SİBER AKADEMİ
EĞİTİM MERKEZİ

İSTANBUL GELİŞİM ÜNİVERSİTESİ

İGÜ SİBER AKADEMİ

TÜRKİYE'YE SALDIRAN APT GRUPLARI VE SALDIRI ANALİZLERİ

Hazırlayan

Hasan Meriç YILDIZ

Ödev Danışmanı

Mehmet DEMİR

İSTANBUL – 2024

ÖDEV TANITIM FORMU

YAZAR ADI SOYADI	**:** Hasan Meriç YILDIZ
ÖDEVİN DİLİ	**:** Türkçe
ÖDEVİN ADI	**:** TÜRKİYE'YE SALDIRAN APT GRUPLARI VE SALDIRI ANALİZLERİ
BÖLÜM	**:**Digital Forensics and Incident Response
ÖDEVİN TÜRÜ	**:** Final
ÖDEVİN TES. TARİHİ	**:** 20.12.2024
SAYFA SAYISI	**:** 58
ÖDEV DANIŞMANI	**:** Mehmet DEMİR

Beyan

Bu ödevin/projenin hazırlanmasında bilimsel ahlak kurallarına uyulduğu, başkalarının ederlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğu, kullanılan verilerde herhangi tahrifat yapılmadığını, ödevin/projenin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir ödev/proje olarak sunulmadığını beyan eder, aksi durumda karşılaşacağım cezai ve/veya hukuki durumu kabul eder; ayrıca üniversitenin ilgili yasa, yönerge ve metinlerini okuduğumu beyan ederim.

Tarih
20.12.2024

Öğrenci Adı Soyadı

Hasan Meriç Yıldız

Kabul ve Onay Sayfası

numaralı Hasan Meriç Yıldız'ın "TÜRKİYE'YE SALDIRAN APT GRUPLARI VE SALDIRI ANALİZLERİ" adlı çalışması, benim tarafımdan Final ödevi olarak kabul edilmiştir.

Mehmet DEMİR

Özet

Bu çalışmada, Gelişmiş Sürekli Tehditler (APT) kavramı kapsamlı bir şekilde ele alınmış, APT saldırılarının dinamikleri, kullanılan teknikler ve alınabilecek önlemler üzerinde durulmuştur. Öncelikle, APT'nin tanımı ve temel özellikleri açıklanmış; ardından bu tehditlerin hedef seçme yöntemleri ve saldırı aşamalarında kullanılan göstergeler (Indicators of Compromise - IoC) detaylandırılmıştır.

Türkiye'nin APT grupları tarafından hedef alınma nedenleri, bu saldırıların jeopolitik ve ekonomik etkileri çerçevesinde incelenmiş, Türkiye'ye saldırı düzenleyen öne çıkan APT grupları tanıtılmıştır. Ayrıca, Taktikler, Teknikler ve Prosedürler (TTP) kavramı üzerinde durulmuş, bu TTP'lerin alt tekniklere bölünmesi ve saldırıların nasıl yapılandırıldığı örneklerle açıklanmıştır.

Son olarak, APT saldırılarından korunmak için uygulanabilecek stratejiler ve saldırılara karşı alınması gereken önlemler ayrıntılı bir şekilde sunulmuş; güçlü erişim politikaları, güncel sistemler, ağ güvenliği ve farkındalık artırıcı eğitimlerin önemi vurgulanmıştır. Bu çalışma, APT tehditlerine karşı hem bireylerin hem de kurumların bilinçlenmesi ve siber güvenlik stratejilerinin güçlendirilmesine katkı sağlamayı amaçlamaktadır.

İçindekiler Tablosu

Kısaltmalar

APT: Advance Persistent Threat

DNS: Domain Name System

DLL: Dynamic Link Library

VBS: Visual Basic Script

IOC: Indicators of Compromise

IP: Internet Protocol

CVE: Common Vulnerabilities and Exposures

MD5: Message Digest Algorithm 5

SHA1: Secure Hash Algorithm 1

SHA256: Secure Hash Algorithm 256-bit

BAE: Birleşik Arap Emirlikleri

NATO: North Atlantic Treaty Organization

ABD: Amerika Birleşik Devletleri

BT: Bilgi Teknolojileri

HTTP: Hypertext Transfer Protocol

SWIFT: Society for Worldwide Interbank Financial Telecommunication

TTP: Tactics, Techniques, and Procedures

LDAP: Lightweight Directory Access Protocol

HTTPS: Hypertext Transfer Protocol Secure

C2: Command and Control

SIEM: Security Information and Event Management

LOG: Log File (kayıt dosyası)

TLS: Transport Layer Security

SSL: Secure Sockets Layer

DLP: Data Loss Prevention

WMI: Windows Management Instrumentation

UAC: User Account Control

VPN: Virtual Private Network

MFA: Multi-Factor Authentication

DCCC: Democratic Congressional Campaign Committee

SAAS: Software as a Service

IIS: Internet Information Services

AWS RDS: Amazon Web Services Relational Database Service

CRM: Customer Relationship Management

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

EDR: Endpoint Detection and Response

APT(Advanced Persistent Threat) Nedir?

APT (Advanced Persistent Threat) yani gelişmiş sürekli tehdit anlamına gelen bir kısaltmadır. Günümüzde APT gruplarının çoğu devlet destekli olmakla birlikte, devlet destekli olmayan ve kendi içinde örgütlenebilen APT grupları da mevcuttur. Bunlar normal bilgisayar korsanlarından farklı olarak gelişmiş yöntemler kullanan, bir sisteme gizli bir şekilde sızıp uzunca bir süre o sistemde kalabilen gelişmiş bilgisayar korsan gruplarıdır.

Advanced (Gelişmiş): APT grupları bilişim dünyasındaki yetenekli kişilerden oluşur. Bu kişiler birçok istihbarat toplama yöntemlerini etkin olarak kullanabilme yeteneğine sahiptir. Birçoğu devlet tarafından desteklenip devletin istihbarat altyapısından faydalansa da kendi imkanları ile illegal ve legal yollardan hedefine dair bilgi toplayan gruplar bulunmaktadır. Yapılan saldırıların hepsi çok gelişmiş olarak sayılmasa da (örneğin bilinen bir zafiyeti kullanma vb.) bu kişiler istedikleri zaman hedefine uygun zararlı yazılım, strateji ve çeşitli yöntemleri üretip bir arada kullanarak hedefine en uygun şekilde ulaşabilir.

Persistent (Sürekli): APT gruplarının birçok saldırısı sızdıkları sistemde uzun süre kalabilmeyi amaçlar, aynı zamanda sisteme daha sonra tekrar girebilmek için olabildiğince fazla açık kapı bırakmaya çalışırlar. Bu saldırılar çoğu zaman finansal veya başka bir kazanç içermek için yapılır, çoğu zaman da belirli hedeflere yönelik saldırı yürütürler.

Threat (Tehdit): APT grupları yüksek seviyeli tehdit olarak kabul edilir çünkü bu kişilerin bilgisayar ortamında istediği kötü eylemi gerçekleştirebilme kabiliyetleri vardır. Yapılan saldırıda gelişigüzel yerine koordineli bir şekilde çalıştıkları için tehdit seviyelerini epey yükseltiyor. Aynı zamanda bu kişiler genellikle iyi finanse edildikleri için motive olup etkili bir şekilde saldırılarını gerçekleştirebiliyorlar.

IOC NEDİR

IoC (Indicator of Compromise - Saldırı Göstergesi), bir sistemin güvenliği ihlal edildiğine veya bir siber saldırıya maruz kaldığına dair iz veya kanıt sağlayan belirteçlerdir. Bu göstergeler, zararlı faaliyetlerin tespit edilmesi, izlenmesi ve analiz edilmesi süreçlerinde kritik bir rol oynar. IoC'ler genellikle sistem log dosyalarındaki anormal girişlerden, beklenmedik ağ trafiğine, bilinmeyen dosyalara veya kötü amaçlı yazılımların bıraktığı izlere kadar geniş bir yelpazeyi kapsar. Örneğin, belirli bir IP adresinden gelen alışılmadık derecede yüksek trafik, yetkisiz erişim girişimlerini gösteren log kayıtları veya zararlı bir dosyaya işaret eden hash değerleri birer IoC olarak kabul edilir.

IoC'lerin doğru bir şekilde tespit edilmesi ve yorumlanması, siber saldırılara karşı erken uyarı mekanizmalarının devreye girmesini sağlar. Ayrıca, bu göstergeler sayesinde saldırının kaynağı ve amacı daha iyi anlaşılır ve buna uygun müdahale stratejileri geliştirilebilir. IoC'ler, özellikle tehdit avcılığı (threat hunting) ve olay müdahale (incident response) süreçlerinde temel yapı taşlarından biri olarak kullanılır. Ancak, IoC'lerin etkili bir şekilde kullanılabilmesi için sürekli güncel tutulması ve organizasyonel tehdit istihbaratı süreçleriyle entegre edilmesi gereklidir.

Örneğin:

79c7219ba38c5a1971a32b50e14d4a13, OilRig grubuna ait bu hash, bu grubun bir IoC’si olarak kabul edilir.

Bu hash değeri, VirusTotal gibi güvenlik sitelerinde aratılarak tehdit hakkında detaylı bilgi edinilebilir. Bu örnekte yapılan inceleme sonucunda, Saitama.Agent.exe isimli bir dosya olduğu ve backdoor zararlısını içerdiği görülmektedir.

Türkiye'ye Saldırı Uygulayan APT Grupları

Türkiye, coğrafi konumu, enerji koridorlarındaki stratejik rolü ve savunma sanayisindeki güçlü adımları nedeniyle APT gruplarının sıkça hedefi olmaktadır.

Bu saldırıların ana motivasyonları arasında jeopolitik çıkarlar, ekonomik rekabet avantajı sağlama, kritik altyapılara zarar verme ve stratejik bilgi toplama yer alır. Türkiye'ye yapılan APT saldırılarında, özellikle enerji projeleri, savunma sanayi, kamu kurumları ve iletişim altyapıları öncelikli hedefler olarak öne çıkar. Ayrıca, uluslararası anlaşmalar ve ekonomik politikalar da bu grupların ilgisini çeken bir diğer faktördür.

APT saldırıları genellikle uzun vadeli bir strateji doğrultusunda planlanır ve hedef sistemlere sızdıktan sonra izlerini gizleme konusunda oldukça başarılıdır. Kimlik avı (phishing), zararlı yazılımlar (malware) ve sıfırıncı gün açıklarını (zero-day vulnerabilities) kullanma gibi yöntemlerle gerçekleştirilen bu saldırılar, tespit edilmesi ve durdurulması son derece güç tehditler oluşturur.

Türkiye'nin kritik altyapılarındaki güvenlik açıklarından faydalanan bu gruplar, yalnızca bilgi çalmakla kalmaz; aynı zamanda iletişim ve enerji gibi hayati sektörlerde kesintilere neden olabilecek operasyonlar da düzenleyebilir. Türkiye'ye yönelik APT saldırıları, sadece ulusal güvenlik değil, aynı zamanda ekonomik istikrar ve kamu hizmetleri açısından da ciddi bir tehdit oluşturmaktadır. Bir sonraki bölümde, Türkiye'yi hedef alan başlıca APT grupları, bu grupların karakteristik özellikleri ve kullandıkları yöntemler detaylı bir şekilde ele alınacaktır.

