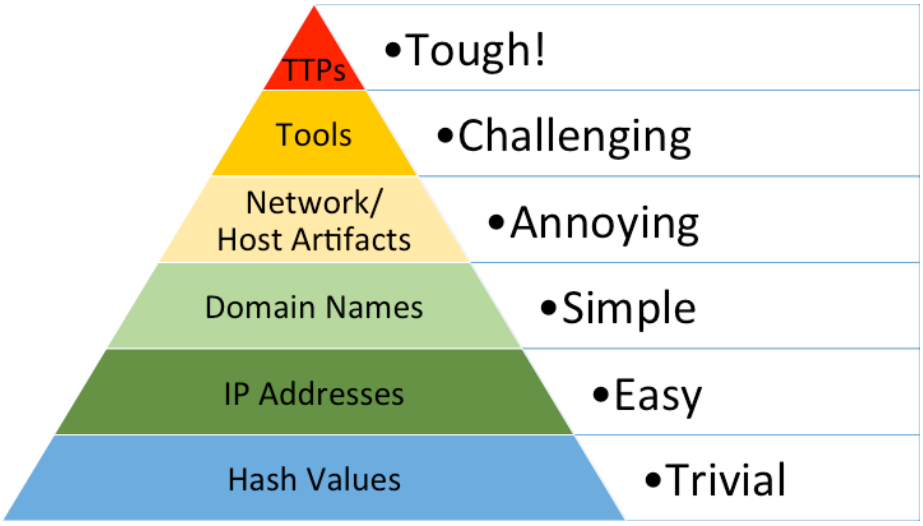


Sandworm Ekibi, trafo merkezlerine yetkisiz komutların gönderilmesi de dahil olmak üzere bir dizi SCADA talimatını belirtmek için MicroSCADA SCIL-API'yi kullandı.

PYRAMID OF PAIN

Pyramid of Pain siber tehdit istihbarat ve avcılıkta kullanılan bir modeldir. 2013 yılında David J. Bianco tarafından oluşturulmuştur. Saldırganların işlemlerini tespit etmek veya engellemek için kullanılan IoC'lerin yani bir siber saldırının gösterge türlerinin saldırgan üzerinde etkileri ve engellemenin ne kadar zor olduğunu gösterir.

Pyramid of Pain'in önemi aslında aşağıdaki tabloda gizlidir. Katman katman engelleme yapabilirsiniz burada ama hangisi daha güvenli inceleyelim.



Hash Values

Hash'ler dosyaların benzersiz parmak izleridir. Saldırganların MS uygulamalarını makrolarla saldırdığını düşünün. Bu dosyanın hashini aldınız ve engellediniz. Saldırıyı bir kere yedim ve engelledim diye düşünüyorsanız bu biraz yanlış olur. Dosyalarda yapılan küçük oynamalar hasahleri değiştirir. Daha derin bir örnek vermek istersen Cobalt Strike'ın C2 dosyasında sadece bir byte değiştirerek Windows Defenderı atlatabiliyorsunuz. Yani bu saldırganlar için çok acı verici değil.

IP Adresses

Bir IP'den şüphelendiniz ve onu engellediniz diyelim. Dünyadaki tek saldırgan o değil bunu unutmayın. Üstelik VPN ve Proxy kullanarak bunu aşabilirler. Ayrıca sanal sunucu satın alıp bile size zarar vermeye çalışabilirler.

Domain Names

C2 sunucuları için açıla domainler olabilir. Bunları engellemek de size katkı sağlayabilir. Katkısı yine de daha az olacaktır. Bir üst sırada bulunmasının sebebi maliyettir.

Network / Host Artifacts

Sistem logla ve ağ kalıntıları bunlara örnek olabilir. Bu ne anlama geliyor? Otomatize edilmiş araçlarla tarama yapılmış ise loglarda kalıntıları olacaktır. Bu log çıktılarına göre engellemeler yapılırsa saldırgan otomatik yapmış olduğu işi yeniden eliyle yapmak zorunda kalacaktır.

Örneğin Powershell üzerinden Invoke-Webrequest isteği zararlı olduğu için çoğu yerde engellenmiştir. Saldırganlar bunu atlatmak için ise kodu Base64 ile kodlayarak yazmaya başlamışlardır. Acı onları üst noktaya taşımıştır. Siz bunu da engellerseniz. O başka yollar arayıp vakit kaybedecektir.

