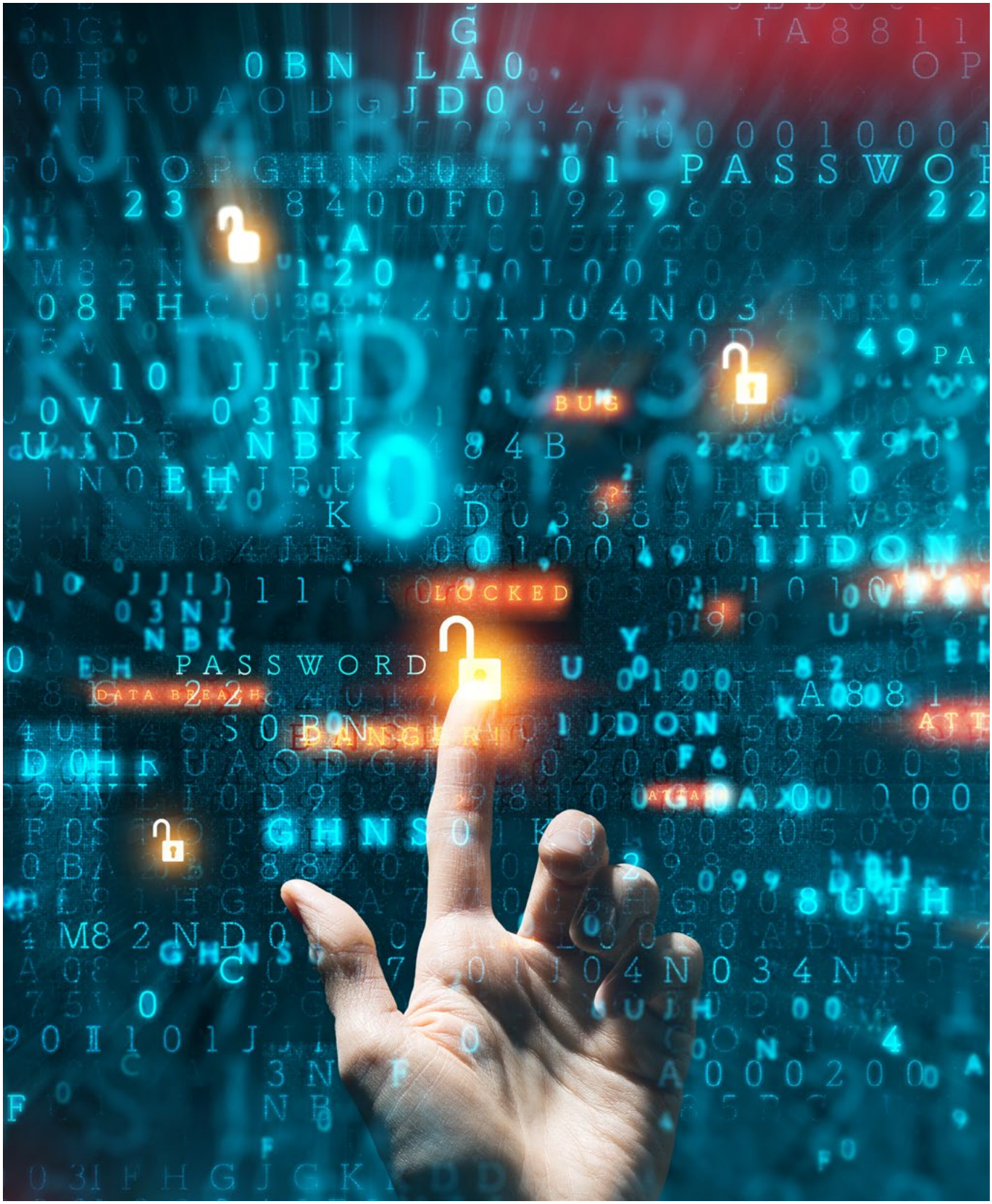
STM Cyber

SİBER TEHDİT DURUM RAPORU

EKİM-ARALIK 2022

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi



İÇİNDEKİLER

Sorumsuzluk ve Fikri Mülkiyet Hakkı Beyanı 2
İÇİNDEKİLER 3
ŞEKİLLER 5
GİRİŞ 5
TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK 5
1. Fidye Yazılım Hizmetlerinin Sınıflandırılması 5
1.1. Özet 5
1.2. Giriş 5
1.3. Arka Plan Bilgisi 5
1.4. Taksonominin Oluşturulması 6
1.5. Tartışma ve Öneriler 7
1.6. Sonuç 7
2. Deniz Platformlarında Siber Güvenlik 7
2.1. Denizcilik Siber Risk Yönetimi Regülasyonu 7
2.2. Deniz Platformlarında Siber Saldırılar 8
2.3. Gemilerde Siber Saldırılara Hassas Sistemler 10
3. AXLocker Fidye Yazılımı ile Hesaplarınız Çalınabilir! 11
3.1. Fidye Yazılımı (Ransomware) Nedir? 11
3.2. Fidye Yazılımları Nasıl Tespit Edilebilir? 12
3.3. Fidye Yazılım Çeşitleri Nelerdir? 12
3.4. Fidye Yazılımından Nasıl Korunulmalıdır? 12
4. Matrix Mesajlaşma Protokolü Zafiyetleri 12
4.1. Zafiyet 1: Eksik Adaptasyondan Gizlilik İhlali 12
4.2. Zafiyet 2: Bant Dışı Doğrulama İhlali 13
4.3. Zafiyet 3: Yarı-güvenilen Kişilik Taklidi 13
4.4. Zafiyet 4: Güvenilen Kişilik Taklidi 13
4.5. Zafiyet 5: Yarı-güvenilen Kişilik Taklidinden Doğan Gizlilik İhlali 13
4.6. Zafiyet 6: IND-CCA İhlali 13
5. Veri Silme Yazılımlarının Önemi 13
5.1. Verilerin Silinmesinin Gerekliliği 13
5.2. Veri Silme Yazılımları 14

6. Silah Sistemleri Siber Güvenliği 14
7. ProxyNotShell: CVE-2022-41040 ve CVE-2022-41082 Zafiyetleri 16
7.1. ProxyNotShell Nedir? 16
7.2. ProxyNotShell'in Teknik Detayları 16
8. Mor Takım Nedir 17
8.1. Mavi Takım 17
8.2. Kırmızı Takım 17
8.3. Kırmızı Takım ve Sızma Testi Arasında Bulunan Farklar 17
8.4. Tehdit Aktörleri ve Gelişmiş Sürekli Tehditler (APTs) 17
8.5. Siber Ölüm Zinciri 18
8.6. MITRE ATT&CK Matrisi 19
8.7. Teknikler, Taktikler, Prosedürler 20
8.8. Acı Piramidi 20
8.9. Kırmızı Takım Çalışmalarını Simüle Eden Uygulamalar 20

DÖNEM KONUSU 20
9. CB DDO BİG Rehberi Uyumluluk Denetimi 20
9.1. Bilgi ve İletişim Güvenliği Rehberi 20
9.2. Bilgi ve İletişim Güveliği Denetim Rehberi 21
9.3. Denetim Çalışmalarına Hazırlık 21
9.4. Bilgi ve İletişim Güvenliği Denetim Metodolojisi 21

HONEYPOT VERİLERİ 22

KAYNAKÇA 25

ŞEKİLLER

Şekil 1: RaaS İş Bölümü Taksonomisi[6] 6
Şekil 2: Deniz Platformları Siber güvenlik[9] 7
Şekil 3: Siber Saldırılar[10] 8
Şekil 4: Gemi Teknoloji Ağları ve Saldırılara Hassas Sistemler[15] 10
Şekil 5: Ransomware[17] 11
Şekil 6: Axlocker Ransomware Örneği[19] 12
Şekil 7: Dijital Veriler de Silinmelidir[25] 13
Şekil 8: Format Atılması ve Veri Silme Yazılımlarının Uygulanması Arasındaki Fark[26] 14
Şekil 9: Savaş Uçağında Konumlandırılmış Gömülü Yazılımlar ve BT Sistemleri[27] 15
Şekil 10: Kimliği Doğrulanmış Olarak Gönderilen HTTP İsteği[54] 16
Şekil 11: Kimliği Doğrulanmış Olarak Gönderilen HTTP İsteğine Dönen HTTP Cevabı[54] 16
Şekil 12: Fancy Bear Grubunun Crowd Strike Tarafından Çizimi[56] 18
Şekil 13: Siber Ölüm Zinciri[31] 18
Şekil 14: Mitre Attack Matrisi[32] 19
Şekil 15: Mitre Attack Matrisi Devamı[32] 19
Şekil 16: Teknik, Taktik ve Prosedürler[33] 20
Şekil 17: Acı Piramidi[34] 20
Şekil 18: Bilgi ve İletişim Güvenliği Rehberi[35] 21
Şekil 19: Bilgi ve İletişim Güvenliği Denetim Rehberi[36] 21
Şekil 20: Gelen saldırıların ülkelere göre dağılımı 22
Şekil 21: Parola etiket bulutu 23
Şekil 22: Kullanıcı adı etiket bulutu 24

GİRİŞ

2022 yılının son çeyreğinde Siber Güvenlik Müdürlüğü tarafından hazırlanan raporumuzda her zaman olduğu gibi birçok güncel konuyla karşınızdayız.

Fidye yazılım hizmetleri, son yılların en popüler siber tehditlerinden biridir. Bu nedenle, fidye yazılım hizmetlerinin sınıflandırılması konusu bu raporda önemli bir yer tutuyor.

Deniz platformlarında siber güvenlik konusu da bu dönemde önem kazanmıştır. Bu platformlara düzenlenen siber saldırıların önlenmesi ve mevcut siber güvenlik önlemlerinin geliştirilmesi konusunda önemli bilgiler sunuluyor.

AXLocker fidye yazılımı, son dönemde siber saldırılardaki en yaygın yöntemlerinden biri oldu. Kullanıcıların hesaplarını çalma amacını taşıyan AXLocker fidye yazılımı konusuna açıklık getiriyoruz.

Raporumuzun diğer bir konusu olan Matrix mesajlaşma protokolü popüler bir mesajlaşma protokolüdür. Raporda bu protokolün son dönemde ortaya çıkan zafiyetlerinin nasıl önlenebileceği ele alınıyor.

Bilgisayarlarımızdaki önemli verilerin güvenli bir şekilde silinmesine yardımcı olan veri silme yazılımlarının önemi raporumuzun bir başka konusunu oluşturuyor.

Günümüzde, yüksek hassasiyet gerektiren ortamlarda kullanılan silah sistemlerinin siber güvenlik önlemleri son derece önem kazanmış bulunuyor. Raporumuzun bir başlığını da bu önlemler oluşturuyor.

DDO BİG Rehberi çerçevesinde, kamu kurumlarında ve kritik altyapı hizmetleri sağlayan özel sektör şirketlerinde uygulanacak bilgi ve iletişim güvenliği kurallarını yayınlamıştır. Dönem konusu olarak rehber özelindeki detayları incelemeyi seçtik.