OilRig (APT34)

- **Menşei:** İran
- **Bilinen diğer isimleri:** Helix Kitten, IRN2, EUROPIUM
- **MITRE ATT&CK:** https://attack.mitre.org/groups/G0049/
- **Hedef:** Orta Doğu ülkeleri, Türkiye, Amerika Birleşik Devletleri
- **Motivasyon:** Orta Doğu'da politik etkisini artırmak ve istikrarsızlık yaratmak için medya ve hükümet verilerini kullanarak stratejiler geliştirmek.
- **Saldırı türleri:** Spear phishing, DNS tunneling ile veri sızdırma, PowerShell tabanlı araçlar (örneğin, Karkoff vb.).
- **Saldırı teknikleri:** Sistem bilgisi toplama (T1087), iletişim protokolü istismarı (T1071), kod enjeksiyonu (T1059), kimlik bilgisi çalma (T1555), sızma sonrası eylemler (T1573), veri sızdırma (T1048).
- **2024 Faaliyetleri:** OilRig özellikle başta Birleşik Arap Emirlikleri ve Körfez bölgesindeki ülkeleri hedef alarak, Windows sistemlerinde bir güvenlik açığı (CVE-2024-30088) kullanarak saldırılar gerçekleştirdi. Bu zafiyet, grubun Microsoft Exchange sunucularına sızmasına ve gelişmiş araçlarını devreye sokmasına olanak tanımıştır.
- **Türkiye Faaliyetleri:** Daha çok enerji sektörüne yönelik sızma girişimlerinde bulunmuşlardır. Petrol ve doğalgaz çalışmalarına yönelik kritik ve işe yarar bilgi toplama faaliyetleri gerçekleşmiştir. Ülkemizde İranlı firmalar ile rekabet eden enerji firmalarına yönelik kimlik avı saldırıları ve çeşitli sosyal mühendislik yöntemleri kullanılmıştır.
- **IoC (Indicators of Compromise):**
  FileHash-MD5 79c7219ba38c5a1971a32b50e14d4a13
  FileHash-SHA1 b39b3a778f0c257e58c0e7f851d10c707fbe2666
  FileHash-SHA256
  26884f872f4fae13da21fa2a24c24e963ee1eb66da47e270246d6d9dc7204c2b
- **Domain:** asiaworldremit.com, joexpediagroup.com, uber-asia.com

MuddyWater

- **Menşei:** İran
- **Bilinen diğer isimleri:** Seedworm, TEMP.Zagros, Static Kitten
- **MITRE ATT&CK:** https://attack.mitre.org/groups/G0069/
- **Hedef:** Orta Doğu ülkeleri, Türkiye, Azerbaycan, Pakistan, Afganistan
- **Motivasyon:** İran'ın bölgesel stratejik çıkarlarını desteklemek, istihbarat toplamak ve ülkelerin içişlerine müdahale etmek.
- **Saldırı türleri:** Spear phishing, DLL yan yükleme (DLL hijacking), PowerShell tabanlı araçlar, Microsoft Office ve Exchange açıklarının (örneğin CVE-2017-0199, CVE-2020-0688) istismarı.
- **Saldırı teknikleri:** Kimlik avı saldırıları (T1566.001), kullanıcı tarafından çalıştırılan zararlı yazılım (T1204), PowerShell kod yürütme (T1059), kayıt defteri çalıştırma anahtarları (T1547), uzaktan yönetim araçları (T1047).
- **2024 Faaliyetleri:** Son zamanlarda MuddyWater APT grubu tarafından yapılan saldırılarda kullanılan ve bugün hala aktif olan VBS/DLL tabanlı implantları açığa çıkarıldı. İmplantlar Mısır, Kazakistan, Kuveyt, Fas, Umman, Suriye ve BAE'deki birden fazla hükümet ve telekomünikasyon kuruluşunda bulundu. Tehdit aktörü, wscript.exe yardımcı programıyla kötü amaçlı bir VBS dosyasını çalıştıran zamanlanmış görevler aracılığıyla kalıcılık elde etmektedir.
- **Türkiye Faaliyetleri:** MuddyWater, Türk hükümetini hedef alarak SloughRAT adlı uzaktan erişimli bir Truva atı göndermek için girişimlerde bulunmuştur. Ayrıca Kasım 2021'de Cisco Talos, TÜBİTAK dahil olmak üzere Türkiye devlet kurumlarını hedef alan bir kampanya tespit edilmiştir.
- **IoC (Indicators of Compromise):**
  FileHash-MD5 09cc6bebec6db77a401507d33ec3987c
  FileHash-SHA1 2a6ddf89a8366a262b56a251b00aafaed5321992
  FileHash-SHA256
  61f83466b512eb12fc82441259a5205f076254546a7726a2e3e983011898e4e2
- **Domain:** advanceorthocenter.com, lalindustries.com, win7-updates.com

Charming Kitten (Magic Hound)

- **Menşei:** İran
- **Bilinen diğer isimleri:** APT35, Phosphorus, TA453.
- **MITRE ATT&CK:** https://attack.mitre.org/groups/G0059/
- **Hedef:** Türkiye, Orta Doğu ülkeleri, ABD, İsrail, Birleşik Krallık ve İspanya
- **Motivasyon:** Casusluk ve bilgi hırsızlığı; siyasi stratejiler geliştirme ve hassas bilgileri sızdırma.
- **Saldırı türleri:** Spear phishing, kötü amaçlı yazılım (powerstar backdoor), IPFS (InterPlanetary File System).
- **Saldırı teknikleri:** Kullanıcı denetimi atlama (T1548), kimlik bilgisi çalma (T1555), keylogger tuş yakalama (T1056), kayıt defteri çalıştırma anahtarları (T1547).
- **2024 Faaliyetleri:** Grubun 2024 yılında bilinen bir saldırısı olmadı ancak bilinen son saldırılarında yeni araçlar ve yöntemler kullanarak global bir şekilde saldırılar düzenledi. Bu saldırılarda özellikle "PowerLess" olarak adlandırılan bir PowerShell tabanlı arka kapı aracı öne çıktı. Bu araç, kötü amaçlı yazılımları indirip çalıştırabilir, şifre çalma ve bilgi toplama işlevlerine sahiptir. Bu araç, doğrudan PowerShell.exe'yi çağırmadan .NET çerçevesi içinde çalışarak algılamadan kaçınmaktadır.
- **Türkiye Faaliyetleri:** 2021'de Türkiye'deki kamu kurumlarına yönelik bir kampanya gözlemlendiği gibi, 2024'te de Türk hükümetine ve özel sektör kuruluşlarına yönelik yeni sızma girişimleri raporlanmıştır.
- **IoC (Indicators of Compromise):**

  FileHash-MD5 542128ab98bda5ea139b169200a50bce

  FileHash-MD5 3d67ce57aab4f7f917cf87c724ed7dab
- **Domain:** drive-accounts.com, yah00.site, instagram-com.site, acconut-verify.com, skynevvs.com

Fancy Bear (APT28)

- **Menşei:** Rusya
- **Bilinen diğer isimleri:** Sofacy, STRONTIUM, Tsar Team, IRON TWILIGHT
- **MITRE ATT&CK:** https://attack.mitre.org/groups/G0007/
- **Hedef:** NATO (Türkiye), Ukrayna, Gürcistan ve Kafkasya Ülkeleri
- **Motivasyon:** Casusluk, bilgi çalma, siyasi etkiler yaratma ve rakiplerini siber yöntemlerle istikrarsızlaştırma. Kritik altyapılara yönelik uzun vadeli tehditler oluşturma.
- **Saldırı türleri:** Spear phishing, kötü amaçlı yazılım (x-agent ve x-tunnel), Zafiyet sömürüsü (örn. CVE-2023-23397), Zero-Day saldırıları.
- **Saldırı teknikleri:** Zafiyet istismarı (T1190), kimlik avı, bilgi toplama (T1590), uzaktan çalınan hesaba erişim (T1078).
- **2024 Faaliyetleri:** Fancy Bear, enerji ve savunma sektörlerini hedef alan saldırılar düzenlemiştir. Bu saldırılarda özellikle zafiyet istismarları ve gelişmiş kimlik avı teknikleri öne çıkmaktadır. NATO üyesi olan Türkiye, grubun dolaylı hedefleri arasında yer almakta ve stratejik sektörlerde çalışan Türk kuruluşları risk altında bulunmaktadır.
- **Türkiye Faaliyetleri:** Türk askeri savunma sanayi şirketlerini hedef almışlardır. Türkiye'nin Suriye ve Doğu Akdeniz politikalarına dair bazı bilgilere ulaşmaya çalıştığı tespit edilmiştir.
- **IoC (Indicators of Compromise):**

  FileHash 46e2957e699fae6de1a212dd98ba4e2bb969497d

  FileHash c53930772beb2779d932655d6c3de5548810af3d

  Domain: beststreammusic.com, bbcweather.org, protonhardstorage.com, moderntips.org, bulgariatripholidays.com

Cozy Bear (APT29)

- **Menşei:** Rusya
- **Bilinen diğer isimleri:** UNC2452, NOBELIUM, StellarParticle, Dark Halo
- **MITRE ATT&CK:** https://attack.mitre.org/groups/G0016/
- **Hedef:** NATO (Türkiye), Ukrayna, ABD, Birleşik Krallık, Fransa, Almanya
- **Motivasyon:** Casusluk, bilgi çalma, uluslararası ilişkilere dair bilgi çalma, askeri, ticari ve enerji sektörlerini hedef alarak avantaj sağlama.
- **Saldırı türleri:** Spear phishing, kötü amaçlı yazılım, kimlik bilgisi çalma, web sitelerine zararlı kod yerleştirme, watering hole saldırıları.
- **Saldırı teknikleri:** Bruteforce saldırıları (T1110), kimlik avı, bilgi toplama (T1590), eski çalışan hesaplarını ele geçirme (T1078), bilinen zafiyetleri kullanma (CVE-2023-38831), watering hole saldırıları (T1071), bulut sistemlere sızarak cihaz doğrulama kurallarını baypas eder ve cihazlarını sisteme kaydeder (T1098), PowerShell kod yürütme (T1059).
- **2024 Faaliyetleri:** Cozy Bear, 2024 yılında hükümet sistemlerine ve savunma altyapılarına saldırmıştır. Bu saldırılar özellikle çoklu faktör korumasının olmadığı bulut sistemlerine yönelik yapılmıştır.
- **Türkiye Faaliyetleri:** Cozy Bear grubunun daha önce Türkiye'de hükümet ve stratejik sektörleri hedef aldığı bilinmektedir. Türkiye'nin NATO üyeliği ve bölgesindeki stratejik rolü, Cozy Bear'ın odak noktası olmasına neden olmaktadır.
- **IoC (Indicators of Compromise):**

  FileHash 057e79801070572be543fdd7111657517827457f

  FileHash d4a5d44184333442f5015699c2b8af28
- **Domain:** azuresecuritycenter.onmicrosoft.com, pdf-docs.online, muslimnewsdaily.com, sense4baby.fr, satkas.waw.pl

Chafer (APT39)

- **Menşei:** İran
- **Bilinen diğer isimleri:** REMIX, KITTEN, Cobalt Hickman
- **MITRE ATT&CK:** https://attack.mitre.org/groups/G0087/
- **Hedef:** Türkiye, İspanya, ABD, Mısır, Irak, Suudi Arabistan
- **Motivasyon:** Telekomünikasyon, seyahat, akademik ve BT firmaları gibi şirketlere sızıp bilgi çalmak ve arka kapı bırakmak.
- **Saldırı türleri:** Spear phishing, kötü amaçlı yazılım, kimlik bilgisi hırsızlığı.
- **Saldırı teknikleri:** kimlik avı saldırıları, bilgi toplama (T1590), kullanıcı tarafından çalıştırılan zararlı yazılım (T1204), PowerShell kod yürütme (T1059).
- **2024 Faaliyetleri:** 2024'teki faaliyetleri konusunda bilgiler oldukça sınırlıdır. Ancak önceki saldırılarına yakın saldırılar yaptığı düşünülmektedir.
- **Türkiye Faaliyetleri:** 2018 Şubat ayında turkiyebursları.gov.tr adresine saldırı gerçekleştirmişlerdir. Bu saldırıda MechaFlounder adlı python tabanlı bir payload kullandıkları tespit edilmiştir. Bu saldırıda Chafer grubu 185.177.59.70 IP adresinden yürütülebilir bir dosya indirmiştir. Win10-update.com adresinden HTTP isteği ile indirilen "lsass.exe" adlı dosya çalıştırılarak sistemlerde yetkisiz erişim sağlanmıştır.
- **IoC (Indicators of Compromise):**

  FileHash 804460a4934947b5131ca79d9bd668cf

  FileHash b38561661a7164e3bbb04edc3718fe89
- **Domain:** s224.win7-update.com, s21.win7-update.com, win10-update.com

Wicked Panda (APT41)

- **Menşei:** Çin
- **Bilinen diğer isimleri:** Brass Typhoon, BARIUM
- **MITRE ATT&CK:** https://attack.mitre.org/groups/G0096/
- **Hedef:** Türkiye, İspanya, İtalya, Tayvan, Tayland, Birleşik Krallık
- **Motivasyon:** Lojistik, medya, otomotiv ve BT firmaları gibi şirketlere sızıp bilgi çalmak, arka kapı bırakmak ve uzun süre içeride kalmak.
- **Saldırı türleri:** Spear phishing, kötü amaçlı yazılım, kimlik bilgisi hırsızlığı, arka kapı kullanımı, dosya hırsızlığı.
- **Saldırı teknikleri:** kimlik avı, bilgi toplama (T1590), sistemde kalıcılık sağlama (T1505), çalıştırılabilir dosya yürütme (T1569), Dll yükleme (T1574), OneDrive üzerinden dosya kaçırma (T1567).
- **2024 Faaliyetleri:** APT41, küresel ölçekte siber operasyonlarını artırmıştır. Özellikle İtalya, İspanya, Tayvan, Türkiye ve Birleşik Krallık'taki çeşitli sektörlerde faaliyet gösteren kuruluşları hedef almıştır. Bu saldırılarda, hassas verileri çalmak amacıyla gelişmiş taktikler kullanılmış ve hedef ağlarda uzun süreli kalıcılık sağlanmaya çalışılmıştır. Ayrıca, APT41'in yeni ve modüler bir araç seti olan DeepData framework'ünü kullanarak Güney Asya'daki hedeflerine yönelik izleme ve gözetim kapasitesini genişlettiği rapor edilmiştir.
- **Türkiye Faaliyetleri:** 2024 yılında APT41, Türkiye'deki çeşitli sektörleri hedef almıştır. Özellikle küresel nakliye ve lojistik, medya ve eğlence, teknoloji ve otomotiv sektörlerinde faaliyet gösteren birçok kuruluş, Çin merkezli APT41 hacker grubunun saldırılarına maruz kalmıştır.
- **IoC (Indicators of Compromise):**