Tools

Yukarıda da biraz bahsettiğim gibi araçlar konusunda yapılan engellemeler onlar için sıfırdan yeni araçlar yazmaya yönlendirecektir. Yenilerini yazamadıkları yerlerde onları çeşitli yöntemlerle gizlemeye çalışacaklardır. Cobalt Strike ve Metasploit gibi C2 sunucularını baştan yazmak maliyetli olduğu için gizlerler. İçerikleri bir yerden bir yere bağlantı kurmak olduğu için bunu engellemenin yolu ağı kontrol etmek daha iyi bir seçenektir.

TTPS

Taktik teknik ve prosedür olarak adlandırılan bu kısımda bir saldırının komple tamamını bilmiş olursunuz ve ona göre önlem alırsınız. Bunun önemini şöyle anlatabilirim. Örneğin saldırgan kalıcılık sağlamak adına görev zamanlayıcısına bir görev ekleyebilir. Siz SIEM'de eklenen yeni bir görev oluşturulduğunda uyarı ver diye kural eklerseniz bunu tamamıyla engellemiş olursunuz. Bu konuda bize yardımcı olan Mitre Att&ck tablosunu detaylıca inceleyebilirsiniz.

TTP (Taktik Teknik ve Prosedür)

TTP kısaltması başlıkta da görebileceğiniz gibi teknik taktik ve prosedür olarak kısaltması vardır. Bu başlık bize 3 sorusu sorar; nasıl, ne ve neden? Taktik kısmında peki neler yapabilirler?

Taktikler saldırganların yüksek seviyeli planlanmış olan saldırılarıdır. Hedef sistemin kontrolünü veya bilgilerini ele geçirmeye çalışırlar. İşte burada "Neden?" sorusuna cevap ararız. Bundan sonraki adımımız teknikte ne oluyor peki?

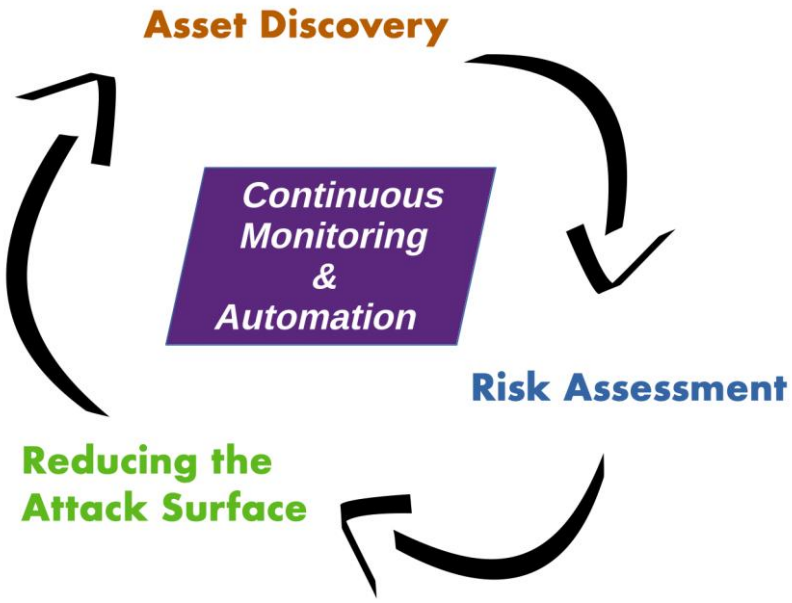
Teknikler daha orta seviye metotlar kullanılarak veya araçlarla güvenliğinizi kırmaya çalışırlar. Açıklaması taktiğe göre daha detaylı olandır. Burada "Ne?" sorusuna cevap ararız. Bu tekniklere örnek olarak:

- Phishing saldırıları
- Spearfishing saldırıları
- Malwareler
- DDos saldırıları

TTP Based Threat Hunting ve Detection Engineering

Detection Engineer

Detection engineer aslında bizim daha üst seviyelerimizde olan bilgili deneyimli kişilerdir. Onlar da monitoring yaparlar fakat altlarından gelen bilgileri kontrol ederek anomali var mı diye bakarlar. İyi bir detection engineer aslında sürekli dönen bir çark şeklinde olamlıdır. Kendini gündemden geri bırakmamalı altlarını bu konuda bilgilendirmeli kendi deneyimlerini aşağıya aktarabilmelidir. Ağ güvenliği ve sistem güvenliği başta olmak üzere birçok konuda bilgi sahibidirler. Bunun yanı sıra işletim sistemleri hakkında bilgileri de üst düzeydir. Daha da eklersek yazılımı koyabiliriz.