Keyifli okumalar diler ve yeni yıl için sağlık, mutluluk ve başarı dolu güzel dileklerimizi sunarız.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

1. Fidye Yazılım Hizmetlerinin Sınıflandırılması

1.1. Özet

Fidye yazılımları, elde edilecek parasal getiri karşılığında alınan riskin nispeten düşük olması nedeniyle popüler bir siber suç haline geldi. Birçok kuruluş ve hükümet, verilerini daha iyi korumak için gerekli yatırımı yapmak yerine, ele geçirilen verilerini geri almak için ödeme yapmayı tercih ediyor. Bu da suçluları daha fazla motive ediyor. Sonuç olarak, yeni bir tür suç ortaya çıktı: Fidye Yazılım Hizmeti (ing. Ransomware as a Service, RaaS). Bu yeni fenomeni burada tasarım bilim araştırmaları (İng. Design Science Research -DSR) perspektifinden inceliyoruz ve bir RaaS iş bölümü sınıflandırması tanıtıyoruz. Amacımız, fidye yazılımlarının ticarileştirilmesi sürecinde yer alan farklı aktörlerin rollerini belirleyip sınıflandırmak, böylece onların bir RaaS planına dahil olma düzeylerini daha iyi ayırt edebilmek ve onlara karşı daha iyi korunma önlemleri alabilmektir.

1.2. Giriş

Siber suçlar son birkaç yılda yükselişte ve 2025 yılına kadar dünyaya yılda 10,5 trilyon dolara mal olacağı tahmin ediliyor[1]. En kazançlı siber suçlardan biri olan fidye yazılım saldırıları 2019 ile 2020 saldırıları dünya çapında yüzde 62 artmıştır. Daha da endişe verici bir olan, fidye yazılımının artık metalaşarak Fidye Yazılım Hizmeti (RaaS) olarak karaborsada sunulur hâle gelmiş olmasıdır. RaaS fidye yazılıma erişimi kolaylaştırır, sıfırdan oluşturmak için zaman ve kaynak ayırmaya gerek kalmaz. Hazır olarak sunulan bu hizmeti satın almak, sıfırdan oluşturmaya nispeten çok daha kârlıdır[2]. RaaS ile mücadelede ilk adım, sürece dahil olan çeşitli aktörlerin daha iyi anlaşılmasını sağlamak ve aralarındaki ilişkilerinin karmaşık doğasını tasvir etmek olmalıdır. Bu çalışmaya rehberlik eden araştırma sorusu şudur: "Çeşitli fidye yazılımı hizmeti uzmanlıklarını nasıl sınıflandırabiliriz?" Bu soruyu yanıtlamak için RaaS aktörlerinin farklı rollerini belirlemek gerekiyor. Sınıflandırmada tasarım bilim araştırmalarının metodolojisini kullanıyoruz[3].

1.3. Arka Plan Bilgisi

Fidye yazılımı (İng. Ransomware), şantaj yazılımı veya fidye virüsü anlamına gelir. Fidye virüsleri bulaştıkları bilişim sistemleri üzerinde dosyalara erişimi engelleyerek kullanıcılardan fidye talep eden zararlı yazılımlardır. Fidye yazılımı, dosyaları ele geçirmek ve verilere erişilemez hâle getirmek için güvenlik açıklarından yararlanan bir kötü amaçlı yazılım kategorisidir. Bu tür saldırıların failleri, kullanıcıların bu kaynaklara yeniden erişebilmek için fidye ödemesini talep eder. Programlama becerisi olmayan kişilerin aktif saldırganlar hâline gelmesini ve fidye yazılımı ekonomisine dahil olmasını sağlayan RaaS bu kazançlı alanı daha da genişletti. Darknet pazar yerleri RaaS'ın hızlı büyümesine temel oluyor. Ayrıca blok zinciri teknolojisindeki yeni gelişmeler de suçluların fidye yazılımı oluşturmasını ve paylaşmasını kolaylaştırıyor. Bu gelişmeler yüksek kârlı büyük kuruluşların maruz kalma riskini etkilemezken daha küçük ölçekteki kuruluşları mağdur etmektedir.

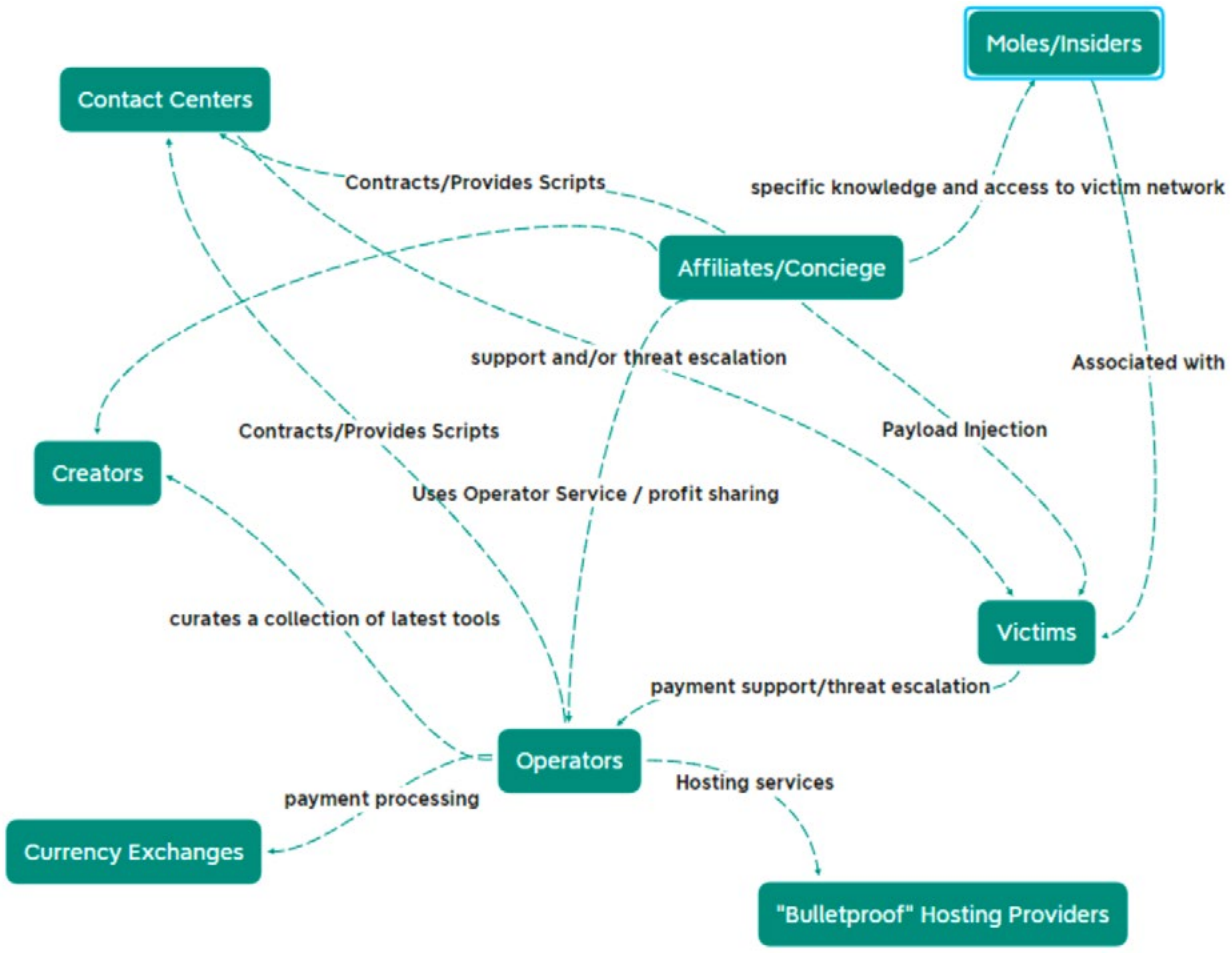
RaaS'ı açıklamak için organizasyon teorisini kullanacağız. Normalde suç dünyasındaki mafyaları, çeteleri veya tefecileri temsil etmek için kullanılan bir yöntem olmasına rağmen bu teori, hâlihazırda organize siber haraççılığı açıklamak için de kullanılıyor[4], [5]. Ama katma değer, haberleşme ve pazarlama yaklaşımları gibi benzer konuları ele aldığı için RaaS için de kullanılabilir.

1.4. Taksonominin Oluşturulması

RaaS taksonomisi, dağıtık bir ağ olarak tasarlandı. Ortaya çıkan RaaS uzmanlıklarının ne olduğunu anlamak, kuruluşlara ve hükümetlere karşı yeni ve daha yoğun siber tehdit üreten yeni kurumsal dinamikleri anlamaya yönelik yeni araştırmaları motive edecektir.

Literatür incelememize, ilgili vaka incelemelerine ve halka açık bilgilere dayanarak, RaaS İşbölümü Taksonomisi oluşturuldu. İlk olarak, belirlenen tüm kaynaklar, belirli rollerden veya uzmanlıklardan bahsetmek için kodlandı. İkincisi, çeşitli ilk kod dizileri, uzmanlık kategorileri hâlinde kümelendi. Ön sonuçlarımız, tipik bir fidye yazılımı saldırısında tek bir fail veya grup yer alırken, bir RaaS şemasında rolün yedi uzmanlığa bölündüğünü gösteriyor.

- **Kurucular (İng. Creators):** RaaS içinde kullanılan çeşitli yazılım araçlarının ve teknolojilerinin yazarlarıdır. Bunlara, açıktan yararlanma yazılımı yaratıcıları ve bu tür suçları istemeden destekleyen yazılım yaratıcıları dahildir. Bu ikinci kategorinin bir örneği, veri klonlama araçları, pen-test araçları, şifreleme araçları ve blok zinciri arayüz yazılımı gibi yazılımların yaratıcılarını içerir.
- **Operatörler (İng. Operators):** Çeşitli araçları bir araya getiren ve üye oldukları ve bağlı kuruluşlarla etkileşime girdikleri arayüzler oluşturan entegratörler olarak hareket ederler. Şifreli e-posta ve mesaj panoları bu tür arayüzlerin basit biçimlerini oluştururken, bağlı kuruluşların bir saldırıyı doğrudan koordine edebildiği web portalları daha gelişmiş biçimlerdir.
- **Bağlı Kuruluşlar (İng. Affiliates):** Hedef kurbanı belirleyen ve saldırı başlatan bağlı kuruluşlar, bir operatör tarafından sağlanan arabirimi kullanır ve kurbanın belirli ayrıntılarından/bilgilerinden yararlanır. Elde ettikleri özel bilgiler, başarılı bir saldırı şansını artırır.
- **Köstebekler (İng. Moles):** Belirli bilgileri kurban sisteme doğrudan erişimi birleştirmek fidye yazılımı saldırısının başarı şansını artırır. Köstebekler, bir bağlı şirketle işbirliği yapabilir veya doğrudan bir operatörle



Şekil 1: RaaS İşbölümü Taksonomisi[6].

arayüz kurabilir. Köstebekler, saldırılara yardımcı olmak için ayrıntılı bilgiler sağlar ve genellikle doğrudan kurbanların ağlarına bir istismar ekler. Bunlar çoğu zaman, işverenlerine kin besleyen hoşnutsuz çalışanlar olabilirler.