  FileHash fcff642268898fcf65702a214aefbf9e

  FileHash ac125aea0b703de37980779599438b4a
- **Domain:** www.eloples.com, ios-certificate-update.com, android-system-update.com

Lazarus Group (APT38)

- **Menşei:** Kuzey Kore
- **Bilinen diğer isimleri:** Hidden Cobra, NICKEL, GLADSTONE, Beagleboyz
- **MITRE ATT&CK:** https://attack.mitre.org/groups/G0082/
- **Hedef:** Güney Kore, ABD, Japonya, Türkiye, Hindistan, Avrupa ve Asya ülkeleri
- **Motivasyon:** Teknolojik ve askeri bilgiler çalmak, maddi kazanç elde etmek.
- **Saldırı türleri:** Spear phishing, kötü amaçlı yazılım, bankacılık uygulamaları truva atları, SWIFT sistemleri üzerinden dolandırıcılık, kripto para borsası saldırıları.
- **Saldırı teknikleri:** kimlik avı (T1566), kripto para cüzdanlarını hedef alma (T1213), zararlı yazılımların şifrelenmesi ve gizlenmesi (T1027)
- **2024 Faaliyetleri:** Daha önce iddia edildiği şekilde WannaCry fidye yazılımını üreten bu grup, 2024 yılında Hindistan'da WazirX adı verilen yerel kripto para borsasını hackleyip 234,9 milyon dolar değerinde vurgun gerçekleştirmiştir.
- **Türkiye Faaliyetleri:** 2018 yılında Zeytin Dalı Harekâtı başlamasıyla birlikte Türk finans kuruluşlarına yönelik siber saldırılarda bulunmuşlardır.
- **IoC (Indicators of Compromise):**

  FileHash 5a89aac6c8259abbba2fa2ad3fcefc6e

  FileHash 05da32043b1e3a147de634c550f1954d
- **Domain:** https://www.btcfrog.com/qr/bitcoinpng.php?address, https://www.rentasyventas.com/incluir/rk/imagenes.html

Saldırılarda Kullanılan Programlar

Gelişmiş APT grupları, saldırılarını düzenledikleri zaman hedeflerine erişmek için çeşitli zararlı yazılımları kullanırlar. Bu zararlıları bazen kendileri üretirler, bazen ise öncesinde üretilmiş bir zararlı yazılımı kullanırlar. Bu zararlılar saldırganların amacına göre farklı yeteneklere sahip olabilir; bazıları kimlik bilgisi çalmaya odaklanırken, bazılarıysa sistemlere arka kapı (backdoor) yerleştirerek arka planda gizli erişim sağlamaya veya sistemdeki verileri şifreleyerek fidye talep etmeye yönelik tasarlanmıştır.

Aşağıda, APT grupları tarafından sıkça kullanılan bazı zararlı yazılımlar ve işlevleri yer almaktadır:

MuddyWater – SloughRat: SloughRAT, MuddyWater tarafından Türkiye ve Arap yarımadasındaki ülkeleri hedef almak için kullanılan Windows betik dosyası tabanlı bir Uzaktan Erişim Truva Atı (RAT) olarak öne çıkmaktadır. Çok katmanlı karartma (obfuscation) teknikleri kullanarak gerçek uzantılarını gizler ve çalıştırılabilmesi için belirli bir işlev adına ihtiyaç duyar. Enfekte ettiği sistemlerden bilgi toplayarak, bu bilgileri sabit kodlanmış Komuta ve Kontrol (C2) sunucusuna iletir. Ayrıca, C2 sunucusundan komutlar alarak saldırganın hedef sistem üzerinde uzaktan kontrol sağlamasına olanak tanır. MuddyWater, bazı saldırılarda SloughRAT'ı kullanarak açık kaynaklı bir ters tünelleme aracı olan Lingolo'yu dağıtmış ve böylece hedef sistemdeki bağlantıları kötüye kullanmıştır. SloughRAT, MuddyWater'ın hedef sistemlere uzun süreli erişim sağlamasına, bilgi sızdırmasına ve kötü amaçlı yükleri yaymasına yardımcı olmaktadır.

Charming Kitten – PowerLess: PowerLess Backdoor zararlısı, tespit edilmemek için PowerShell'i doğrudan çalıştırmak yerine .NET bağlamında yürütülen bir arka kapı (backdoor) zararlısıdır. Modüler yapıya sahiptir ve aşamalı olarak yüklenen zararlı bileşenleri içerir. Keylogger ve bilgi çalan yazılımlar gibi ek zararlılar indirebilir.

Çalışma prensibi, PowerShell süreçlerini gizleyerek güvenlik yazılımlarını atlatmak ve şifrelenmiş iletişim ile komuta sunucusuyla bağlantı kurmaktır. Açık kaynaklı kriptografi kütüphaneleri kullanılarak veriler şifrelenir. Zararlı yazılım, hedef sistemde kalıcılık sağlamak ve iz bırakmadan çalışmak için çeşitli teknikler uygular.

Fancy Bear – X-Agent & X-Tunnel: X-Agent, Windows, Linux, iOS ve Android sistemlerine bulaşabilen bir casus yazılım olup, uzaktan komut yürütme, dosya aktarımı ve keylogging yeteneklerine sahiptir. Sistemlere genellikle oltalama saldırılarıyla bulaşır ve bulaştıktan sonra ağ içinde farklı cihazlara yayılabilir. Zararlı yazılımın Android versiyonu, belirli hedeflere yönelik olarak sahte uygulamalar aracılığıyla dağıtılmıştır.

X-Tunnel ise ağ tünelleme aracı olarak kullanılarak NAT arkasındaki sistemlerle bağlantı kurulmasını sağlar ve uzaktan komut yürütmeye olanak tanır. X-Agent ile birlikte çalışarak hedef sistemlerden bilgi sızdırılmasını kolaylaştırır. Saldırganlar, bu araçları dağıtmak için açık kaynaklı RemCOM aracını kullanmış ve olay kaydı temizleme gibi adli analiz karşıtı teknikler uygulamıştır.

Lazarus Group – WannaCry: WannaCry, fidye yazılımlarının çalışma prensiplerini küresel ölçekte gösteren en kritik örneklerden biridir. Bu zararlı yazılım, SMBv1 protokolündeki EternalBlue (CVE-2017-0144) açığını kullanarak sistemlere bulaşır ve ağ içinde solucan mantığıyla yayılabilir.

Bulaşma gerçekleştiğinde, WannaCry hedef sistemde dosyaları RSA ve AES algoritmalarını kullanarak şifreler. Şifrelenen dosyalar için ".WNCRY" uzantısı eklenir ve fidye notu bırakılarak belirli bir Bitcoin adresine ödeme talep edilir. Yazılımın en dikkat çekici özelliklerinden biri, bulaştığı sistemin yerel ağında açık SMB portlarını tarayarak diğer savunmasız cihazlara kendisini otomatik olarak kopyalayabilmesidir.

Zararlı yazılımın bir kill-switch mekanizması içerdiği de keşfedilmiştir. WannaCry, belirli bir alan adına HTTP isteği yapar ve yanıt almazsa çalışmaya devam eder. Ancak, bu alan adı aktif hale getirildiğinde WannaCry'ın yayılma süreci durdurulmuştur. Buna rağmen, SMB açığını kapatmayan sistemlerde zararlının farklı varyantları aktif olmaya devam etmiştir.

WannaCry'ın etkileri, özellikle güncellenmemiş Windows sistemlerinde büyük kayıplara yol açmıştır. Bu tür saldırılar, güvenlik yamalarının zamanında uygulanmasının ve SMB gibi kritik protokollerin ağ içinde dikkatle yönetilmesinin önemini bir kez daha göstermiştir.

Mimikatz: Mimikatz, sistem belleğinden kimlik bilgilerini çıkarabilen ve kimlik doğrulama mekanizmalarını atlatmak için kullanılan bir araçtır. Başlangıçta güvenlik araştırmaları için geliştirilmiş olsa da saldırganlar tarafından yetkisiz erişim, ayrıcalık yükseltme ve yatay hareket gibi amaçlarla aktif olarak kullanılmaktadır.

Mimikatz'ın temel yetenekleri arasında:

Kimlik Bilgisi Çıkarma: LSASS (Local Security Authority Subsystem Service) belleğinden şifre hash'leri, açık metin şifreler ve Kerberos biletleri elde edebilir.

Kimlik Doğrulama Bypass: Pass-the-Hash, Pass-the-Ticket ve Overpass-the-Hash teknikleri ile kimlik doğrulama süreçlerini atlayabilir.

Ayrıcalık Yükseltme: Sistem üzerinde yüksek ayrıcalıklara sahip kullanıcı hesaplarının kimlik bilgilerini ele geçirerek yönetici yetkileri elde edebilir.

Lateral Movement: Ele geçirilen kimlik bilgileri sayesinde ağ içinde farklı sistemlere yayılabilir.

Mimikatz, Metasploit, Cobalt Strike, Empire ve PowerSploit gibi saldırı sonrası araç setlerinde yer almakta olup, hala aktif olarak kullanılmaktadır. İlk olarak 2007 yılında Benjamin Delpy tarafından geliştirilen bu araç, yıllar içinde daha fazla özellik eklenerek saldırganlar için kritik bir bileşen haline gelmiştir. Günümüzde de hem savunma hem de saldırı amaçlı kullanılan en önemli güvenlik araçlarından biridir.

TTP Nedir

TTP, açılımı tactics, techniques ve procedures(taktik, teknik, prosedür) olan APT gruplarının saldırılarına verilen addır. Siber suçluların kullandığı saldırı türlerini açıklamak için kullanılır. Üç kısımdan oluşur: Taktik, teknik ve prosedür. İnternetteki en iyi siber güvenlik kaynaklarından biri olan MITRE ATT&CK sitesinde bu TTP'ler detaylı olarak açıklanır.

Taktik: Bir siber suçlunun davranış ve stratejisinin detaylı açıklaması. Taktik, siber suçlunun hedefine ulaşması için kullandığı davranış ve eylemlerini içerir.

Teknik: Siber suçluların taktikleri kullanmak için uyguladıkları yöntemlerdir. Örneğin kimlik avı saldırısı yapmak (phishing).

Prosedür: Siber suçluların belirli teknikleri uygulama biçimidir. Kullanılan araçları, izlenecek yolları açıklamayı hedefler. Örneğin PowerShell kullanarak bir kodu yürütme yolu.

APT Gruplarının Kullandığı TTP’lerin Türleri

Gelişmiş Kalıcı Tehdit (APT) grupları, hedef sistemleri ele geçirmek, bilgi sızdırmak ve zarar vermek için çeşitli Taktikler, Teknikler ve Prosedürler (TTP'ler) kullanır. Bu TTP'ler, saldırının her aşamasında belirli bir amaca hizmet eder ve genellikle saldırı yaşam döngüsünü oluşturur. Aşağıda bu tür TTP'ler ve her birinin amacı açıklanmaktadır:

Reconnaissance (Keşif): Saldırganlar, hedef hakkında bilgi toplamak için çeşitli teknikler kullanır. Bu aşamada, hedef ağ, sistem veya kullanıcılar hakkında veriler elde edilir. Amaç, saldırıyı planlamak ve hedefin zayıf noktalarını anlamaktır.

Resource Development (Kaynak Geliştirme): Bu aşamada saldırganlar, saldırıyı gerçekleştirmek için gerekli altyapıyı oluşturur. Örneğin, kötü amaçlı yazılım geliştirme, komuta ve kontrol sunucularını kurma veya kimlik bilgilerini ele geçirme gibi faaliyetler gerçekleştirilir.

Initial Access (İlk Erişim): Saldırganlar, hedef sisteme veya ağa ilk kez giriş yapmayı hedefler. Bunun için oltalama (phishing), kötü amaçlı yazılım (malware) veya zafiyetlerin kullanılması gibi yöntemler uygulanabilir.

Execution (Çalıştırma): Hedef sistemde saldırganın yüklediği kod veya komutların çalıştırılmasıdır. Bu aşamada, saldırganlar kötü amaçlı yazılımları etkinleştirir veya sistem üzerinde kontrol sağlamaya çalışır.

Persistence (Kalıcılık): Saldırganlar, hedef sistemde uzun süreli bir varlık oluşturmayı amaçlar. Bunun için arka kapılar (backdoor), kötü amaçlı yazılımlar veya değiştirilmiş yapılandırmalar kullanılır.

Privilege Escalation (Ayrıcalık Yükseltme): Saldırganlar, daha yüksek yetkiler elde ederek sistem üzerinde daha fazla kontrol sağlamayı hedefler. Örneğin, yönetici haklarını ele geçirmek bu aşamaya örnek olabilir.

Defense Evasion (Savunmadan Kaçış): Bu aşamada saldırganlar, güvenlik araçları ve savunma mekanizmalarını atlatmayı hedefler. Örneğin, kötü amaçlı yazılımları şifrelemek veya güvenlik yazılımlarını devre dışı bırakmak bu kapsamdadır.