Attack surface managementini iyi kavramış bilen ve uyguluyandır detection engineer. SIEM, XDR ve EDR kurulumu yapabilir. SIEM'e kurallar ekleyebilir. XDR ve EDR kullanarak threat hunting yapabilir.

TTP Tabanlı Tehdit Avcılığı Nasıl Çalışır?

1. **Veri Toplama**: Ağ trafiği, loglar, endpoint verileri gibi çeşitli kaynaklardan veri toplanır.
2. **Analiz**: Toplanan veriler, bilinen TTP'lerle karşılaştırılır. Bu, saldırganların kullandığı tekniklerin ve taktiklerin belirlenmesine yardımcı olur.
3. **Tehdit Tespiti**: Analiz sonucunda, olası tehditler belirlenir. Bu, bilinen saldırı modelleriyle eşleşen davranışların tespit edilmesini içerir.

4. **Müdahale**: Tespit edilen tehditlere karşı uygun güvenlik önlemleri alınır. Bu, güvenlik duvarlarının güncellenmesi, sistem yamalarının uygulanması veya kullanıcıların bilgilendirilmesi gibi adımları içerebilir.

Faydaları

- **Proaktif Yaklaşım**: TTP tabanlı tehdit avcılığı, saldırıları önceden tespit etmeye ve önlemeye yardımcı olur.
- **Detaylı Analiz**: Saldırganların davranış kalıplarını anlamak, daha etkili savunma stratejileri geliştirmeyi sağlar.
- **Uyarlanabilirlik**: Yeni ve gelişen tehditlere karşı hızlı bir şekilde adapte olunabilir.

SENERYO

Saldırının başlangıcı olarak kurbana bir mail gönderilir. Patronundan mail geldiğini sanan kurbanımız spear-fishing saldırısı altındadır. Saldırgan sosyal mühendislik ile topladığı bilgileri kullanarak patronunu taklit eden bir mail atmışlardır. Mailde ekteki dosyaların araştırılması istenmektedir. Ekteki bulunan zip dosyasının şifreli olduğu şifresinin yine ekteki fotoğrafta yazdığını belirtmektedir. Dosyayı açan kurban Word dosyasına tıkladığında içindeki zararlı makro zipte iki kere sıkıştırılarak gizlenmiş olan .ps1 dosyayı çalıştırır. Bu powershell dosyası internet tabanlı bir komuta kontrol sunucusu ile bağlantı kurar.

Web shelli şifrelemek için SSL sertifikası kullanan saldırgan kendini ağ trafiğinden de korumaya almıştır. Saldırgan bağlantıyı kurup gizledikten sonra discovery aşamasına geçerek SoftPerfect Network scanner kullanmıştır.

Active directory içinde olduğunu fark eden saldırgan whoami/priv komutu çalıştırarak **SeTcbPrivilege** tokenının etkin olup olmadığını kontrol eder. Bunun da çıktısını alınca token manıpulation işlemine başlar. **KERB_S4U_LOGON** kullanarak bir başka kullanıcının şifresini bilmeden tokenını oluşturur ve kendini admin grubuna medium integrity olarak atar.

Yetki yükseltmesini yapan saldırgan kalıcılık sağlamak için üstüne görev zamanlayıcısına .ps1 dosyasının her kullanıcı girişi yapıldığında çalışacak şekilde ayarlar ve ismini updater.exe koyarak gözden kaçmayı umar. Her yere yetkisi olan saldırgan verileri kopyalayıp komuta kontrol sunucusundan sızdırır.

5 taktik için 2 teknik demiştiniz ama benimkisi 8 taktik oldu umarim beğenirsiniz.

Inital Access

T1566.001 Spearphishing Attachment

Execution

T1059.001 Command and Scripting Interpreter: PowerShell

Persistence

T1053.005 Scheduled Task/Job: Scheduled Task

Privilege Escalation

T1134.001 Access Token Manipulation: Token Impersonation/Theft

Defense Evasion

T1036 Masquerading

Discovery

T1087 Account Discovery

Collection

T1005 Data from Local System

Command and Control

T1001.003 Data Obfuscation: Protocol or Service Impersonation

Exfiltration

T1041 Exfiltration Over C2 Channel

KAYNAKÇA

https://app.letsdefend.io/

https://attack.mitre.org/