- **İletişim Merkezleri (İng. Contact Centers):** Sözleşme merkezleri iki ana fonksiyona hizmet eder. İlk olarak, fidye yazılımı kurbanlarına fidyeyi ödemelerine yardımcı olmak için destek sağlarlar. İkinci olarak, kurbanın şifrelenmiş verilere yeniden erişim sağlamak için fidye ödemeye istekli olmadığını varsayalım (örneğin, kurtarmaları gereken verilerin yedekleri veya başka kopyaları var). Bu tür durumlarda iletişim merkezleri kurbanla iletişim kurar ve mağdurun verilerinin bir kısmını halka ifşa etmekle tehdit eder.
- **"Kurşun Geçirmez" Barınma Sağlayıcıları (İng. Bulletproof Hosting Providers):** Saldırıları belirleyen ve başlatanlar ile RaaS hizmetini çalıştıranlar arasında ayrım yapıldığında, web tabanlı arayüzler kullanan bir koordinasyon aracı gereklidir. Bu işlevi "kurşun geçirmez" olarak bilinen barınma sağlayıcılar yerine getirir[5].
- **Döviz Büroları (İng. Currency Exchanges):** RaaS kurbanları fidyeyi çeşitli kripto para birimleri kullanarak öder. RaaS failleri kripto para birimlerini kullanabilseler de bu gelirleri yerel bir para birimine çevirmeyi de tercih edebilirler.

1.5. Tartışma ve Öneriler

Siber suç örgütlerinin saldırılarının artan karmaşıklığı, işlevsel uzmanlaşma ve farklı işbölümlerine ayrılmasında da görülmektedir[7]. Artan karmaşıklık ve organizasyonlaşma, RaaS gruplarının daha büyük ve daha karmaşık saldırılar düzenleme olanağını artırır[8]. Bu tür işbölümlerine ve uzmanlaşmanın durumunu ortaya koymak, araştırmacıların ve kolluk kuvvetlerinin uzmanlaşmış roller tarafından sergilenen belirli davranışlara odaklanmasına yardımcı olacaktır. Buradaki amacımız, RaaS hakkındaki bilgileri sınıflandırmak olduğu için, işbölümünü tipik bir RaaS yapısında açıklamak ve bu nispeten yeni alana bilgi eklemek için bir taksonomi geliştirdik. Önceki fidye yazılımları ile yeni ortaya çıkan RaaS arasındaki temel ayrım, fidye yazılımını kullanmak isteyen saldırganın bunu sıfırdan inşa etme zorunluluğunun ortadan kalkmış ve bunun bir siber suç örgütü haline getirilmiş olmasıdır. Bu yazıda sunulan sınıflandırma, araştırmacılara aktörlerin kullandığı belirli davranışlara, motivasyonlara, beceri edinme sürecine odaklanmada yardımcı olabilir.

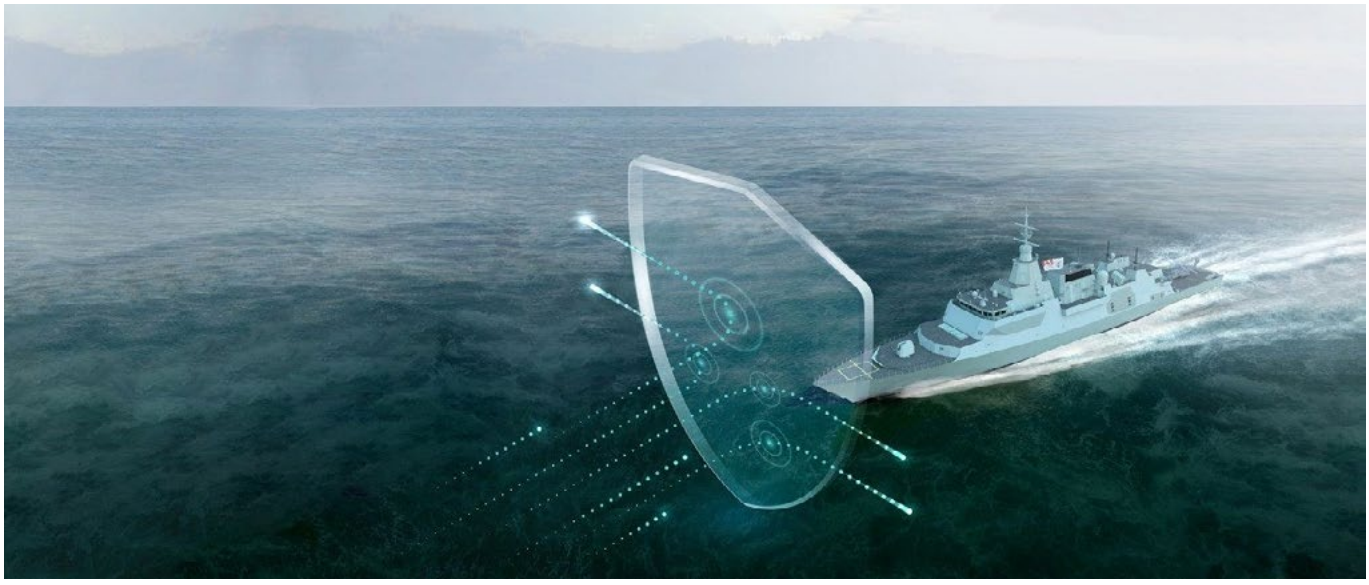
1.6. Sonuç

Artan uzmanlaşma sayesinde RaaS, çok özel ve uzman katılımcılardan oluşan bir grup aracılığıyla sunuluyor. Taksonomimiz, katılımcıların sahip olduğu ana işlevleri tarif ediyor. Ancak aktörler genellikle birden fazla rol üstlenir. Bununla birlikte, örgütsel yapılar olgunlaştıkça, bu tür işbölümlerinin daha yaygın olmasını bekleyebiliriz. Taksonomimiz, herhangi soyut bir RaaS örgütünü ve uzmanlıkları tanıtmaktadır. Bu, karmaşık yeni bir olguyu keşfetmede ilk adımıdır ve sağladığımız bilgiler, çeşitli RaaS aktörlerinin katılım düzeylerini daha iyi ayırt etmek için kolluk kuvvetlerine faydalı olabilir.

2. Deniz Platformlarında Siber Güvenlik

2.1. Denizcilik Siber Risk Yönetimi Regülasyonu

Deniz Emniyeti Komitesi (International Maritime Organization –IMO), Haziran 2017'deki 98'inci oturumunda MSC.428(98) Emniyet Yönetim Sistemlerinde Denizcilik Siber Risk Yönetimine yer verilmesi kararını almıştır.



Şekil 2: Deniz Platformları Siber güvenlik[9].

Karar doğrultusunda, 1 Ocak 2021'den sonra Uygunluk Belgesinin ilk yıllık doğrulamasından geç olmamak üzere, mevcut emniyet yönetim sistemlerinde siber risklerin uygun şekilde ele alınması gerekmektedir. IMO bu kapsamda "Deniz Platformlarında Siber Güvenlik Kılavuzu"nu (MSC-FAL.1/Circ.3, Temmuz 2017) hazırlamıştır.

IMO kılavuzu, bir dizi kuruluş tarafından daha da geliştirilmiş ve desteklenmiştir. Bu kapsamda aşağıda belirtilen yönerge ve rehber niteliğinde çalışmalar yapılmıştır.

Avrupa Birliği Siber Güvenlik Ajansı (ENISA) tarafından Liman Siber Güvenliğine yönelik, Denizcilik sektöründe siber güvenlik için iyi uygulamalar (Kasım 2019) ve Limanlar için Siber Risk Yönetimi (Aralık 2020) kılavuzları yayınlanmıştır.

Denizcilik örgütleri ve sektör girişimcilerinden (IUMI, BIMCO, ICS, Intertanko, Intercargo, Cruise Lines International Association ve The Oil Companies) oluşan Uluslararası Denizcilik Forumu (International Marine Forum) ortak bir çalışma sonucunda "Gemilerde Siber Güvenlik Kılavuzu v4" dokümanını hazırlamıştır (Aralık2020).

IACS (International Association of Classification Societies) IMO'nun "Deniz Platformlarında Siber Güvenlik Kılavuzu"nu referans alarak "No. 166 (2020) Recommendation on Cyber Resilience" tavsiyesini hazırlamıştır. IACS daha sonra deniz platformlarının siber dayanıklılığına ilişkin Nisan 2022 tarihinde yürürlüğe girmiş olan zorunlu gereksinimler dokümanları UR E26 ve UR E27'yi (Unified Requirements -UR) yayınlamıştır. Bu UR'ler, 1 Ocak 2024'te ve sonrasında kurulacak yeni deniz platformlarına uygulanacaktır, ancak burada yer alan bilgiler geçici olarak zorunlu olmayan rehberlik olarak uygulanabilir.

UR E26, deniz platformu tasarımı, inşası, devreye alınması ve operasyon ömrü boyunca hem Operasyonel Teknoloji (OT) hem de Bilgi Teknolojisi (IT) ekipmanlarının deniz platformu ağına güvenli entegrasyonunu sağlamayı amaçlar. Bu UR, siber dayanıklılık için deniz platformunu bir bütün olarak ele alır ve Ekipman Tanımlama, Koruma, Saldırı Tespiti, Müdahale, Kurtarma olmak üzere beş temel unsuru kapsar.

UR E27, sistem bütünlüğünün ekipman tedarikçileri tarafından güvence altına alınmasını ve sağlamlaştırılmasını amaçlar. UR E27, deniz platformundaki sistemlerin ve ekipmanların siber dayanıklılığı için gereksinimleri, kullanıcılar ile platformdaki bilgisayar tabanlı sistemler arasındaki arayüzle ilgili ek gereksinimleri ve yeni cihazların ürün tasarım ve geliştirme aşamalarındaki güvenlik gereksinimlerini tanımlar.