Credential Access (Kimlik Bilgisi Erişimi): Saldırganlar, kullanıcı adı, şifre veya diğer kimlik doğrulama bilgilerini ele geçirmeye çalışır. Bu bilgiler genellikle daha fazla erişim sağlamak için kullanılır.

Lateral Movement (Yatay Hareket): Saldırganlar, bir sistemden diğerine geçiş yaparak ağda daha geniş bir erişim elde etmeye çalışır. Bu süreçte ele geçirilen kimlik bilgileri veya zafiyetler kullanılır.

Collection (Toplama): Hedef sistemden veya ağdan hassas veriler toplanır. Örneğin, kullanıcı bilgileri, finansal veriler veya ticari sırlar bu aşamada ele geçirilebilir.

Command and Control (Komuta ve Kontrol): Saldırganlar, hedef sistemle iletişim kurmak ve bu sistemi uzaktan kontrol etmek için bir altyapı oluşturur. Genellikle bu iletişim, tespit edilmemek için şifrelenmiş kanallar üzerinden yapılır.

Exfiltration (Dışa Aktarım): Hedef sistemden çalınan verilerin saldırganın kontrolündeki bir dış kaynağa aktarılmasıdır. Bu genellikle şifreli bağlantılar veya meşru hizmetler üzerinden yapılır.

Impact (Etkileme): Saldırganlar, hedef üzerinde belirli bir etki yaratmayı hedefler. Örneğin, sistemleri devre dışı bırakmak, veri bütünlüğünü bozmak veya fidye yazılım saldırıları düzenlemek bu aşamada gerçekleşir.

TTP’lerin Alt Teknikleri

MITRE ATT&CK framework'ü, siber saldırıları belirli taktikler ve bunların altında yer alan alt teknikler üzerinden sınıflandırır. Alt teknikler, saldırganların her bir taktiği gerçekleştirmek için kullandıkları daha özgül yöntemleri ifade eder. Yani, bir taktik, saldırganın genel amacını gösterirken, alt teknikler bu amaca ulaşmak için kullanılan spesifik araçlar ve yolları temsil eder.

Saldırganlar, genellikle daha geniş taktik hedeflerini gerçekleştirmek için alt teknikleri kombinler. Örneğin, Persistence (Kalıcılık) taktiği altında, saldırganlar sistemlere kalıcı erişim sağlamak amacıyla çeşitli alt teknikler kullanabilirler. Bu alt teknikler, sistemin yeniden başlatılması ya da bir saldırı tespit mekanizmasının devreye girmesi durumunda bile, saldırganların erişimini sürdürmelerine olanak tanır.

Alt teknikler, saldırganların kullandığı her bir spesifik saldırı yöntemini tanımlar. Örneğin, T1547 alt tekniği, Persistence sağlamak amacıyla sistemde otomatik olarak çalışan bir hizmet eklemeyi anlatırken, T1059 alt tekniği, komutları çalıştırmak için kullanılan bir saldırı yöntemini belirtir.

Alt tekniklerin analiz edilmesi, saldırganların kullandığı yöntemlerin daha iyi anlaşılmasını sağlar ve bu sayede güvenlik uzmanları, savunma stratejilerini daha hedeflenmiş bir şekilde geliştirebilir. Taktiklerin altında bulunan bu detaylı alt teknikler, siber saldırılara karşı daha etkili savunmalar oluşturmak için kritik öneme sahiptir.

Örneğin, T1087 (Hesap Keşfi) tekniğinin bir alt türü olan T1087.002 (Alan Adı Hesabı) tekniği, saldırganların alan adı hesaplarını listeleyerek özel ayrıcalıklara sahip kullanıcıları hedeflemesine olanak tanır. Bu amaçla, "net user /domain", "net group /domain" ve PowerShell komutları gibi araçlar kullanılabilir. Chimera, bu tekniği uygulamak için "net user /dom" ve "net user Administrator" komutlarını kullanarak alan adı ve yönetici hesaplarını listelemiştir.

T1087(Hesap Keşfi)

Amacı: Sızılan sistemdeki veya Active Directory ortamındaki kullanıcı hesaplarını keşfetmesine yarar. Edinilen bilgi hedef sistemin yapısını anlamaya, yetkili hesapları belirlemeye ve sonraki saldırıda hangi hesaplara saldırılması gerektiğini açıklar.

Uygulanışı: Yerel sistemlerde saldırganlar kullanıcı hesaplarını listelemek için belirli araçları veya komutları kullanırlar. Windows'ta "net user" komutu çalıştırılarak kullanıcı hesapları görüntülenebilir. Linux veya MacOS sistemlerde /etc/passwd dosyasını okuyarak sistemdeki kullanıcılar keşfedilir. Hedef ağda Active Directory kullanılıyorsa, LDAP sorguları veya özel araçlar (örneğin PowerView, BloodHound) kullanılarak geniş çaplı hesap sorgusu yapılabilir. Örnek: "Get-ADUser" PowerShell komutu çalıştırılarak kullanıcı bilgisi çekilebilir.

Zafiyetler: Sistemde veya Active Directory ortamında yetersiz denetim sonucu bırakılmış eski kullanıcı hesapları, hatalı yapılandırılmış erişim izinleri ve zayıf parola politikaları, bu tür saldırıları kolaylaştırabilir.

Potansiyel Sonuçlar: Yetkili hesaplar üzerinden önemli bilgiler çalınabilir. Normal kullanıcılar üzerinden sistem üzerinde fark edilmeden keşif yapılabilir.

Tespit Zorluğu: Sistemin içerisinde yapılan sorgular, sistem yöneticileri tarafından kullanılan sorgularla benzerlik gösterdiği taktirde fark edilmesi zorlaşabilir. Ancak saldırganın kullandığı sorgular yüksek sayıda ve kısa süre içinde sıklıkla tekrar ederse SIEM (Güvenlik Bilgi ve Olay Yönetimi) araçlarında uyarı olarak ortaya çıkabilir.

Gerçek Dünya Örnekleri: Lazarus Group Linux sistemlerde yerel kullanıcı hesaplarını hedef alır ve belirlenen hesaplar arasında lateral movement (yatay hareket) yapar. Fancy Bear (APT28), Active Directory'de keşif yapmak için LDAP sorgularını kullanır.

Alt Teknikleri: T1087.001, T1087.002, T1087.003, T1087.004

T1071 (Uygulama Katmanı Protokolü)

Amacı: Bu teknik, saldırganların sızdıkları sistemde kurduğu iletişimleri normal bir trafik göstermesi amacıyla kullanılır.

Uygulanışı: Sızılan sistemde zararlı yazılımlar çalıştırılarak komuta ve kontrol sunucusuyla haberleşme sağlanır. Genellikle şifrelenmiş (HTTPS) veya gizlenmiş veri paketleri kullanılarak gerçekleştirilir. Örneğin HTTP/HTTPS üzerinden Base64 kodlanan veri kullanılarak C2 iletişimi yapılır.

Zafiyetler: Ağdaki trafiğin analiz edilmemesi veya zayıf ağ izleme araçlarının kullanılması, bu tür sızıntıların fark edilmesini zorlaştırabilir.

Potansiyel Sonuçlar: Saldırganlar kimselere fark edilmeden önemli verileri çalabilir, sistemde uzun süre kalabilir ve hedef ağda geniş çaplı zararlı aktiviteler gerçekleştirebilir.

Tespit Zorluğu: Bu tekniğin tespiti genellikle zordur çünkü saldırganlar, şüpheli gözükmeyen normal protokolleri kullanarak, normal kullanıcı davranışlarını taklit eder. Bazı durumlarda SIEM araçları ve trafik analizi sistemleri anormal iletişim olaylarını tespit edebilir. Örneğin sürekli aynı C2 IP adresine iletişimde bulunma gibi.

Gerçek Dünya Örnekleri: Cozy Bear (APT29), kullandıkları zararlı yazılımları HTTPS üzerinden komuta ve kontrol sunucusuna bağlayabilmek için T1071 tekniğini kullanır.

Alt Teknikler: T1071.001, T1071.002, T1071.003, T1071.004, T1071.005

T1059 (Komut ve Komut Dosyası Yorumlayıcısı)

Amacı: Betik yorumlayıcısı ve komut satırı kullanımıyla hedef ağda veya sistemde komut çalıştırmak, zararlı işlemler yapmak ve kontrol sağlamak için kullanılır. Bu teknik sayesinde saldırganlar, sistemde keşif yapabilir, yetki yükseltebilir ve zararlı uygulamalarını çalıştırabilirler.

Uygulanışı: Windows'ta Komut istemcisi cmd.exe veya PowerShell gibi araçlar, Linux'ta ise bash kullanılarak uygulanır.

Zafiyetler: Hatalı yapılandırılmış izin politikaları ve komut satırı erişiminin sınırlandırılmaması bu tekniği uygulanabilir yapmaktadır.

Potansiyel Sonuçlar: Yetkisiz erişim, oluşabilecek veri kaybına, zararlı yazılım çalıştırılmasına ve sistem üzerinde tam kontrol erişim edilmesine yol açabilir.

Tespit Zorluğu: Çalıştırılan komutlar, sistemin yöneticilerinin komutlarına benzerlik gösterdiği için bunların tespiti zordur. Fakat sistem günlüklerinin (log) sürekli analiz edilmesi saldırıları tespit etmede işe yarayabilir.

Gerçek Dünya Örnekleri: Chafer (AP39) ve MuddyWater gibi APT grupları, hedef sisteme erişim sağlamak için PowerShell kullanarak bu tekniği kullanmıştır.

Alt Teknikler: T1059.001, T1059.002, T1059.003, T1059.004, T1059.005, T1059.006, T1059.007, T1059.008, T1059.009, T1059.010, T1059.011

T1555 (Parola Yöneticilerinden Kimlik Bilgileri Keşfi)

Amacı: Parola yöneticilerinde saklanan kimlik bilgilerini ele geçirmeye yöneliktir. Bu teknik sayesinde önemli yetkilere sahip hesaplara ulaşılabilir ve sistemde yetki sahibi olunabilir.

Uygulanışı: Parola yönetim araçlarının güvenlik açıklarını veya yapılandırma zafiyetlerini istismar ederek kimlik bilgilerini ele geçirir. Örneğin Windows kullanılan sistemlerde "cmdkey" komutu veya Mimikatz gibi araçlar kullanılarak yerel olarak saklanılan hesap bilgilerine ulaşılabilir. Aynı zamanda Google Chrome ve Mozilla Firefox gibi tarayıcılarda kullanılan parola yöneticisi depolarına uygun komutlar ve saldırılar da gerçekleştirilebilir.

Zafiyetler: Parola yönetim araçlarının eksik veya hatalı yapılandırılması ve zayıf erişim politikalarına sahip olunması bu zafiyete yol açabilir.

Potansiyel Sonuçlar: Saldırganlar ele geçirdikleri parola ve hesaplarla sistemde erişim elde edebilir, hassas bilgilere ulaşabilir veya ağda yatay hareket (lateral movement) yapabilir, bunun sonucunda şirketi büyük zarara uğratabilir.

Tespit Zorluğu: Parola yöneticilerinin hedef alınması, yerel olarak yürütüldüğünden tespit edilmesi epey zor olabilir. SIEM araçları ve sistem günlükleri, parola veya hesap çalma girişimlerinin algılanmasına yardımcı olabilir.

Gerçek Dünya Örnekleri: APT41, hedeflerinin hesap bilgilerini, şifrelenmiş ya da düz metin halde bulunan parolaları veri tabanlarından elde etmiştir. Bir başka saldırılarında BrowserGhost aracını kullanarak tarayıcılarda saklanan parolaları ele geçirmişlerdir. Bu yöntemde, normal kullanıcılar bir sisteme şifrelerini girdiklerinde otomatik doldurma özelliğini aktif ettikleri için saldırganlar tarafından hedef haline gelmişlerdir.

Alt Teknikler: T1555.001, T1555.002, T1555.003, T1555.004, T1555.005, T1555.006

T1573 (Şifrelenmiş Kanal)

Amacı: Hedef sistemle komuta ve kontrol (C2) sunucusu arasındaki iletişimi gizli tutmak adına şifrelenmiş kanallar kullanır. Bu yöntem WireShark gibi ağ trafiği analiz araçlarının bu iletişimdeki zararlı görülebilecek hareketleri görmesini engellemeye çalışmaktadır.

Uygulanışı: Bahsedilen şifreli kanallar, genellikle TLS/SSL gibi protokoller kullanılarak veya özel şifreleme algoritmaları kullanılarak oluşturulur. Hedef sistemde çalıştırılacak olan zararlı yazılımlar bu şekilde şifrelenmeye uyumlu olarak tasarlanır ve kullanılır.

Zafiyetler: Şifreli ağ trafiğinin içeriğini analiz etmek için gerekli araçların eksikliği veya yanlış yapılandırılmış olması sistemde gezinen saldırganları fark etmeyi imkânsız hale getirebilir.

Potansiyel Sonuçlar: Şifrelenmiş kanallardan sızıp içeride fark edilmeden bulunan saldırganlar, uzun süre kimse tarafından fark edilmeden sistem içinde kalabilir.

Tespit Zorluğu: Şifrelenen trafik genellikle sistem yöneticilerinin hareketleriyle aynı gözüktüğünden dolayı tespit edilmesi epey zordur. Ama saldırgan yoğunlukta trafik veya sürekli aynı sunucularla iletişim kuruyorsa, anomali tespitiyle yakalanması mümkün olabilir.

Gerçek Dünya Örnekleri: Cozy Bear (APT29) grubu, C2 komuta kontrol iletişimlerini gizli tutmak için şifrelenmiş protokoller kullanarak içine sızdıkları sistemlerde uzun süre kalmayı başarmışlardır. Bu sürede hassas bilgileri de ele geçirmişlerdir.

Alt Teknikler: T1573.001, T1573.002

T1027 (Kod Karartma - Obfuscation)

Amacı: Saldırganlar, zararlı yazılımlarını veya komutlarını tespit edilmekten kaçınmak için kod karartma (obfuscation) tekniklerini kullanır. Bu teknikler, saldırganların eylemlerini gizlemesine yardımcı olur ve güvenlik araçlarının zararlı içerikleri analiz etmesini zorlaştırır. Kod karartma, genellikle kötü amaçlı yazılımların kaynak kodunu, betiklerini veya komutlarını karmaşıklaştırarak okunabilirliğini azaltmayı hedefler.

Uygulanışı: PowerShell komutlarını Base64 ile şifreleme, zararlı dosyaları sıkıştırma ya da şifreleme gibi yöntemlerle kod karartma gerçekleştirilir. Ayrıca, Invoke-Obfuscation gibi araçlarla komutlar karmaşıklaştırılabilir veya VMProtect gibi yazılımlar kullanılarak dosyalar gizlenebilir.

Zafiyetler: Şifrelenmiş veya sıkıştırılmış içerikleri analiz edemeyen güvenlik araçları bu tekniklere karşı savunmasızdır.

Potansiyel Sonuçlar: Saldırganlar, tespit edilmeden zararlı yazılımlarını çalıştırabilir ve güvenlik çözümlerini aşarak saldırılarını başarıyla gerçekleştirebilir.

Tespit Zorluğu: Kod karartma yöntemleri genellikle yasal dosya ve komutlar gibi görünmek üzere tasarlandığından tespit edilmesi zordur. Ancak, şüpheli Base64 şifrelemeleri, olağandışı derecede karmaşık PowerShell komutları ve sıkıştırılmış dosyalar üzerindeki olağandışı aktiviteler tespit için ipuçları sağlayabilir.

Gerçek Dünya Örnekleri: APT41, VMProtected dosyalar kullanmıştır. MuddyWater, Invoke-Obfuscation ve Base64 teknikleriyle PowerShell komutlarını karartmıştır.

Alt Teknikler: T1027.001, T1027.002, T1027.003, T1027.004, T1027.005, T1027.006, T1027.007, T1027.008, T1027.009, T1027.010, T1027.011, T1027.012, T1027.013, T1027.014

T1048 (Alternatif Protokol Üzerinden Veri Sızdırma)

Amacı: Bu teknik sızılan sistemden tespit edilmeden veri çalmak için kullanılır. Özellikle bu teknik ağ izleme araçlarını atlatmak için iyi bir tercihtir.

Uygulanışı: Veriler ağ dışı yöntemlerle (örneğin, çıkarılabilir medya, yazıcılar ve taşınabilir cihazlar) sistemden elde edilir. Ayrıca bu veriler genellikle şifrelenmiş şekilde depolanır ve taşınır.

Zafiyetler: Örnek olarak ofisin yeterli güvenlik önlemlerinin alınmaması, dışarıdan herhangi bir kişinin fiziki bir şekilde gelip sistemlere yetkisiz erişim sağlamasına sebep olur.

Potansiyel Sonuçlar: Verilerin bu şekilde elde edilmesi, kritik bilgilerin çalınmasına ve müşteri bilgilerinin sızdırılmasına sebep olabilir. Bu kayıp, şirketin itibarını kaybetmesine, hukuki cezalar çekmesine ve finansal kayıp yaşamasına sebep olabilir.

Tespit Zorluğu: Bu yöntem fiziksel olarak yapıldığı için ağ tabanlı güvenlik araçları tarafından tespit edilemez. Ancak, çıkarılabilir medyanın kullanımını izlemek, fiziksel güvenliği artırmak ve DLP (Data Loss Prevention) çözümleri kullanmak bu saldırılardan etkilenme oranını azaltabilir.

Gerçek Dünya Örnekleri: OilRig, ele geçirdiği verileri birincil C2 kanalından farklı olarak FTP üzerinden sızdırmıştır. Bu tekniği Türkiye saldırılarına kullandıkları düşünülmektedir.

Alt Teknikler: T1048.001, T1048.002, T1048.003

T1566 (Phishing - Oltalama)

Amacı: Bu teknik sıklıkla kimlik bilgisi ele geçirme veya hedef sistem üzerinde zararlı yazılım çalıştırma gibi amaçlarla yapılır. Bir sosyal mühendislik türüdür karşıdaki kişiyi e-postalar, mesaj veya telefon araması yöntemiyle aldatmaya dayalı bir tekniktir.

Uygulanışı: Saldırganlar kurbanlarına ulaşmak için farklı yöntemler kullanır. Örneğin sahte e-postalar, telefon mesajı, telefon araması veya sahte web siteleri bunlara örnek gösterilebilir. Genellikle aciliyet duygusu içerir, kurban bu tuzağa yakalandığında önemli bilgilerini saldırganlara çaldırmış olur.

Zafiyetler: Kullanıcıların kendisine gelen mesaj, arama, sahte web sitesi ve e-postaları dikkatli incelememesi bu tuzağa yakalanmalarına sebep olabilir.

Potansiyel Sonuçlar: Çalınan bilgilerle ne yapılacağı bilgiden bilgiye değişitr. Örneğin kredi kartı bilgileri çalınmışsa bu kart kullanılıp alışveriş yapılabilir. Bir iş mailinin bilgileri çalınmışsa o çalışana gelen ve giden maillere bakılabilir. Hatta çalınan iş maili üzerinden başka çalışanlar kandırılabilir.

Tespit Zorluğu: Bu yöntem genellikle düşük tespit oranına sahiptir çünkü saldırgan rolünü çok iyi bir şekilde gerçekleştirir. Bu tarz saldırılardan korunmak için şirket içerisinde siber güvenlik farkındalığı adı altında eğitimler verilebilir.

Gerçek Dünya Örnekleri: OilRig grubu düzenledikleri saldırılarda genellikle e-posta yöntemiyle hedeflerine ulaşmaya çalıştığı gözlenmiştir.

Alt Teknikler: T1566.001, T1566.002, T1566.003, T1566.004

T1204 (Kullanıcı Tarafından Zararlı Yazılım Yürütme)

Amacı: Sosyal mühendislik türü olan bu saldırı, kullanıcının bilgisayarına sızdırılan dosyayı açmaya ikna edilmesini amaçlar. Kullanıcı bu zararlı dosyayı çalıştırırsa, sistemi saldırganların eline geçirmiş olur.

Uygulanışı: Bu saldırı genellikle e-posta ekleriyle, sahte web siteleriyle veya bazen de USB aygıtlar ile sisteme aktarılan zararlı yazılımlar aracılığıyla yapılır. Bu zararlı yazılımlar sistem kullanıcısı tarafından çalıştırıldığında, saldırganlar sisteme erişmiş olur.

Zafiyetler: Siber güvenlik farkındalığının düşük olması bu tarz saldırılara maruz kalmayı artırabilir.

Potansiyel Sonuçlar: Kullanıcılar, sisteme illegal yollardan sokulan bu zararlı yazılımları çalıştırırlarsa, önemli ve hassas bilgiler çalınabilir, maddi zarar yaşanabilir ve sistem çökebilir.

Tespit Zorluğu: Bu teknik kullanıcı davranışına bağlı bir teknik olduğu için başta fark edilmesi zor olabilir. Ancak, kullanıcı siber güvenlik farkındalığına sahipse ve sistemlerde bu virüsleri tarayabilecek bir yazılım varsa zarar yaşanmadan bu durumun içinden çıkılabilir.

Gerçek Dünya Örnekleri: Fancy Bear (APT28), hedeflerine sahte web sitesine yönlendiren e-posta iletileri gönderdi. Aynı zamanda başka saldırılarında tekrar e-posta yoluyla sahte Microsoft Office ekleri göndererek bu saldırıyı gerçekleştirmeye çalıştılar.

Alt Teknikler: T1204.001, T1204.002, T1204.003

T1547 (Otomatik Başlatma)

Amacı: Bu teknik, kullanıcı sistemi açtığında zararlı yazılımın arka planda sistem tarafından otomatik olarak çalıştırması için kullanılır. Bu sayede uzun süreli sistemden bilgi çekilebilir.

Uygulanışı: Windows sistemlerde kayıt defteri girdilerinin ayarlarıyla çeşitli oynamalar yapıldığında bu teknik etkinleştirilebilir. MacOS sistemlerde ise launchd plist dosyalarıyla oynama yapıldığında bu teknik etkinleştirilebilir.

Zafiyetler: Zayıf erişim politikaları ve kullanıcı farkındalığının düşük olması bu tekniğin arka planda gizlice çalışmasına sebep olur.

Potansiyel Sonuçlar: Arka planda çalışan zararlı yazılımlar fark edilmediği taktirde uzun süre sistemde faaliyet gösterebilir. Bu süre içinde saldırganlar, sistemden istedikleri bilgileri kolayca elde edebilirler.

Tespit Zorluğu: Kayıt defteri girdileri düzenli olarak denetlenmezse bu tekniğin fark edilmesi zorlaşabilir. Bunun tespit edilmesi için uç nokta güvenliği araçları ve başlangıç yapılandırma izleyicileri kullanılabilir.

Gerçek Dünya Örnekleri: MuddyWater, sızdıkları sistemlerde kalıcılığı sağlamak için HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SystemTextEncoding kayıt defteri anahtarını eklemiştir. Aynı şekilde PROMETHIUM grubu da kalıcılık elde etmek amacıyla kayıt defteri anahtarlarını kullanmıştır.

Alt Teknikler: T1547.001, T1547.002, T1547.003, T1547.004, T1547.005, T1547.006, T1547.007, T1547.008, T1547.009, T1547.010, T1547.012, T1547.013, T1547.014, T1547.015

T1047 (Windows Yönetim Araçları - WMI)

Amacı: Saldırganlar bu Windows servisini, hedef sistemde zararlı komutlar yürütmek, bilgi çalmak ve zararlı yazılımları yaymak için kullanır. WMI, sistem yönetimi için kullanılan bir araç olduğundan, bu saldırıları fark etmek zor olabilir.

Uygulanışı: WMI kullanılarak uzaktan komut çalıştırılabilir. Örneğin, "wmic process call create" komutu çalıştırıldığında sistemde zararlı bir yazılım başlatılabilir. "Get-WmiObject" komutu çalıştırılıp sistemde aktif çalışan işlemleri, servisleri ve kullanıcı bilgileri elde edilebilir. WMI Event Subscriptions özelliği kullanılarak zararlı yazılımlar kalıcı hale getirilebilir.

Zafiyetler: WMI genellikle sistem yöneticisi tarafından düzenlenebilir. Ancak, sistem yöneticisinin hesabı ele geçirildiyse veya zayıf erişim denetimleri varsa bu teknik rahatlıkla uygulanabilir.

Potansiyel Sonuçlar: Saldırıya uğrayan sistemlerde uzaktan kontrol sağlanabilir, hassas bilgiler ele geçirilebilir, kalıcılık elde edilebilir, ağ içinde yatay hareket yapılabilir ve daha fazla sisteme erişim sağlanabilir.

Tespit Zorluğu: WMI sistem yöneticileri tarafından sıkça kullanıldığından, saldırganların yaptığı hareketleri gizlemesi kolaydır. Bunun tespiti için SIEM araçları ve günlük analizleri kontrol edilirse anormal WMI kullanımı tespit edilebilir. Örneğin beklenmeye saatlerde veya yüksek sayıda WMI sorgusu kullanılırsa bu hareketler şüphe uyandırabilir.

Gerçek Dünya Örnekleri: APT32, uzaktan komut çalıştırmak için bu yönteme başvurmuştur. APT41 grubu ise, bu tekniği bilgi toplamak ve zararlı yazılımları yaymak için kullanmıştır.

Alt Teknikler: Bu tekniğin herhangi bir alt tekniği bulunmamaktadır.

T1548 (Erişim Kontrolünü Atlatma)

Amacı: Bu teknik saldırıya uğramış sistemde yetki artırmak veya mevcut kısıtlamaları atlatarak hassas bilgilere erişim sağlamak için kullanılır.

Uygulanışı: Windows sistemlerde "RunAs", Linux sistemlerde ise "sudo" gibi komutlarla meşru kullanıcıyı taklit ederek komutlar yönetici olarak çalıştırılabilir.

Zafiyetler: Zayıf kimlik doğrulama yöntemleri, yanlış veya eksik erişim politikaları sistemi bu tarz saldırılara açık hale getirir.