2.2. Deniz Platformlarında Siber Saldırılar

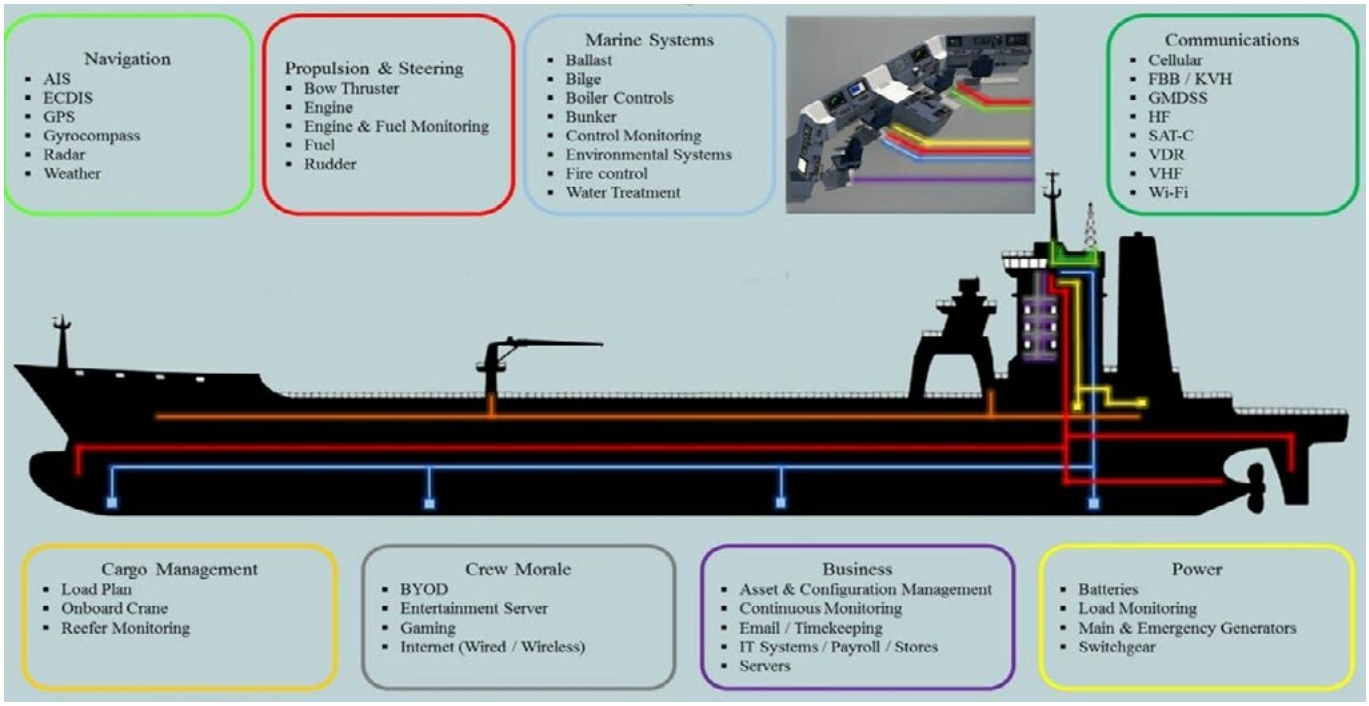
Saldırganlar kötü amaçlı yazılım (Malware) ile platformun bilgi teknolojilerine, operasyonel teknolojilerine ve endüstriyel kontrol sistemlerine erişebilir ve GPS, AIS, ECDIS gibi seyir sistemlerini devre dışı bırakabilir, yanıltarak yönlendirilebilir, elektronik ortamda tutulan verileri çalabilir veya şifreleyerek fidye talep edilebilirler.

Şekil 3: Siber Saldırılar[10].

Bir deniz platformunun yerleşik bilgi teknolojisi ve operasyonel teknoloji sistemlerinin, karadaki sistemler kadar kolay hack'lenebileceği ve bu tür güvenlik ihlallerinin gemilerin, limanların, deniz tesislerinin ve diğer unsurların emniyet ve güvenliğine önemli zararlar verme potansiyeline sahip olduğu, günümüze kadar süregelen siber saldırılar ve etkileri incelendiğinde açıkça anlaşılmaktadır.

Siber Saldırının Yılı	Siber Saldırı	Bilinen Detaylar
2008	Yapılan bir deney ile "MN Pole Star" gemisinin AIS, ECDIS ve GPS sistemleri yanıltıldı.	İngiltere ve İrlanda Denizcilik İdaresi, Savunma Bakanlığı ve Savunma Bilim ve Teknoloji Laboratuvarı işbirliği ile okyanusun belli bir bölgesine yanıltıcı sinyaller gönderdi. Buraya yöneltilen MN Pole Star gemisinin AIS, ECDIS ve GPS gibi kritik köprü üstü seyir cihazları karıştırıldı ve bozuldu. Benzer bir durum kötü hava koşullarında limana yanaşmaya kalkan bir gemide yaşanırsa manevra güvenliğinin tehlikeye düşebileceği ispatlandı.
2010	Endüstriyel kontrol sistemleri hedef alındı.	Güney Kore'den Güney Amerika'ya götürülen bir petrol platformunun sistemleri zararlı yazılım kullanılarak çökertildi. Platformun arızalarının giderilip tekrar operasyona başlaması 19 gün sürdü. Benzer bir durum platformun dinamik pozisyonlama sistemini çökertseydi çok daha kötü sonuçlar ortaya çıkabilirdi.
2011	Hacker'lar IRISL firmasına saldırdı.	Hacker'lar IRISL'e (İran İslam Cumhuriyeti Denizcilik Firması) saldırıp konteyner numaralarını ve varış bilgilerini bozarak sistemi karıştırdılar. Firma yüklerin takibini yapamadı ve kayıplar yaşadı.
2011 - 2013	Belçika'nın Antwerp Limanı bilgisayarlarına sızıldı.	2011 ve 2013 yılları arasında hacker'lar Antwerp Limanı bilgisayarlarına sızarak bazı konteynerlerin yerini tespit ettiler ve evraklarını değiştirdiler. Bu konteynerler sahte isim ve evraklar ile liman dışına çıkarılarak kötü amaçlar için kullanıldı.
2012	Yanıltıcı ve karıştırıcı sinyaller ile 200'den fazla açık deniz gemisinin GPS'leri bozuldu.	Gemilerin GPS (Uydu Konumlama) cihazları bozularak açık deniz seyirleri zorlaştırıldı. Cihazlar uzaktan müdahale ile etkisiz hâle getirildi.
2012	Avustralya Gümrük ve Sınır Koruma İdaresinin bilgisayarlarına sızıldı.	2012 yılında Avustralya Gümrük İdaresinin bilgisayarlarına girildi ve bazı konteynerlerin otoriteler tarafından şüpheli olarak işaretlenip işaretlenmediğini kontrol ettiler. Bu sızma sonucu ilgilendikleri konteynerlerin takip edildiğini anlayıp limandan çekmekten vazgeçtiler.
2013	Yanıltıcı GPS sinyali ile yat rotasından çıkarıldı.	Teksas-Austin Üniversitesi araştırmacıları "White Rose of Drax" isimli yatı, Akdeniz'de sahte GPS sinyalleri ile rotasından çıkarabileceklerini gösteren bir çalışma yaptılar ve gemi zabitanını yanılttılar.
2014	Bir Amerikan limanı GPS karıştırma yüzünden operasyonlarını durdurdu.	Amerika'da bir liman, GPS karıştırıcı sinyaller nedeniyle gemi trafiğini yönetemediği için operasyonlarını durdurma noktasına geldi ve belli bir süre kapandı.
2014	FBI GPS karıştırma konusunda sektörü uyardı.	FBI özel sektörü uyararak GPS karıştırma ile yük hırsızlığının yapıldığını bildirdi. 46 olayda çalıntı arabaların bu yolla Çin'e kaçırıldığı belirtildi.
2017	Maersk firmasının Kopenhag'daki merkezine NotPetya isimli virüs ile saldırıldı.	27 Haziran 2017 öğleden sonra hacker'lar "NotPetya" isimli r virüs ile Maersk firmasının merkez ofisine saldırı düzenledi. Firmanın dünya çapındaki (130 ülkede 574 ofis) 80.000 çalışanın dizüstü bilgisayarları 76 liman ve 800'den fazla açık deniz gemisi ve yük evrakları bu saldırıdan etkilendi. Bu saldırı firmaya 350 milyon dolarlık hasar verdi.
2018	COSCO firmasına yapılan siber saldırı şirket ağının çökmesine neden oldu.	Çin merkezli denizcilik devi COACO'nun network sistemi siber saldırıyla çökertildi. Şirketin operasyonları aksatıldı.
2019	Kuveyt deniz taşımacılık organizasyonlarına ait bilgilerin ifşa edildi.	2019 yılının Eylül ayında XHunter adındaki bir siber saldırı ile Kuveyt deniz taşımacılık organizasyonlarına ait bilgiler ifşa edildi.
2019	San Diego polis merkezi ve limanı işlemez hâle getirildi.	Eylül 2019'da Samsam Ransomware saldırısı ile San Diego polis merkezi ve limanını işlemez hâle getirildi ve Bitcoin talep edildi.
2019	Ryuk Ransomware saldırısı ile denizcilik tesisi işlemez hâle getirildi.	Aralık 2019'da Ryuk Ransomware saldırısı ile ABD Sahil Güvenlik tarafından açıklanan bilgiye göre bir denizcilik tesisi işlemez hâle getirildi.
2020	Fidye yazılımı kullanılarak siber saldırı gerçekleştirildi.	Hürmüz Limanı'na yapılan siber saldırı sonucu limandaki bazı işletim sistemleri zarar gördü.
2020	Mediterranean Shipping Company kötü amaçlı yazılım saldırısına maruz kaldı, şirket saldırıyı kontrol altına almak için sunucularını devre dışına aldı.	Mediterranean Shipping Company (MSC), kötü amaçlı yazılım saldırısının veri merkezi kesintisine neden olduğunu ve bunun da ana müşterilerinin kullandığı web sitelerinin birkaç gün boyunca kapalı kalmasına neden olduğunu doğruladı.
2021	Oltalama ile fidye yazılımı yüklenmesi sağlanmıştır.	Güney Kore'nin ulusal amiral gemisi taşıyıcısı HMM'e e-posta ile oltalama saldırısı gerçekleştirilerek, sisteme sınırlı erişim sağlandı.

Tablo 1: Denizcilikte Yapılan Siber Saldırılar[11], [12] [13], [14].



Şekil 4: Gemi Teknoloji Ağları ve Saldırılara Hassas Sistemler[15].

2.3. Gemilerde Siber Saldırılara Hassas Sistemler

Denizciliğin emniyeti, güvenliği ve deniz çevresinin korunması için kritik olan çok sayıda sistemin işletilmesi ve yönetimi için siber güvenlik çok önemli hâle gelmiştir. Bu sistemlerin uluslararası standartlara uygun olması, siber tehditlere karşı dayanıklı olduğu anlamına gelmez. Bu sistemleri birbirine bağlamak veya ağ oluşturmak, yeni saldırı yüzeyleri oluşturur ve siber risklere yol açabilir. Siber risklere karşı savunmasız sistemler, zafiyetleri ve siber saldırı sonucu oluşabilecek zararlara ilişkin örnek tablo aşağıda yer almaktadır.