Potansiyel Sonuçlar: Bu teknik başarılı olarak uygulandığında sistemde zararlı yazılımlar çalıştırılabilir, hassas bilgiler çalınabilir ve sistem üzerinde tam kontrol elde edilebilir.

Tespit Zorluğu: Yetki yükseltme veya kimlik sahteciliği dediğimiz bu olay gerçekleşirse fark edilmesi zor olabilir çünkü genellikle sistem yöneticilerinin aktivitelerini taklit eder. Ancak SIEM araçları veya güvenlik günlüğü, bu yetki yükseltme girişimlerini fark edebilir.

Gerçek Dünya Örnekleri: MuddyWater geçmişte yaptığı saldırılarda User Account Protocol (UAC) atlatmak için çeşitli teknikler kullanmıştır.

Alt Teknikler: T1548.001, T1548.002, T1548.003, T1548.004, T1548.005, T1548.006

T1056 (Giriş Yakalama - KeyLogger)

Amacı: Bu teknik bir bilgi toplama tekniğidir. Sızılan sistemde kullanıcının klavye kullanımını kayıt etmeye yarar. Aynı zamanda buna keylogger denir.

Uygulanışı: Örneğin bir phishing (oltalama) maili ile sisteme keylogger yüklendiğinde Windows hizmetlerinde zararlı bir hizmet oluşturulur ve klavye vuruşları kayıt edilmeye başlanır.

Zafiyetler: Kullanıcıların dikkatsizce yazılım yükleyip çalıştırmaları bu tür saldırılara yol açabilir. Örneğin lisans ücreti ödememek için herhangi bir siteden indirilen programın içinde keylogger saklı olabilir

Potansiyel Sonuçlar: Saldırı sonucu toplanan bilgiler, saldırganların çok hassas bilgilere erişmesine sebep olabilir.

Tespit Zorluğu: Keylogger yazılımlar arka planda gizlice çalışır bu yüzden fark edilmesi zor olabilir. Ancak güvenlik duvarları, SIEM araçları sistemde doğru bir şekilde yapılandırılmışsa bunların önüne geçilebilir.

Gerçek Dünya Örnekleri: Chafer (APT39), hem klavye hem de fare hareketlerini takip etmek için bu tekniği uygulamıştır.

Alt Teknikler: T1056.001, T1056.002, T1056.003, T1056.004

T1190 (Zafiyetli Uygulamalardan Yaranma)

Amacı: Bu teknik, güvenlik açığı içeren zafiyetli uygulamaların saldırganlar tarafından nasıl sömürüldüğünü gösterir. Herhangi zafiyetli bir uygulamadaki güvenlik açığı saldırganlar tarafından sömürülerek büyük zararlara yol açabilir.

Uygulanışı: Saldırganlar, öncelikle hedef sistemdeki genel erişime açık uygulamaları tarayarak potansiyel güvenlik açıklarını tespit eder. Örneğin, Fortinet FortiOS VPN'deki CVE-2018-13379 gibi bir açık kullanıldığında, saldırgan, hedef cihazın SSL VPN portalına erişerek sistemden hassas dosyaları indirebilir. Bu dosyalar, kullanıcı adı ve parola gibi kimlik bilgilerini içerebilir. Saldırgan bu bilgileri kullanarak hedef sisteme yetkisiz erişim sağlar ve sistemde derinlemesine keşif veya veri sızdırma gibi işlemler yapabilir.

Zafiyetler: Güncel olmayan yazılımlar, eksik güvenlik yamaları veya internete açık ve savunmasız servislerin bulunması, sistemi bu tür saldırılara karşı daha elverişli yapar.

Potansiyel Sonuçlar: Bu teknik uygulandığında, sistemde zarara yol açabilir, hassas bilgiler çalınabilir veya diğer sistemlere sızılabilir. Bunlar da bir şirket için büyük kayıpların yaşanmasına sebep olur.

Tespit Zorluğu: Uygulamalarda oluşan zafiyetler, kurumun bilgisi dışında gerçekleştiği için bunun tespiti zor olabilir. Ancak, log analizleri ve SIEM araçları detaylı ve düzgün bir biçimde incelenirse bu saldırılardan etkilenme oranı düşebilir. Aynı zamanda güncellemeler eksiksiz ve hızlı bir şekilde yapılırsa aynı şekilde bu saldırılardan etkilenme oranı ciddi oranda düşer.

Gerçek Dünya Örnekleri: Cozy Bear (APT29), Citrix'teki CVE-2019-19781 ve FortiGate VPN'deki CVE-2018-13379 gibi açıkları kullanarak saldırılar gerçekleştirmişlerdir.

Alt Teknikler: Bu tekniğin herhangi bir alt tekniği bulunmamaktadır.

T1590 (Ağ Yapısı Hakkında Bilgisi Toplama)

Amacı: Bu teknik, saldırganların hedef sistemin ağ altyapısı, güvenlik sistemleri, iş akışları veya çalışan bilgileri gibi kritik detayları tespit ederek daha isabetli ve etkili saldırılar gerçekleştirmesini sağlamayı amaçlamaktadır.

Uygulanışı: Hedef şirketin DNS kayıtlarını, IP adreslerini ve alt alan adı kayıtlarını incelemek için "whois" ve "sublist3r" gibi araçlar kullanılabilir. Shodan ve ZoomEye gibi arama motorlarıyla hedefin internete açık servislerini, cihazlarını ve yapılandırması tespit edilebilir.

Zafiyetler: Hedef şirket, yayınladıkları iş ilanlarında kullandıkları teknolojiler, e-posta adresleri veya proje detaylarını açık bir şekilde belli etmesi, çalışanlarının sosyal medyada çalıştıkları ofis hakkında gönderiler paylaşması ve kullandıkları teknolojiler hakkında paylaşımlarda bulunması şirket için zafiyet oluşturabilir.

Potansiyel Sonuçlar: Saldırganlar topladıkları tüm bilgilerle hedef şirketin ağ yapısını modelleyebilir, zafiyetlerini tespit veya tahmin edebilir ve sosyal mühendislik saldırıları planlayabilir.

Tespit Zorluğu: Hedeften bilgi toplama aşaması diğer yöntemlere göre ağ dışında gerçekleştiği için fark edilmesi çok zordur. Ancak aktif olarak tarama araçları kullanılıyorsa veya DNS sorguları çok sık gerçekleşiyorsa SIEM araçları bu anormalliği tespit edip alarm verebilir. Örneğin aynı IP adresinden yoğun DNS sorgusu gelmesi veya yoğun alt alan adı keşfi yapılması SIEM araçlarının uyarı vermesine sebep olabilir.

Gerçek Dünya Örnekleri: Turla grubu, 2022'de yaptıkları bir keşif kampanyasında, hedefin Microsoft Word uygulamasının sürüm ve türünü belirlemek için HTTP üzerinden kendi kontrolündeki sunucuya istek gönderen belgeler kullanmıştır.

Alt Teknikler: T1590.001, T1590.002, T1590.003, T1590.004, T1590.005, T1590.006

T1078 (Ele Geçirilmiş Kullanıcı Üzerinden Saldırı)

Amacı: Bu teknik, saldırganların ele geçirdikleri kullanıcı hesaplarını kullanarak hedef sistemlere yetkili bir kullanıcı gibi erişim sağlamayı, bu şekilde sistem üzerinde komutlar çalıştırmayı, veri çalmayı ve daha fazla yetki kazanmayı amaçlar.

Uygulanışı: Saldırganlar ele geçirmek istedikleri kullanıcıları phishing, credential dumping veya brute force gibi saldırılarla elde ettikten sonra sisteme saldırı aşamasına geçerler.

Zafiyetler: Sistemdeki kullanıcıların zayıf veya tahmin edilebilir parolalar kullanmaları, çok faktörlü kimlik doğrulamasını (MFA) kapalı tutmaları ve phishing gibi yöntemlere karşı bilinçsiz olmaları bu tarz saldırılara karşı onları saldırıya açık hale getirir.

Potansiyel Sonuçlar: Saldırganlar, sistemde oturum açtıktan sonra veri çalabilir, diğer kullanıcıları ve yetkilerini düzenleyebilir, ağda yatay hareket yaparak diğer cihaz veya sistemlere erişebilir.

Tespit Zorluğu: Gizlice çalınan bu hesapların kullanılması normal bir kullanıcı gibi gözüktüğünden tespit edilmesi zor olabilir. Ancak aynı hesaba farklı IP'lerden giriş yapılıyorsa, normalden daha fazla veya normal olmayan saatlerde giriş yapılıyorsa ve sistem günlüklerinde hesap kullanımı detaylarına düzenli ve dikkatli bakılırsa bu saldırının tespiti mümkün olabilir.

Gerçek Dünya Örnekleri: Cozy Bear (APT28), phishing yoluyla ele geçirilen kimlik bilgilerini kullanarak DCCC ağına erişim sağlamış ve bu erişimi sürdürmüştür. Ayrıca, IoT cihazlarındaki varsayılan şifreleri kullanarak kurumsal ağlara giriş yapmıştır.

Alt Teknikler: T1078.001, T1078.002, T1078.003, T1078.004

T1110 (Kaba Kuvvet Saldırısı – Brute Force)

Amacı: Bu teknik, saldırganların hedef sistemdeki kullanıcı hesaplarına yetkisiz erişim sağlamak için kaba kuvvet yani brute force saldırıları, parola tahmin etme veya parolaların kriptografik çözümlenmesi gibi yöntemlerle kimlik bilgilerini ele geçirmeyi amaçlamaktadır.

Uygulanışı: Saldırganlar ele geçirdikleri kullanıcı adı veya e-postalara erişim sağlamak için bu yönteme başvururlar. Örneğin Kali Linux işletim sisteminde bulunan dünyada açığa çıkmış tüm parolaların bulunduğu rockyou.txt dosyasıyla bir kullanıcı adına veya e-posta hesabının parolasını kırmak için kaba kuvvet saldırısı yapılabilir.

Zafiyetler: Kullanıcıların zayıf parolalar seçmesi, tahmin edilebilir parolalar seçmesi ve çok faktörlü kimlik doğrulamasını kullanmamaları onları saldırıya elverişli hale getirir.

Potansiyel Sonuçlar: Saldırganlar, brute force saldırısı yaparak ele geçirdiği hesaplara eriştikten sonra istedikleri tüm işlemleri gerçekleştirebilirler.

Tespit Zorluğu: Brute force saldırısı bir hesaba sürekli giriş denemesi yaptığı için her bir başarısız oturum açma girişimi, loglar aracılığıyla veya SIEM araçlarıyla fark edilebilir. Ancak saldırganlar bu saldırıyı yavaş bir şekilde gerçekleştirirse fark edilmesi zorlaşabilir fakat işlemi yavaşlatmak, parolayı kırmak için gereken süreyi epey artıracaktır.

Gerçek Dünya Örnekleri: OilRig, kimlik bilgilerini ele geçirmek için brute force tekniklerini kullanmıştır. Ayrıca Chafer (AP39) grubu, Ncrack aracı ile çeşitli saldırılar yapmıştır.

Alt Teknikler: T1110.001, T1110.002, T1110.003, T1110.004

T1098 (Hesap Manipülasyonu)

Amacı: Saldırganlar, sistemdeki ele geçirdikleri hesapların yetkilerini artırabilir ve yeni kullanıcılar oluşturarak sistemde kalıcı olarak kalmayı amaçlarlar.

Uygulanışı: Saldırganlar ele geçirdikleri hesapları kullanarak önce kendi yetkilerini yükseltirler ve sonrasında yeni hesaplar açarak kalıcı olmayı hedeflerler. Örneğin, Active Directory ortamlarında sahte hesaplar oluşturarak sistem yönetimi erişimleri sağlanabilir.

Zafiyetler: Zayıf ve tahmin edilebilir parola kullanmak bu hesapların çalınmasına sebep olabilir. Yönetici hesaplarının kötü korunması ve çok faktörlü kimlik doğrulama kullanılmaması da bu tarz saldırılara davetiye çıkarabilir.

Potansiyel Sonuçlar: Saldırganlar ele geçirilen hesapları kullanarak kalıcılık elde edebilirler, hassas bilgiler çalabilirler ve yatay hareket yaparak ağa daha fazla hasar verebilirler.

Tespit Zorluğu: Hesap manipülasyonu, genellikle hedef sistemin normal kullanıcı yönetim işlemleri gibi görünebilir. Bu nedenle fark edilmesi zordur. Ancak anormal hesap etkinlikleri veya yeni oluşturulan hesapların izlenmesi, bu tür faaliyetlerin tespit edilmesine yardımcı olabilir.

Gerçek Dünya Örnekleri: OilRig, kimlik bilgilerini ele geçirmek için brute force tekniklerini kullanmıştır. Ayrıca Chafer (AP39) grubu, Ncrack aracı ile çeşitli saldırılar yapmıştır.