Sistem	Zafiyetler	Sonuçlar
Otomatik Tanımlama Sistemi (AIS)	- Sinyal paraziti - Yanlış bilgi paylaşımı - Kötü amaçlı yazılım - Yanıltma - Şifreleme olmaması - Sinyal karıştırma	- Geminin kaçırılması - Verilerin imhası - Değerli verilerin çalınması
Elektronik Harita Gösterim ve Bilgi Sistemi (ECDIS)	- Eski işletim sistemleri - Güvenli olmayan güncelleme ortamları	- Navigasyon sistemleri ile iletişim kaybı - Geminin kaçırılması - Hassas veri hırsızlığı - Bilgisayarları ve işletim sistemlerini tehlikeye atmak
Küresel Navigasyon Uydu Sistemi (GNSS) ve Küresel Konumlama Sistemi GPS	- Sinyal karıştırma - Zayıf sinyal gücü - Sinyal paraziti - Yanıltma - DoS/DDoS saldırıları - Paket modifikasyonu	- Geminin kaçırılması - Navigasyon sistemleri ile ilgili sorunlar - Yanlış gemi konumu - Gemi operasyonunun kesintiye uğraması - Servislerdeki gecikmeler
Radar	- Sinyal karıştırma - Yanıltma - DoS/DDoS saldırıları	- Navigasyon sistemleri ile iletişimin kesilmesi - Can ve mal kaybı - Kargo yönetiminde gecikmeler
Küresel Denizcilik Tehlike ve Güvenlik Sistemi (GMDSS)	- Kötü amaçlı yazılım - Yanıltma - DoS/DDoS saldırıları	- Yanlış gemi konumu - ECDIS'e yeni saldırılar

Tablo 2: Siber Saldırılara Hassas Sistemler[15]. (devam ediyor)

Sistem	Zafiyetler	Sonuçlar
Endüstriyel Kontrol Sistemleri (ICSs)	- Yetersiz erişim kontrol yönetimi - Bütünlük kontrolü için destek azlığı - Bilgi teşhiri - Kötü yama yönetimi - Donanım arızaları - Uygun olmayan güvenlik yapılanması - Ağ segmentasyonu eksikliği - Zayıf şifre politikaları - Güvenlik duvarlarının olmaması - Şifreleme eksikliği - Zayıf uzaktan erişim politikaları - Zayıf USB politikası - Sistemin güvenli çalışması için eğitim eksikliği	- Geminin kaçırılması - ICS'nin kullanılamaması - Veri sızıntısı - Tesislerde fiziksel hasar - Güvenlik sistemlerine müdahale - Planlanmamış kapatmalar - Ekipman hasarı
Tahrik ve Makine Yönetimi/Güç Kontrol Sistemleri	- Kötü amaçlı yazılım - DoS/DDoS saldırıları - Kaçakçılık - Çalma - Manipülasyon saldırıları	- Hassas verilerin ifşası - Geminin kaçırılması - Geminin yön değiştirmesi - Güç sisteminin kesintiye uğraması - Gemi hasarı - Mali zarar
Very Small Aperture Terminal (VSAT)	- Kötü amaçlı yazılım - Sahte sinyaller - Çalma	- Hassas verilerin çalınması - Kötü amaçlı yazılım yükleme - GPS koordinatlarının değiştirilmesi
BT Ağ Sistemleri	- Zayıf erişim kontrolü - DoS/DDoS saldırıları - Zayıf şifre politikaları - Kötü amaçlı yazılım saldırıları - Kötü yama yönetimi - Uygun olmayan güvenlik yapılandırması - Kötü güvenlik dokümantasyonu - Ağ segmentasyonu eksikliği - Güvenlik duvarı olmaması - Şifreleme eksikliği - Zayıf uzaktan erişim politikaları - Zayıf USB politikası - Sistemin güvenli çalışması için gerekli eğitim eksikliği	- Zararlı yükleme - İzinsiz fiziksel giriş - İzinsiz mantıksal giriş - Gizli belgelerin çalınması - Mali hasar - Hassas verilerin çalınması - İtibar zedelenmesi

Tablo 2: Siber Saldırılara Hassas Sistemler[15]. (önceki sayfadan devam)

3. AXLocker Fidye Yazılımı ile Hesaplarınız Çalınabilir!

3.1. Fidye Yazılımı (Ransomware) Nedir?

Fidye yazılımları 2010 yılından itibaren siber güvenlik alanında saldırganlar için ciddi bir gelir kaynağı olmuştur. Fidye yazılımı, saldırganların telefon, bilgisayar ve benzeri dijital cihazlarda bulunan elektronik verileri ele geçirip sonra dosyalara yeniden erişim sağlama karşılığında belirli bir miktar para, yani fidye talep etmek için kullandıkları zararlı yazılımlara denir. Saldırganlar, fidye yazılımlarını çok çeşitli yöntemlerle cihazlara bulaştırmaktadır. Örneğin; sosyal mühendislik yöntemini kullanarak, kötü amaçlı reklam içeriklerinden ve güvenlik zafiyetlerinden yararlanırlar. Fidye talebinde de çeşitli şekillerde bulunabilirler. İlk olarak fidye yazılımı virüsü bulaştığında dosyaların belirli bir kısmını ya da tamamını şifreleyebilirler. Böyle bir durumla karşılaşıldığında dosyalara erişmek mümkün olmaktan çıkar. Bunun üzerine saldırgan dosyaların şifresini paylaşmak için fidye talebinde bulunur. İkinci bir yöntem ise kendini güvenilir bir kişi olarak göstererek korsan yazılım ile bilgisayarı kilitlediğini söyler. Ardından para talebinde bulunur. Son olarak hassas verileri kamuoyunda paylaşmak tehdidiyle fidye talebinde bulunabilir. Son zamanlarda saldırılarda çeşitli yöntemler gelişmiş olup saldırı boyutları genişlemiş ve birçok önemli firma, kurum ve kuruluş bu saldırılara maruz kalmıştır [16].

Şekil 5: Ransomware[17].

3.2. Fidye Yazılımları Nasıl Tespit Edilebilir?

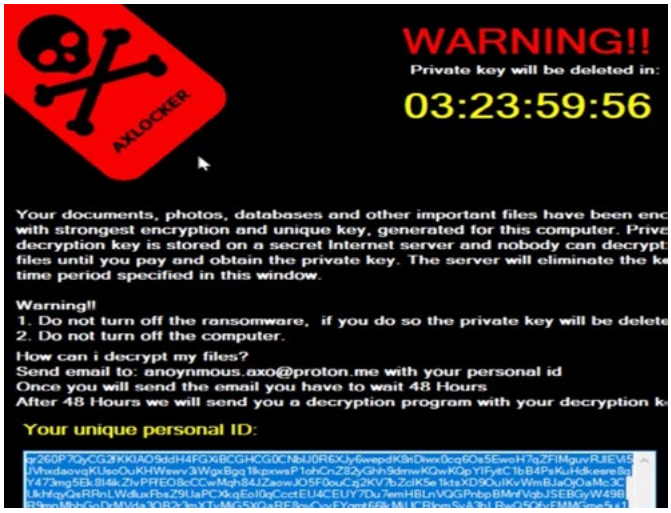
Signature-based (imza-tabanlı) olarak bilinen hash örnekleri karşılaştırılarak, makine öğrenmesi gibi yöntemlerle geçmiş bilgiler öğrenilerek ya da honeypot gibi sistemlerle saldırganlar tuzağa düşürülerek şüpheli durumlar yakalanabilir ve zararlı durumlar tespit edilebilir[18].

3.3. Fidye Yazılım Çeşitleri Nelerdir?

- **Scareware:** Tedirginlik oluşturarak, aslında verileri şifrelemeden fidye almayı amaçlayan bir yazılım çeşididir.
- **Screen Locker:** Ekranı kilitleyen bir görüntü oluşturarak fidye almayı hedefleyen bir yazılım çeşididir.
- **Encrypting Ransomware:** Dosyaları şifreleyerek verilere erişimi gerçekten engelleyen yazılım çeşididir.
- **Leakware:** Saldırganın verilere izinsiz erişim sağlayarak kopyaladığı ve bunları paylaşacağı tehdidiyle fidye almayı hedeflediği yazılım çeşididir.
- **Lockers:** Bilgisayarı tamamen kilitlemek için işletim sistemine bulaşan bir fidye yazılımıdır.

Son zamanlarda sıkça duyulan bir Lockers fidye yazılım çeşidi olan AXlocker, verileri kilitlemek için kullanılır. Zararlı cihaza bulaştığında bulunan dosyaları tarayıp AES algoritması ile şifreler. AXLocker, dosya adlarını değiştirmez. Saldırgan, diğer fidye yazılım türlerinden farklı olarak fidye talebini başka bir ortamdan iletir ve kurbana kısa bir süre tanıdığını vurgular.

Cyble'daki araştırmacılar AXLocker fidye yazılımının bir örneğini incelediler. İnceleme sonucunda saldırganların şifrelemekle yetinmeyip sosyal medyalarından Discord uygulamasındaki hesaplarını da çaldıklarını tespit etmişlerdir. AES algoritması kullanılmasına rağmen şifrelenmiş dosyalara dosya adı uzantısı eklenmemektedir. Dosyalar olduğu gibi görünmektedir[20].



Şekil 6: Axlocker Ransomware örneği[19].

Discord hesaplarını çalmak için, AxLocker aşağıdaki düzenli ifadeleri kullanmaktadır:

- Discord\Local Storage\leveldb
- discordcanary\Local Storage\leveldb
- discordptb\leveldb
- Opera Software\Opera Stable\Local Storage\leveldb
- Google\Chrome\User Data\\Default\Local Storage\leveldb
- BraveSoftware\Brave-Browser\User Data\Default\Local Storage\leveldb
- Yandex\YandexBrowser\User Data\Default\Local Storage\leveldb

Bu düzenli ifadeler kullanılarak hesapların çoğunun çalındığı görülmüştür.

3.4. Fidye Yazılımından Nasıl Korunulmalıdır?

Tehlike oluşturacağını düşündüğümüz url, e-posta gibi bağlantılardan uzak durulmalıdır. E-posta girişinde kimlik doğrulması yapılmalıdır. Önemli olduğu düşünülen dosyalar yedeklenmelidir. Güncellenmiş antivirüs programları kullanılmalıdır. Güçlü spam filtreleri kullanılmalıdır. Güncellemeler sıklıkla yapılmalıdır. Tarayıcı oluşturulması önerilir. Kişisel bilgilerin paylaşılmasından kaçınılmalıdır. Bilinen kara listeye eklenen IP'lerin engellenmesi gibi çeşitli yollarla fidye yazılımından korunabilir.

4. Matrix Mesajlaşma Protokolü Zafiyetleri

Matrix, merkezi bir sunucu yerine sunucular arası bağlantılarla çalışan bir mesajlaşma protokolüdür. Uçtan uca şifreleme için Double Ratchet[21] bazlı Olm ve Megolm sistemlerini kullanır[22]. Matrix, çeşitli proje, şirket ve kamu kuruluşlarının yanında Alman ordusunun özel gizlilik seviyesindeki (VS-NfD) iletişiminde kullanılmaktadır[23].

Londra Üniversitesi, Sheffield Üniversitesi ve Brave'den araştırmacılar, Matrix protokolünün tasarımında ve resmi kütüphanelerinde toplam altı zafiyet saptamıştır. Bu zafiyetlerin beşi pratik olarak uygulanabilir[24].

4.1. Zafiyet 1: Eksik Adaptasyondan Gizlilik İhlali

Signal protokolünde, merkezi sunucunun yanında her kullanıcının kanonik cihazı bulunur. Bu ana cihaz, diğer cihazların (uç noktaların) bağlanması ve mesajları almasını sağlar. Böylelikle karşı taraf, kullanıcının kanonik cihazı tarafından doğrulanmamış cihazlara mesaj şifrelemez.

Matrix'de kanonik cihaz kavramı olmadığından yeni cihaz eklemez. Bu görev, protokol tasarımında sunuculara düştüğünden ilk zafiyet ortaya çıkmaktadır.

Kullanıcılarından birini barındıran herhangi bir sunucu, kendisine de şifrelenen bir uç noktayı grup üyesi ya da kullanıcı cihazı altında ekleyebilmektedir.

4.2. Zafiyet 2: Bant Dışı Doğrulama İhlali

Domain ayrıştırması, operasyonların, yapılan benzer operasyonların kullanımına göre ayrılması prensibidir. Çeşitli yollarla elde edilebilir, yaygın kullanımı hash fonksiyonunun veriye uygulanmadan önce özetlenecek verinin tip ve/veya sürümünün verilmesidir.

Teorik olarak gereksinim olmamasına rağmen, mühendislik uygulaması olarak çeşitli karıştırma saldırılarının önüne geçtiği için tasarım süreçlerinde domain ayrıştırması kullanılması tercih edilmektedir. Bu uygulamanın eksikliği nedeniyle ikinci zafiyet ortaya çıkmaktadır.

Bu zafiyette, niyetli bir sunucu, bir kişi ilk kaydolduğu zaman alternatif kimlik anahtarı oluşturup aynı zamanda bir cihaz olarak kaydeder. Resmi JavaScript kütüphanesinde olan bir hata nedeniyle bant dışı doğrulama mekanizması, kimlik anahtarı yerine cihaz anahtarı üzerinden yapılabilir. Bunun sonucunda bant dışı doğrulamanın onayına rağmen bir sunucu MITM saldırısı gerçekleştirebilir.

4.3. Zafiyet 3: Yarı-güvenilen Kişilik Taklidi

Bu zafiyette, art niyetli bir sunucu ile kullanıcı cihazı, resmi kütüphanede olan bir hata nedeniyle diğer kullanıcılarının Megolm oturumlarını taklit edebilir. Zafiyetin kullanılması ile yollanan mesajların gerçekliği hakkında uyarı geldiğinden dolayı tam güvenilen taklit değildir. Ancak, yapılabilen çeşitli operasyonlardan dolayı yarı-güvenilen durumunu kazanır ve zafiyet 4 ve 5'in altyapısını sağlar.

4.4. Zafiyet 4: Güvenilen Kişilik Taklidi

Bu zafiyette, yarı-güvenilen Megolm oturumları üzerinden "Olm" protokol mesajları yollanması ile protokol karışma saldırı yapılabilmektedir. "Olm" mesajları, bu saldırı sonucunda güvenilir mesaj olarak değerlendirilir.

4.5. Zafiyet 5: Yarı-güvenilen Kişilik Taklidinden Doğan Gizlilik İhlali

Bu zafiyette, yarı-güvenilen Megolm oturumu üzerinden şifrelenen yedeklerin SSSS ile paylaşılmış anahtarlarını elde edebilir. Zafiyetin düzeltilmesi için Megolm üzerinden yedekleme işlemleri yasaklanarak "Olm" kullanılır.

4.6. Zafiyet 6: IND-CCA İhlali

Matrix, mesajlar dışı şifreleme (yedekler vb.) için AES-CTR + HMAC-SHA-256 kullanmaktadır. AES-GCM'in donanımsal hızı ve ChaCha20-Poly1305'in yazılımdaki hızına sahip olmadığından tercih edilmemesine rağmen normalde güvenli bir Encrypt-then-MAC şemasıdır. Ancak, mesaj doğrulama kodunda CTR modunun IV'si dahil edilmediğinden son zafiyet ortaya çıkmaktadır.

Bir şifre/deşifre Oracle'ı, hedeflenen bir şifrelenmiş metni dolaylı yoldan çözebildiğinden IND-CCA güvenlik seviyesi ihlal edilmektedir. Bu zafiyet, protokolün bir hatası olup bir Oracle bulunana kadar teorik bir saldırı olarak kalmaktadır.

5. Veri Silme Yazılımlarının Önemi

5.1. Verilerin Silinmesinin Gerekliliği

Günümüzün yüksek teknoloji cihazlarında oldukça fazla veri depolanmaktadır. Dijital veriler sayısız ortam ve platforma yerleşmiş durumdadır ve veri akışı aralıksız devam etmektedir. Bilgisayar ve sunucu diskleri, cep telefonları, hafıza kartları ve taşınabilir cihazlar bu ortam ve platformların yalnızca birkaçıdır. Bu ortamlarda yer alan verilerin yanlış kişiler tarafından ele geçirilmesi ve kötü amaçla kullanılması oldukça büyük sorunlara neden olmaktadır. Bu sebeple BT varlıkları el değiştirdiğinde veya atıl duruma geldiğinde veri silme yöntemleri

Şekil 7: Dijital veriler de silinmelidir[25].

kullanılmalıdır. En çok tercih edilen veri silme yöntemleri aşağıda listelenmiştir.

- Fiziksel imha
- Degauss (manyetik alanı nötr hale getirme işlemi)
- Format işleminin uygulanması
- Donuk depolama
- Veri üzerine yazma işlemi gerçekleştiren veri silme yazılımları

5.2. Veri Silme Yazılımları

Çoğu kurum ve kuruluşun veri silmek ve varlık elden çıkarmak için bir bütçesi yoktur. Bu sebeple verileri silmek için format atmak gibi güvenli olmayan yöntemlere başvurulmaktadır.

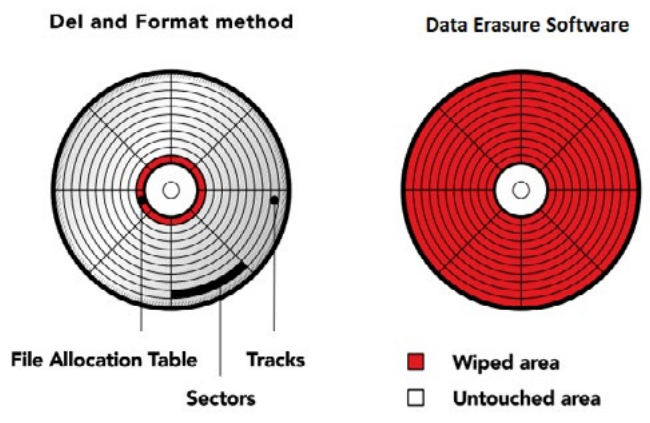
Basit bir veri silme yöntemi olan format atma işlemi verilerin geri dönüşü olmayacak şekilde silinmesi için yeterli değildir. Bu işlem yalnızca verilere giden yolu (path) siler, verinin kendisi varlığını sürdürmeye devam etmektedir.

Veri silme yazılımları mevcut verinin üzerine veri yazma işlemini uygular ve sürücü sektörlerinin üzerine anlamsız veriler yerleştirir. Veriler kurtarılmaya çalışıldığında, hücrelerde tutulan son veriler geri getirileceği için bunlar asıl veriler değil en son yerleştirilen anlamsız veriler olacaktır. Asıl veriler asla geri getirilemeyecektir.

Veri silme yazılımları ile veriler hiçbir şekilde geri dönüşü olmayacak şekilde silinebilir. Buna diskte yer alan gizli, kilitli ve haritalandırılmamış alanlar da dâhildir.

Veri silme işlemi tamamlandıktan sonra fiziksel imhanın aksine diskler ve diğer ortamlar yeniden kullanılabilir. BT varlıklarının veri silme yazılımları ile silinip geri dönüştürülmesi ya da yeniden kullanılabilir olması kurum ve kuruluşlara ekonomik açıdan katma değer sağlar.

Veri silme yazılımları gerçekleştirdikleri işlemin doğruluğunu kanıtlamak için her silme işleminden sonra bir silme raporu sunarlar. Bu rapor silme işleminin gerçekleştiğini ve verilerin geri getirilemez olduğunu gösterir.



Şekil 8: Format atılması ile veri silme yazılımlarının uygulanması arasındaki fark[26].

Veri silme yazılımları ülkemizde henüz yeterince kullanılmıyor olsa da dünya genelinde devletler, bankalar, hastaneler, şirketler, kuruluşlar ve geri dönüşüm işlemi yapan teknoloji firmaları tarafından kullanılmaktadır. Veri silme yazılımları işletim sistemi ayırt etmeden çalışabilir.

Veri silme yazılımları farklı yöntemler ile veri silme işlemini gerçekleştirebilir. Bu yöntemlerinin bazıları şunlardır.

- MSI paketleri kullanılarak silme
- Ağ üzerinden çoklu silme
- Ağda olmayan varlıklar için taşınabilir cihaz yardımıyla silme

Veri Silme yazılımlarının uygulanabildiği diğer ortamlar aşağıdaki gibidir.

- Dosya ve klasörler
- Mobil cihazlar
- Veri depolama üniteleri

Fiziksel imha süreci düzgün yapılmadığında bellek medyasından arta kalan parçalar kullanılarak veriler yanlış kişiler tarafından ele geçirilebilir. Bununla birlikte fiziksel imhanın çevreye verdiği zararı düşünürsek en güvenli ve çevreci veri silme yöntemi, veri silme yazılımlarının kullanılmasıdır diyebiliriz.

En çok tercih edilen silme yöntemlerine kıyasla veri silme yazılımları daha güvenli, ekonomik ve çevrecidir. Varlık yönetiminin sağlıklı bir şekilde sürdürülebilmesi için kurum ve kuruluşlara yardımcı olur. Veri silme yazılımlarını kullanmak genellikle en doğru çözüm olabilir.

6. Silah Sistemleri Siber Güvenliği

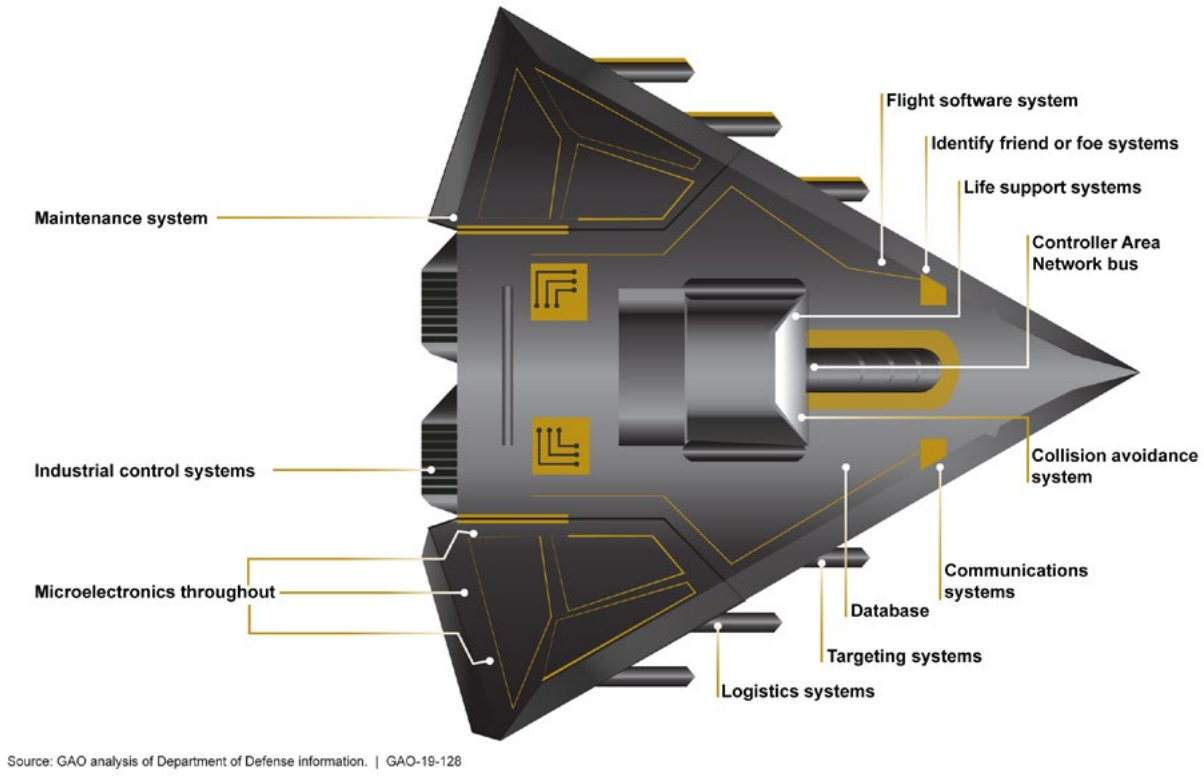
Bu yazıda açık kaynak taraması sonucunda elde edilen ABD Hükümet Sorumluluklar Ofisi'nin raporu incelenerek silah sistemlerinin siber güvenliği kapsamında yapılan tespit ve değerlendirmeler sunulmuştur.