Alt Teknikler: T1098.001, T1098.002, T1098.003, T1098.004, T1098.005, T1098.006, T1098.007

T1505 (Sunucu Yazılımlarının İstismarı)

Amacı: Saldırganlar, sunucularda bulunan ve yazılımın işlevselliğini genişletmek için kullanılan özellikleri kötüye kullanarak sistemlere kalıcı erişim sağlamayı hedefler. Sunucu yazılımları, ek yazılımlar veya kodlar eklenerek yeni işlevler kazandırılabilir. Saldırganlar, bu özelliği kullanarak sisteme zararlı yazılımlar yükleyebilir ve sunucunun normal işleyişini bozarak kendi amaçları doğrultusunda kontrol edebilir.

Uygulanışı: Saldırganlar, hedefin web sunucusuna zararlı kod ekleyerek (örneğin, web shell yerleştirerek) hizmetin işlevselliğini kendi amaçları doğrultusunda manipüle edebilirler. Başka bir örnekte, bulut ortamlarında veya SaaS platformlarında uygulama hizmetlerini kötüye kullanarak hedef sistemler üzerinde saldırılar gerçekleştirilebilir.

Zafiyetler: Güvenlik yaması eksik olan veya güncellenmemiş sistemler bu saldırıya karşı zayıf gözükecektir. Aynı zamanda yanlış yapılandırılmış, korunmayan ve erişim politikası yanlış yapılandırılmış sistemler de bu saldırıya karşı savunmasız olacaktır.

Potansiyel Sonuçlar: Saldırganlar bu hizmetleri, kendilerine uyacak şekilde yeniden düzenledikleri zaman başarılı bir şekilde sistemde kalıcılık elde edeceklerdir. Sadece kalıcılık elde etmekle kalmayıp, hassas verileri çalabilir, sistemi çöktürebilir ve diğer sistemlere de sızarak hedef şirketin itibarını zedeleyecektir.

Tespit Zorluğu: Bu saldırı, genellikle normal sistem işlemleri gibi gözüktüğünden fark edilmesi zor olacaktır. Ancak olağandışı ağ trafikleri, yapılandırmalarda beklenmedik değişiklikler veya daha önce sistemde bulunmayan yeni oluşturulmuş bilinmeyen dosyaların tespiti bu tür saldırıları tespit etmeye yarayabilir.

Gerçek Dünya Örnekleri: OilRig grubu, hedef ağlara erişimini sürdürmek için sıklıkla web shell kullanmıştır. Ayrıca, Lazarus Grubu, Operation Dream Job sırasında Internet Information Systems (IIS) üzerinde çalışan Windows sunucularını hedef alarak Komuta ve Kontrol (C2) bileşenleri yüklemiştir.

Alt Teknikler: T1505.001, T1505.002, T1505.003, T1505.004, T1505.005

T1569 (Sistem Hizmetlerini Yürütme)

Amacı: Bu teknik, saldırganların sistem hizmetlerini kullanarak zararlı yazılımları çalıştırmalarını veya belirli işlemleri başlatmalarını sağlar. Sistem hizmetleri, genellikle yönetici yetkileriyle çalıştığından, saldırganlar bu yetkileri istismar ederek hedef sistemde daha fazla bilgiye erişim sağlar.

Uygulanışı: Bu teknik, kötü amaçlı içerik yürütmek için hizmet kontrol araçlarının (örneğin, sc.exe, Net veya PsExec) kötüye kullanılmasıyla gerçekleştirilir. Saldırganlar, yeni bir hizmet oluşturup çalıştırabilir, mevcut bir hizmeti kötüye kullanabilir veya geçici bir hizmet oluşturarak komutlarını yürütmek için kullanabilir. Örneğin, PsExec aracı, uzak sistemlerde komut çalıştırmak için hizmet kontrol yöneticisi API'sini kullanır.

Zafiyetler: Hedef sistemde güvenlik yapılandırmalarının eksik olması, hizmetlerin yanlış yapılandırılması veya gereksiz yere çalışan hizmetlerin korunmasız bırakılması bu tekniğin başarıyla uygulanmasına yol açabilir.

Potansiyel Sonuçlar: Bu teknikle, saldırganlar sistem üzerinde hızlı bir şekilde komutlarını yürütebilir, zararlı yazılımlarını etkinleştirebilir ve yetkilerini artırabilir. Aynı zamanda, bu yöntem saldırının ileri aşamalarında (örneğin, veri sızdırma veya yatay hareket) kullanılabilecek ek avantajlar sağlar.

Tespit Zorluğu: Sistem hizmetlerinin çalıştırılması genellikle meşru bir işlem gibi göründüğünden, bu tür bir saldırının fark edilmesi zordur. Ancak olağan dışı hizmet etkinlikleri, beklenmeyen yapılandırma değişiklikleri veya sistem loglarında anormal girişler bu saldırıyı tespit etmede ipucu olabilir.

Gerçek Dünya Örnekleri: APT41 grubu, zararlı bir yükleyiciyi çalıştırmak için svchost.exe ve Net araçlarını kullanmıştır. Aynı zamanda DUST adlı zararlı yazılımını çalıştırmak için Windows hizmetlerini kötüye kullanmışlardır.

Alt Teknikler: T1569.001, T1569.002

T1574 (Çalıştırma Sürecinin Manipülasyonu)

Amacı: Saldırganlar, sistemdeki programların veya hizmetlerin çalıştırma sürecine müdahale ederek kendi zararlı yazılımlarını devreye sokmayı hedefler. Bu teknikle, meşru görünen işlemleri kullanarak saldırganların zararlı kodlarını çalıştırmaları sağlanır.

Uygulanışı: Bu teknik, genellikle bir uygulamanın kullandığı dosyaları değiştirme veya dosya yollarını manipüle etme yoluyla gerçekleştirilir. Örneğin, bir yazılımın ihtiyaç duyduğu DLL dosyasının yerine zararlı bir DLL dosyası yerleştirilir. Ayrıca, sistem ayarları veya yapılandırma dosyaları değiştirilerek saldırganın çalıştırmak istediği kod devreye sokulabilir.

Zafiyetler: Eksik güvenlik kontrolleri, meşru uygulamaların kullandığı dosyaların doğrulanmaması veya yanlış yapılandırılmış sistemler, saldırıya açık noktalar oluşturur.

Potansiyel Sonuçlar: Saldırganlar, bu teknikle zararlı yazılımlarını çalıştırarak sistem üzerinde kontrol sağlayabilir, hassas verilere erişebilir veya güvenlik önlemlerini atlatabilir. Saldırılar meşru işlemlerin arkasına saklandığı için tespit edilmesi zordur.

Tespit Zorluğu: Zararlı yazılım meşru bir işlem gibi göründüğünden tespit edilmesi oldukça güçtür. Ancak, olağandışı dosya değişikliklerini izleyen güvenlik araçları veya sistem dosyalarını doğrulayan denetim mekanizmaları ile tespit edilebilir.

Gerçek Dünya Örnekleri: MuddyWater grubu, zararlı yazılımlarını çalıştırmak için meşru programları kullanarak kendi kötü amaçlı DLL dosyalarını yüklemiştir.

Alt Teknikler: T1574.001, T1574.002, T1574.004, T1574.005, T1574.006, T1574.007, T1574.008, T1574.009, T1574.010, T1574.011, T1574.012, T1574.013, T1574.014

T1567 (Web Hizmetlerini Kullanarak Veri Sızdırma)

Amacı: Saldırganlar, verileri hedef sistemden dışarıya aktarmak için meşru ve yaygın kullanılan web hizmetlerini kullanmayı amaçlar. Bu yöntemle, hedef sistemdeki güvenlik kontrollerini aşmak ve fark edilmeden veri sızdırmak hedeflenir. Web hizmetlerinin doğal güvenlik özellikleri ve hedef ağlarda meşru olarak kabul edilen kullanımı, saldırganlara önemli bir avantaj sağlar.

Uygulanışı: Saldırganlar, hedef sistemden elde ettikleri verileri dışa aktarmak için Google Drive, Dropbox veya OneDrive gibi popüler bulut hizmetlerini kullanabilir. Ayrıca, verilerin aktarımı sırasında SSL/TLS şifrelemesi gibi yöntemler kullanılarak iletişim korunabilir ve tespit edilmesi zorlaştırılabilir. Bu tür hizmetler, genellikle güvenlik duvarları tarafından engellenmediği için veri çıkışı kolaylıkla sağlanır.

Zafiyetler: Şirket ağlarının meşru web hizmetlerini filtrelememesi veya anormal veri aktarımlarını izlememesi bu tür saldırılara zemin hazırlar. Aynı zamanda, yanlış yapılandırılmış erişim izinleri ve zayıf veri çıkışı kontrol politikaları bu tekniğin kullanılabilirliğini artırır.

Potansiyel Sonuçlar: Saldırganlar, hedef sistemden çaldıkları hassas bilgileri, meşru bir web hizmeti üzerinden dışa aktararak kurumun ticari sırlarını, müşteri bilgilerini ya da finansal verilerini ele geçirebilir. Bu durum, veri ihlali nedeniyle finansal kayıplara ve itibar zedelenmesine yol açabilir.

Tespit Zorluğu: Web hizmetlerini kullanan trafik, genellikle ağdaki meşru işlemlerle benzer göründüğünden, fark edilmesi oldukça zordur. Ancak, belirli hizmetlere yönelik olağandışı bağlantı yoğunluğu veya beklenmedik veri transferi hacimleri gibi anormallikler, bu tür saldırıları tespit etmek için kullanılabilir.

Gerçek Dünya Örnekleri: Fancy Bear (APT28), veri sızdırma işlemini Google Drive aracılığıyla gerçekleştirmiştir.

Alt Teknikler: T1567.001, T1567.002, T1567.003, T1567.004

T1213 (Bilgi Depolarını Kullanarak Veri Toplama)

Amacı: Saldırganlar, bilgi depolarındaki değerli verileri hedef alarak saldırılarını daha etkili hale getirmeyi amaçlar. Bu depolar; politika belgeleri, ağ diyagramları, teknik dokümantasyon, kimlik bilgileri, müşteri bilgileri veya kaynak kod parçacıkları gibi kritik bilgiler içerebilir. Bu bilgiler, saldırganların kimlik bilgilerini ele geçirme, yanal hareketlilik sağlama veya savunmalardan kaçınma gibi çeşitli hedeflere ulaşmasına olanak tanır.

Uygulanışı: Saldırganlar, genellikle SharePoint, Confluence gibi iş birliği platformları veya AWS RDS, ElasticSearch gibi bulut tabanlı veri hizmetlerini kullanarak bilgi toplar. Bunun yanı sıra, iş süreçleri sırasında kullanılan mesajlaşma platformları ya da CRM veri tabanları da değerli bilgiler içerebilir. Bilgi depoları bazen yanlış yapılandırılmış olabilir ve bu da saldırganların hassas bilgilere erişmesini kolaylaştırır.

Zafiyetler: Erişim izinlerinin geniş olması, güvenlik politikalarının yetersizliği veya bulut tabanlı hizmetlerin yanlış yapılandırılması bu tür saldırılara olanak tanır. Ayrıca, şifrelenmemiş veriler ve yetersiz izleme mekanizmaları, saldırganların bilgiye erişim ve dışa aktarım süreçlerini kolaylaştırır.

Potansiyel Sonuçlar: Saldırganlar, bilgi depolarını kullanarak hedef sistemin güvenlik açıklarını tespit edebilir, hassas bilgileri çalabilir ve bu bilgileri daha büyük saldırılar için kullanabilir.

Tespit Zorluğu: Bu tür saldırıları tespit etmek zor olabilir, çünkü bilgi depolarının meşru bir şekilde kullanılması beklenir. Ancak, olağandışı erişim aktiviteleri, yüksek hacimli veri indirme veya beklenmedik dışa aktarımlar, bu tür faaliyetleri tespit etmek için önemli ipuçları sağlayabilir.

Gerçek Dünya Örnekleri: APT41, kurbanların Oracle veri tabanlarından bilgi toplamak için SQLULDR2 aracını kullanmıştır.

Alt Teknikler: T1213.001, T1213.002, T1213.003, T1213.004, T1213.005

APT Saldırılarından Korunma

APT saldırıları, hedef odaklı, uzun süreli ve son derece karmaşık yapılarıyla dikkat çeker. Bu saldırılar, bireylerden büyük kurumlara kadar herkesi hedef alabilir ve genellikle bilgi çalma, sistemleri bozma veya uzun vadeli gözetleme amacı taşır. Ancak, doğru önlemler alındığında bu tür saldırılardan korunmak mümkündür.

Güçlü Erişim Politikaları: Saldırganlar, genellikle zayıf parolalar ve açık hesaplar üzerinden sisteme sızar. Bu tarz saldırılardan korunmak için şunları yapabilirsiniz:

1. **Çok faktörlü kimlik doğrulama (MFA):** Sadece parola değil, ek doğrulama yöntemleri kullanın (örneğin, telefonunuza gelen kodlar).
2. **Güçlü ve benzersiz şifreler:** "123456" veya "admin" vb. şifrelerden kaçının. Harf, sayı ve sembol içeren kompleks şifreler oluşturun. Örneğin, sh6$hd34&3sHk!3gDh@ gibi.
3. **Kullanıcı yetkilerini kontrol edin:** Tüm kullanıcılar sadece iş için gereken izinlere sahip olmalıdır. Gereksiz yönetici (admin) yetkisi vermeyin.