İncelenen rapor ABD Hükümet Sorumluluklar Ofisinin (US GAO) Ekim 2018 tarihli "GAO-19-128" kimlikli "Weapon Systems Cybersecurity" başlıklı raporudur[27]. Rapor Savunma Bakanlığının (DOD) silah sistemleri siber güvenliğinin mevcut durumunu gözden geçirme amacıyla hazırlanmış ve silah sistemlerinin tedariği bağlamında siber güvenlik özelindeki ilk rapor olmuştur.

Raporun üç temel başlığı ele almaktadır:

1. Silah sistemlerinin siber güvenliğinin mevcut durumuna katkıda bulunan etkenler,
2. Geliştirilen silah sistemlerindeki zafiyetler,
3. Bakanlığın siber-dayanıklı silah sistemleri geliştirilmesi için aldığı önlemler.

GAO raporunda mevcut duruma katkıda bulunan etkenler belirlenirken; yazılım, bilgi teknolojileri, ağ ve silah



Şekil 9: Savaş uçağındaki gömülü yazılımlar ve BT sistemleri[27].

sistemleri konularını içeren ve kamu ve özel sektör kurum ve kuruluşları tarafından 1991 ve 2017 yılları arasında yayınlanmış raporlar gözden geçirilmiştir. Zafiyetlerin belirlenmesi sürecinde ise 2012 ve 2017 yılları arasında geliştirilmekte olan silah sistemlerinin siber değerlendirme raporları kullanılmıştır.

Raporda silah sistemlerini sofistike siber tehditlerden korumadaki artan zorlukların sebepleri olarak;

a. Silah sistemlerindeki bilgisayarlaşmanın artışı,
b. Bu sistemlerdeki siber güvenliğin önceliklendirilmesinde geç kalınması,
c. Güvenli sistem geliştirmenin nasıl yapılacağına ilişkin belirmeye başlayan maddeler sıralanmıştır.

Raporda hayali bir savaş uçağında gözlemlenebilecek farklı gömülü yazılım ve BT sistemleri temsili olarak Şekil-1'de gösterilmiştir:

Silah sistemlerinin bilgisayarlaşmasına yönelik çarpıcı bir istatistik DSB (Defense Science Board) Savunma Yazılımları Görev Gücünün Kasım 2000'de yayınlanan raporunda verilmiştir: 1960 yılında F-4 uçağı için yüzde 8 olan sistem işlevlerinin yazılımla karşılanma oranı 1982'de F-16 uçağı için yüzde 45'e, 2000 yılında F-22 uçağı için yüzde 80'e yükselmiştir[28].

GAO raporunda dikkat çeken konular aşağıda başlıklar altında irdelenmiştir:

Tespit edilen zafiyetler ve zorluklar:

a. **Görev kritik zafiyetler:** Sistemlere yönelik yapılan taramaların bazı sistem bileşenlerini hizmet dışı bıraktırması, yönetici seviyesi parolanın kısa zamanda tespiti ve varsayılan parolanın değiştirilmemesini içeren zayıf parola yönetimi, sistemlerde konumlandırılan Saldırı Tespit Sistemlerinin etkin ve verimli olarak kullanılmaması.
b. **Siber güvenlik işgücü zorlukları:** Sektöre özel yetkin çalışan sayısının kısıtlı olması, özel sektör rekabetinin olumsuz etkileri, siber-dayanıklı (cyber-resilient) sistemler tasarlarken gereken alan uzmanlığı eksikliği.
c. **Zafiyet ve tehdit bilgilerinin paylaşımındaki zorluklar**: Silah sistemleri siber güvenliği konusundaki bilgilerin yüksek seviyede sınıflandırılması sebebiyle DOD bünyesindeki diğer paydaşlarla paylaşılmaması yüzünden güvenlik bakımından kusurlu tasarımların yaygınlaşması.

Tespit edilen olumlu gelişmeler:

a. **Yeni oluşturulan veya güncellen politika, rehber ve genelgeler:** DOD siber güvenlikli silah sistemlerini destekleme amacıyla 2014 yılından itibaren bakanlık çapında en az 15 adet politika, rehber doküman ve genelge yayınlamış veya mevcutları güncellemiştir. Bu alandaki en çarpıcı gelişme; mevcut politikaların kapsamının silah sistemlerini açık bir şekilde

kapsayacak şekilde genişletilmesi olmuştur. Daha önce Bakanlığın ağlarını ve bilgi sistemlerini koruma için uygulanan kontrollerin etki alanı arttırılmıştır.

b. **Sistemler arasındaki zafiyetlere bütünleşik bakış:** Geliştirme ve operasyonel testler öncelikli olarak tekil sistemler seviyesindeki zafiyetlere yoğunlaşırken, görev odaklı yaklaşım zafiyetlerin mevcut görevin başarılmasına etkisine veya belirli yeteneklerin çalışmadığı durumlarda görevin tamamlanması için kullanılabilecek diğer seçeneklere yoğunlaşmaktadır. Bu yaklaşımı tetikleyen bir diğer husus sistemlerin yüzde 100 güvenli olamayacağının kabul edilmesidir. Bu yaklaşım siber dayanıklılık olgusunun bazı politikalarda vurgulanmasını getirmiştir. Siber dayanıklılık, belirli anahtar bileşenlerin belirlenmesi ve korunması ile sistemlerin siber saldırı altında kısıtlı yeteneklerle çalışmaya devam etmesinin sağlanması olarak tanımlanmaktadır.

c. **Gereksinimler seviyesinde ve tedarik süreçlerinde siber güvenliğin ele alınması:** Siber güvenlik gereksinimlerinin ve silah sistemlerinin işleyeceği bilginin giriş ve çıkış akışlarının belirlenmesi, böylelikle sisteme ait saldırı yüzeyinin çıkartılması ve en nihayetinde sistem tasarımının ve uygulanacak siber kontrollerin belirlenmesidir. Günümüzde siber güvenlik endüstrisinde "Tehdit Modelleme" olarak adlandırılan kavramının kullanımı hem askeri hem de sivil sektörlerde artmaktadır.

7. ProxyNotShell: CVE-2022-41040 ve CVE-2022-41082 Zafiyetleri

Microsoft, Windows Exchange e-posta sunucularını etkileyen iki güvenlik açığı yayınladı. Bir öncekine benzer şekilde, bu güvenlik açıkları ProxyNotShell güvenlik açıkları olarak adlandırılmıştır. ProxyNotShell güvenlik açıkları, saldırganlar tarafından zafiyetli Exchange sunucularında uzaktan kod yürütme (RCE) için kullanılmaktadır. Kurban istatistikleri istismar edilen Exchange sunucularının güncel olduğunu ve ProxyShell güvenlik açıklarına karşı yama yapılmış olduğunu göstermektedir.

Keşif sırasında ProxyNotShell güvenlik açıklarının, Exchange sunucusunun en son sürümlerini etkilediği görülmüştür. 8 Kasım 2022'de Microsoft, Exchange Server için güncellemeler yayınladı ve kuruluşlara Exchange sunucularını en son sürüme güncellemeleri tavsiye edildi.

7.1. ProxyNotShell Nedir?

ProxyNotShell, önceki ProxyShell gibi tek bir güvenlik açığı değil, Microsoft Exchange e-posta sunucularının kontrolünü ele geçirmek için aynı anda kullanılabilen bir güvenlik açıkları koleksiyonudur. Exchange sunucularının en son sürümlerini etkiledikleri için, ProxyNotShell güvenlik açıkları sıfır gün güvenlik açıkları olarak kabul edilmektedir[29].

CVE-2022–41040: İlki, Sunucu Taraflı İstek Sahtekârlığı (SSRF) güvenlik açığıdır. Bu güvenlik açığı, kimliği doğrulanmış bir saldırganın ikinci güvenlik açığı olan CVE-2022–41082'yi uzaktan tetiklemesine olanak tanır[30].

CVE-2022–41082: Bu güvenlik açığı, saldırgan PowerShell'e erişebildiğinde Uzaktan Kod Yürütmeye (RCE) izin verir.

CVE-2022–41040 ve CVE-2022–41082 zafiyetlerinin istismar edilmesi, saldırı akışı açısından ve sebebiyet verdiği ataklar olan SSRF/RCE çiftini izlediğinden ProxyShell zafiyetlerine benzetilmiştir. Ancak ProxyShell açıklarından farklı olarak Exchange sunucusuna kimliği doğrulanmış erişim gerektirdiği için bu güvenlik açıkları zincirine ProxyNotShell adı verilmiştir.

7.2. ProxyNotShell'in Teknik Detayları

ProxyNotShell güvenlik açıklarından ilki olan CVE-2022–41040, Exchange Autodiscover ön ucunda bulunan, kimliği doğrulanmamış kullanıcı tarafından gerçekleştirilebilen bir Sunucu Taraflı İstek Sahtekârlığı (SSRF) güvenlik açığıdır. 8.8 (Yüksek) CVSS puanına sahiptir. Saldırganlar, LocalSystem yetkilerine sahip rasgele bir arka uç hizmetine kontrollü bir URI ve kontrollü verilerle rasgele bir istek göndermek için CVE-2022-41040 güvenlik açığından yararlanmaktadır.

ProxyNotShell HTTP İsteği:

```
GET /autodiscover/autodiscover.json?@zdi/PowerShell?serializationLevel=Full;ExchClientVer=15.2.922.7;clientApplication=ManagementShell;TargetServer=;PSVersion=5.1.17763.592&Email=autodiscover/autodiscover.json%3F@zdi HTTP/1.1
Host: 192.168.1.10
Authorization: Basic cG9jdXNlcjpwb2NwYXNzd2QK
Connection: close
```

Şekil 10: Kimliği doğrulanmış olarak gönderilen HTTP isteği[54].

ProxyNotShell HTTP Cevabı:

```
HTTP/1.1 200 OK
Cache-Control: private
Server: Microsoft-IIS/10.0
request-id: af13615a-6dae-40d5-b486-964eb329ba06
X-CalculatedBETarget: win-6kf62kusui9.zdi.local
X-AspNet-Version: 4.0.30319
Set-Cookie: X-BackEndCookie=S-1-5-21-1545661678-133831305-1065626216-1642=u56Lnp2ejJqBnJnLzpyez8rSzsvJydLLnid0p7Lm8nSzsvLyc2anczHx86agYHNz83N0s7P0s/Gq8/Hxc/Ixc/IgYWbltGTkJyek4HP; path=/autodiscover; secure; HttpOnly
```

Şekil 11: Kimliği doğrulanmış olarak gönderilen HTTP isteğine dönen HTTP cevabı[54].