Güncel Yazılım ve Sistemler: Eski ve güncellenmemiş sistemler güncel güvenlik açıklarına karşı savunmasız olduğundan bunları güncellemek kritik bir öneme sahiptir.

1. **Otomatik güncellemeleri etkinleştirin:** İşletim sisteminizi, yazılımlarınızı ve güvenlik çözümlerinizi düzenli olarak güncel tutun. Ama bir sorun olmaması adına her güncellemeden önce yedeklemenizi yapın.
2. **Güvenlik yamalarını yükleyin:** Özellikle büyük güvenlik açıklarını kapatan yamaları gecikmeden uygulayın.

Eğitim ve Farkındalık: Bir sistemin en zayıf halkası çoğu zaman kullanıcılardır. Bu yüzden gerçekleşen saldırıların çoğu sosyal mühendislik saldırılarıdır. Bu sosyal mühendislik saldırılarına karşı eğitim ve farkındalık önemli unsurdur:

1. **E-posta güvenliği:** Tanımadığınız veya şüpheli bir kaynaktan gelen bağlantılara tıklamayın ve ekleri açmayın. Şüphelendiğiniz durumlarda siber güvenlik birimine haber verin.
2. **Phishing (Oltalama) farkındalığı:** Bu yöntem bir e-posta aracılığıyla, telefon sms'i veya bir telefon araması yöntemiyle gerçekleşebilir ve bu çağrılar genellikle acil durum veya ödül vaat eden mesajlar içerir. Dikkatlice inceleyip ona göre hareket edin.
3. **Çalışanlar için eğitim:** Kurumsal bir yapıdaysanız, tüm çalışan personeli siber tehditler hakkında bilgilendirin. Bu eğitimler çalışanların daha dikkatli olmasını sağlayacağından siber tehditlere karşı sizi daha savunmalı yapacaktır.

Ağ Güvenliği: APT saldırganları, ağ üzerinden hareket ederek sistemlere sızabilir. Bu tarz saldırılara karşı ağınızı korumak için bu adımları uygulayabilirsiniz:

1. **Ağ segmentasyonu:** Kritik sistemleri ayrı bir ağda tutarak saldırganların hareket kabiliyetini kısıtlayabilirsiniz.
2. **Firewall ve IDS/IPS:** Güvenlik duvarları ve saldırı tespit/önleme sistemleri kurabilirsiniz.
3. **Şifreleme:** Veri trafiğini şifreleyerek iletişimleri koruma altına alabilirsiniz.

Güvenlik Araçları ve Çözümleri: APT saldırılarını tespit etmek için bazı gelişmiş araçlara ihtiyaç duyabilirsiniz:

1. **Antivirüs ve EDR çözümleri:** Gelişmiş zararlı yazılımları algılamak ve temizlemek için kullanılır.
2. **SIEM araçları:** Sistem aktivitelerini analiz ederek anormal davranışları tespit eder.
3. **Yedekleme çözümleri:** Kritik verilerinizi düzenli olarak yedekleyin ve bu yedekleri çevrimdışı olarak saklayın.

Zafiyet Yönetimi ve Tarama: APT gruplarının saldırılarından korunmak için sisteminizi düzenli olarak zayıflıklara karşı taramanız önerilir:

1. **Zafiyet tarama araçları:** Sisteminizdeki güvenlik açıklarını bulmak için kullanabilirsiniz.
2. **Penetrasyon testleri:** Sistemlerinizi saldırganların gözünden test ederek eksiklikleri ortaya çıkarabilirsiniz.

APT saldırılarından korunmak için alınan önlemler hayati olsa da bu tür tehditlerin tamamen engellenmesi her zaman mümkün olmayabilir. Bu nedenle, saldırıların erken tespiti ve müdahale sürecinin etkin yönetimi, güvenlik stratejisinin ayrılmaz bir parçası olmalıdır. Saldırıların fark edilmesi zor ve uzun süreli saldırılar olduğundan, erken tespit kritik öneme sahiptir. Erken tespit etmek için:

- **Anormal davranışları izleyin:** Örneğin, kullanıcıların alışılmadık saatlerde giriş yapması.
- **Veri trafiğini izleyin:** Hangi verilerin, nereye ve ne sıklıkta gönderildiğini kontrol edin.
- **Logları analiz edin:** Tüm sistem aktivitelerini kaydedin ve düzenli olarak inceleyin.

APT saldırılarının erken tespiti, saldırıyı durdurmak ve hasarı en aza indirmek için kritik bir adımdır. Ancak, bazı durumlarda saldırılar tespit edildiğinde çoktan sistemlere sızılmış olabilir. Bu tür durumlarda hızlı ve etkili bir müdahale, zararı sınırlamak ve saldırganların erişimini engellemek için gereklidir. Peki, bir APT saldırısına maruz kalınırsa hangi adımlar atılmalıdır?

- **Saldırıyı izole edin:** Etkilenen sistemleri acilen ağdan çıkarın.
- **Uzman desteği alın:** Siber güvenlik uzmanlarından veya olay müdahale ekiplerinden hemen yardım isteyin.
- **Kanıtları toplayın:** Olayı analiz etmek ve ileride benzer saldırıları önlemek için tüm detayları en ufak ayrıntısına kadar kaydedin.
- **Kurtarma planınızı devreye alın:** Yedeklerden sistemleri geri yükleyin ve açıkları kapatın.

APT saldırılarından korunmak, sadece teknik araçlarla değil, aynı zamanda bilinçli bir yaklaşımla mümkündür. Düzenli güncellemeler, kullanıcı eğitimi, güçlü güvenlik önlemleri ve proaktif izleme ile sistemlerinizi bu tür tehditlere karşı koruma altına alabilirsiniz. Unutmayın, güçlü bir güvenlik kültürü oluşturmak, saldırganların en büyük düşmanıdır.

Sonuç ve Değerlendirme

Bu çalışma, Gelişmiş Sürekli Tehditler (APT) gibi karmaşık ve uzun vadeli siber tehditlere karşı farkındalığın artırılması ve etkin önlemler alınmasının gerekliliğini vurgulamaktadır. APT grupları, hedeflerine ulaşmak için çeşitli taktikler, teknikler ve prosedürler kullanarak sistemleri uzun süre gözetleyip, kritik verilere ulaşmayı hedefler. Bu nedenle, APT saldırıları yalnızca teknik bir sorun değil, aynı zamanda stratejik bir tehdit olarak değerlendirilmelidir.

APT saldırılarından korunmak için güçlü erişim kontrol mekanizmaları, güncel yazılım ve donanım altyapıları, ağ segmentasyonu ve düzenli güvenlik taramaları gibi yöntemlerin yanı sıra, çalışanların sosyal mühendislik saldırılarına karşı eğitilmesi önem taşımaktadır. Ancak, alınan tüm önlemlere rağmen bu tür saldırıların tamamen engellenmesi her zaman mümkün olmayabilir. Bu nedenle, erken tespit ve hızlı müdahale süreçlerinin etkili bir şekilde yönetilmesi, güvenlik stratejilerinin merkezinde yer almalıdır.

Türkiye özelinde, APT gruplarının saldırılarında jeopolitik ve ekonomik çıkarların etkili olduğu görülmektedir. Bu durum, ülkemizin kritik altyapılarını ve kurumlarını koruma konusunda daha proaktif ve kapsamlı bir yaklaşım benimsemesi gerektiğini göstermektedir. Özellikle, IoC'lerin doğru bir şekilde analiz edilmesi ve TTP'lerin düzenli olarak izlenmesi, bu tehditlere karşı mücadelede önemli bir rol oynamaktadır.

Sonuç olarak, APT saldırılarıyla mücadele, hem teknik çözümleri hem de farkındalık odaklı stratejileri içeren bütüncül bir yaklaşım gerektirmektedir. Bu çalışma, bireylerin ve kurumların bu tehditlere karşı daha bilinçli ve hazırlıklı olmasına katkı sağlamayı hedeflemiş ve APT'lere dair temel bilgileri sistematik bir şekilde sunarak siber güvenlik stratejilerinin geliştirilmesine ışık tutmuştur.

Kaynakça

- AlienVault. (n.d.). OTX. https://otx.alienvault.com/pulse/627b7ceef23d9a59956eecb0
- BeyazNet. (2024). 30. Hafta Siber Güvenlik Haberleri. BeyazNet. https://www.beyaz.net/tr/guvenlik/makaleler/2024_30_hafta_siber_guvenlik_haberleri.html
- Bloomberght. (2018, Şubat 13). Kuzey Kore'den Türkiye'ye siber saldırı. BloombergHT. https://www.bloomberght.com/kuzey-kore-den-turkiye-ye-siber-saldiri-2102112
- Cimpanu, C. (2023, Ocak 10). OilRig hackers now exploit Windows flaw to elevate privileges. Bleeping Computer. https://www.bleepingcomputer.com/news/security/oilrig-hackers-now-exploit-windows-flaw-to-elevate-privileges/
- CrowdStrike. (n.d.). Advanced persistent threat (APT). CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/
- CrowdStrike. (2016). Bears in the midst: Intrusion into the Democratic National Committee. https://www.crowdstrike.com/en-us/blog/bears-midst-intrusion-democratic-national-committee/
- Cybereason. (2024). PowerLess Trojan: Iranian APT Phosphorus adds new PowerShell backdoor for espionage. https://www.cybereason.com/blog/research/powerless-trojan-iranian-apt-phosphorus-adds-new-powershell-backdoor-for-espionage
- Dark Reading. (2024). Toolkit expands APT41's surveillance powers. https://www.darkreading.com/cyberattacks-data-breaches/toolkit-expands-apt41s-surveillance-powers
- Infinitum IT. (n.d.). MuddyWater APT Grubu. https://www.infinitumit.com.tr/muddywater-apt-grubu/
- Infinitum IT. (n.d.). Charming Kitten (APT35). https://www.infinitumit.com.tr/charming-kitten-apt35/
- Infinitum IT. (n.d.). İran destekli APT grubu: APT39 (Chafer). https://www.infinitumit.com.tr/iran-destekli-apt-grubu-apt39-chafer/

- Kaspersky. (2024). APT report Q3 2024. Securelist. https://securelist.com/apt-report-q3-2024/114623/
- MITRE. (n.d.). ATT&CK Techniques. MITRE ATT&CK. https://attack.mitre.org/techniques
- MITRE. (n.d.). MITRE ATT&CK Framework. https://attack.mitre.org/
- Palo Alto Networks Unit42. (2024). OilRig malware campaign updates toolset and expands targets. https://unit42.paloaltonetworks.com/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/
- Picus Security. (2024). APT29 (Cozy Bear): Evolution & techniques. https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques
- PolySwarm. (2024). MuddyWater uses SloughRAT in recent campaigns. https://blog.polyswarm.io/muddy-water-uses-sloughrat-in-recent-campaigns
- SentinelOne. (n.d.). Mimikatz: A deep dive into credential dumping tool. SentinelOne. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/mimikatz/
- SOCRadar. (2022). APT Profile: Who is Lazarus Group? https://socradar.io/apt-profile-who-is-lazarus-group/
- SOCRadar. (2022). 2021 Turkey Threat Landscape Report. https://socradar.io/wp-content/uploads/2022/02/2021-Turkey-Threat-Landscape-Report-TR-2.pdf
- SOCRadar. (2023). Türkiye Threat Intelligence Report. https://socradar.io/wp-content/uploads/2023/05/Turkiye-Threat-Intelligence-Report_.pdf
- Splunk. (n.d.). TTP (Tactics, Techniques, Procedures). https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html
- The Hacker News. (2024). APT41 infiltrates networks in Italy. https://thehackernews.com/2024/07/apt41-infiltrates-networks-in-italy.html
- ThreatMon. (n.d.). Iran-based APTs. ThreatMon. https://threatmon.io/iran-based-apts/
- Trend Micro. (2023). Examining the activities of the Turla Group. https://www.trendmicro.com/tr_tr/research/23/i/examining-the-activities-of-the-turla-group.html

- TRT Haber. (2018, Ocak 22). Zeytin Dalı Harekâtı'nın başlamasıyla Türkiye'yi hedef alan siber saldırılar arttı. TRT Haber. https://www.trthaber.com/haber/bilim-teknoloji/zeytin-dali-harekatinin-baslamasiyla-turkiyeyi-hedef-alan-siber-saldirilar-artti-360570.html
- Wikipedia contributors. (n.d.). Advanced persistent threat. Wikipedia. https://en.wikipedia.org/wiki/Advanced_persistent_threat
- Wikipedia contributors. (n.d.). Cozy Bear. Wikipedia. https://en.wikipedia.org/wiki/Cozy_Bear
- Wikipedia contributors. (n.d.). Fancy Bear. Wikipedia. https://en.wikipedia.org/wiki/Fancy_Bear
- Wikipedia contributors. (n.d.). Lazarus Group. Wikipedia. https://en.wikipedia.org/wiki/Lazarus_Group
- Wikipedia contributors. (n.d.). WannaCry ransomware attack. Wikipedia. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
- Wikipedia contributors. (n.d.). X-Agent. Wikipedia. https://en.wikipedia.org/wiki/X-Agent