ProxyNotShell güvenlik açıklarından ikincisi olan CVE-2022-41082, Exchange PowerShell arka ucunda bulunan bir uzaktan kod yürütme güvenlik açığıdır. 8,8 (yüksek) CVSS puanına sahiptir. Saldırganlar, CVE-2022-41040'ı kötüye kullanarak kimlik doğrulamasını atladıktan sonra, güvenlik açığı bulunan Exchange sunucularında rasgele komutlar çalıştırmak için CVE-2022-41082'den yararlanmaktadır.

Yapılan incelemelerde başarılı bir istismarın ardından saldırganların, kalıcılık sağlamak ve yanal hareket (lateral movement) teknikleriyle ilerlemek için Exchange sunucularına bir arka kapı (backdoor) yerleştirdikleri görülmüştür.

8. Mor Takım Nedir

Mor takım çalışmaları, kırmızı ve mavi takımın ortaklaşa çalışmasından ortaya çıkan bir kavramdır. Kırmızı takım ve mavi takım tanımlamaları askeri terminolojiden çıkmaktadır. Bu kavramlar Birinci Dünya Savaşı sırasında tanıtılmış olup, "Savaş oyunu" olarak da nitelendirilen ve günümüzde birçok yerli, yabancı devlet kuruluşları ve özel sektör kuruluşlarının saldırı ve savunma yeteneklerini test etmek amacıyla uyguladığı tatbikatlardır.

Saldırı tarafında olan ekibe kırmızı, savunma tarafında olan ekibe de mavi rengi verilmiştir. Mor takımı anlamak için kırmızı ve mavi takımları anlamak gerekir.

8.1. Mavi Takım

Mavi takım çalışmalarını, içeriden ve dışarıdan gelebilecek her türlü tehdide karşı koruma sağlamak olarak özetleyebiliriz Organizasyonların mavi takımları, organizasyonun bütün varlıklarını ve topolojisini bilmek zorundadır. Böylece hem içeride bir tehdit var ise avlamak daha kolaylaşacak hem de alınan önlemlerle olası tehditlerin gerçekleşmeden önüne geçilecektir.

Genel olarak mavi takım bütün topolojiyi (sunucular, son kullanıcılar, ağ ve ağ üzerinde bulunan bütün cihazları) izler, sistemsel verileri toplar, kritik ve korunması gereken bilgi/belge/varlıkları sınıflandırır, risk değerlendirmeleri yapar, parola politikaları kurar, güvenlik prosedürlerinin anlaşılmasını ve bunlara uyulmasını sağlamak için personeli eğitmek de dahil olmak üzere birçok şekilde sisteme erişimi sıkılaştırır ve sistemi güvenli yapma konusunda diğer ekiplere katkıda bulunur.

Anlatılan çalışmalara örnek olarak şunlar sayılabilir:

- Mimaride bulunan bütün cihazlara ve akıllı telefonlar gibi harici cihazlara uç nokta güvenlik yazılımı yüklemek ve izlemek
- Güvenlik duvarı erişim kontrollerinin düzgün bir şekilde yapılandırıldığından ve zararlı yazılımlardan koruma yazılımlarının güncel tutulduğundan ve çalıştığından emin olmak
- IDS ve IPS çözümlerini devreye almak ve yönetmek
- Güvenlik açığı tarama yazılımlarını düzenli olarak kullanmak
- Ağ etkinliğini loglamak ve analiz etmek için SIEM çözümleri uygulamak
- Sistemdeki olağan dışı etkinliği tespit etmek ve ilerlemesini önlemek

8.2. Kırmızı Takım

Kırmızı takım, sistemlere saldırma ve sistemin savunmalarını etkisiz hâle getirme alanında çalışan güvenlik uzmanlarından oluşur. Hedef sistemin varlıklarına yetkisiz erişim elde etmek için insanlardaki, süreçlerdeki (bu süreçlere örnek olarak fiziksel girişteki güvenliği veya kurum içinde verilen kartları, kurumun katları arasındaki segmentasyonları örnek verebiliriz) ve teknolojilerdeki zayıflıkları bulmak için her türlü teknik, taktik ve prosedürü kullanırlar. Bu simüle edilmiş saldırıların bir sonucu olarak kırmızı takımlar, organizasyonun mevcut güvenlik durumu hakkında rapor hazırlar, güvenlik durumu zayıf ise nasıl güçlendirilebileceği konusunda önerilerde bulunurlar. Genel olarak sızma testi ile karıştırılsa da arada farklar vardır.

8.3. Kırmızı Takım ve Sızma Testi Arasındaki Farklar

Kırmızı Takım	Sızma Testi
Tehdit aktörlerinin gerçek hayatta gerçekleştirebileceği senaryolar uygulanır. Buna fiziksel girişimler de dahildir. (Kart kopyalamak veya hedef sisteme zararlı yazılım barındıran usb dahil etmek gibi)	Sistemde bulunan zafiyetler hakkında genel bir görüş sağlar.
Kapsam belirsiz ve değişkendir. Genel olarak bir belge veya bilgi sızdırılmaya çalışılır.	Organizasyonun belirlediği kapsam dahilinde test yapılır.
Tehdit aktörlerinin teknik, taktik ve prosedürleri çıkartılarak buna uygun testler yapılır.	Tarama ve bulunan açıklıkların ispatlanmasını kapsayan bir genel metodoloji ile testler yapılır. (OWASP, OSSTMM, vb.)
Organizasyon genelinde birkaç kişi dışında kimsenin haberi olmadan gerçekleştirilir.	Test yapılan organizasyonda çalışan uzmanlar test yapıldığından haberdardır.

8.4. Tehdit Aktörleri ve Gelişmiş Sürekli Tehditler (APTs)

Tehdit aktörleri aslında gelişmiş sürekli tehditlerin arkasındaki aktörlerdir. Gelişmiş kalıcı tehdit (apt), tehdit aktörlerinin hassas verileri çalmak için hedef organizasyonda, operasyonlarını uzunca bir süre gizli bir varlık olarak sürdürdüğü karmaşık ve sürekli bir siber saldırıdır. Hedef olan organizasyona sızmak için kullandıkları senaryoları ayrıntılı olarak planlar ve tasarlarlar.

Ayrıca tehdit aktörleri, genellikle yüksek değerli kuruluşları (Amazon, Facebook, Twitter vb.) ve kritik veri tutan

kuruluşları (istihbarat bilgileri, kişisel veriler, ticari bilgiler vb.) hedef alırlar. Çok iyi finanse edilirler, bu da genelde devletler tarafından yapılabilir.

Potansiyel olarak verebilecekleri zararlar çok büyük olduğu için günümüzde bu tehditlerin araştırılması gibi bir ihtiyaç söz konusudur. Gelişmiş sürekli tehditleri her araştıran kuruluş bu tehditleri kendine göre adlandırır. Bunun için gelişmiş bir sürekli tehdidin birden fazla adı vardır. Adlandırmalar farklı olsa da analizlerde ortak olan noktalar, hedefleri (yani bu grup finansal kurumları hedef alıyor gibi), teknikleri, taktikleri, prosedürleri ve hangi ülkeye ait oldukları veya hangi devlet tarafından fonlandıkları konusundaki görüş ortaktır.

Aşağıda bir grubun farklı şirketler tarafından yapılan farklı adlandırmalarının bir örneği görülmektedir:

- Fancy Bear (Crowd Strike)
- APT28 (Mandiant)
- Pawn Storm (Trend Micro)
- Sofacy Group (Kaspersky)
- Sednit (Eset)
- Tsar Team (Fireeye)
- STRONTIUM (Microsoft)

Şekil 12: Fancy Bear grubunun Crowd Strike tarafından çizimi[56].

8.5. Siber Ölüm Zinciri

Birçok siber terim gibi siber ölüm zinciri de askeri bir terim olan ölüm zincirinden türemiştir. Ölüm zinciri terimi bir saldırının genel yapısını ve işleyişini tarif eder. İlk olarak 2011 yılında Lockheed Martin tarafından geliştirilen siber ölüm zinciri, birkaç yaygın siber saldırının çeşitli aşamalarını ve buna bağlı olarak mavi takımın saldırganları tespit edebileceği, önleyebileceği veya engelleyebileceği noktaları özetler.

Zincir toplam yedi aşamadan oluşur.

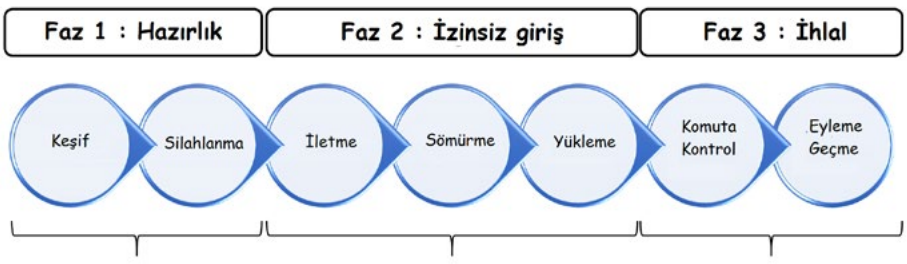
- **Keşif Aşaması**: Hedef hakkında bilgi toplama aşamasıdır. Bu sürecin bir parçası olarak, tehditler hedef sistem kullanıcılarının oturum açma kimlik bilgileri, e-posta adresleri, kimlikleri, fiziksel konumları, yazılım uygulamaları ve kullanılan işletim sistemi ayrıntıları gibi, saldırılarında yararlı olabilecek bilgileri toplarlar. Aktif ve pasif bilgi toplama yapılır.

  Pasif bilgi toplamada; hedef sistem hakkında bilgi toplanırken, sunucu ile doğrudan iletişime geçmeden yapılan bilgi toplama yöntemidir (maltego, shodan, harvester).

  Aktif bilgi toplamada; hedef sistem hakkında bilgi toplanırken sunucu veya sistem ile doğrudan iletişime geçilerek yapılan bilgi toplama yöntemidir (nmap).

Tehditler keşif aşamasında ne kadar fazla bilgi toplayabilirse, saldırı o kadar karmaşık ve inandırıcı olacak ve dolayısıyla başarı olasılığı o kadar yüksek olacaktır.

- **Silahlanma Aşaması:** Bu aşamada tehdit aktörleri, bilinen veya daha önce hiç keşfedilmemiş bir güvenlik açığından yararlanabilen zararlı yazılımlarını hedefe özel hâle getirerek bir saldırı vektörü oluştururlar. Ayrıca sosyal mühendislik veya fiziksel erişim gerekecek bir vektör hazırlanıyor ise o hazırlıklar da bu aşamada gerçekleşir (örnek olarak oltalama için e-posta hazırlanması, fiziksel erişim ile sisteme dahil olma için USB vb. aygıtlar hazırlanması).
- **İletme Aşaması:** Saldırının başladığı bölümdür. Bir önceki adımda planlanan vektöre göre gerçekleştirilir. (Örneğin, tehdit aktörü oltalama kullanmaya karar vermişse bu aşamada zararlı linkli bir e-posta veya bir SMS gönderebilir.)



Şekil 13: Siber ölüm zinciri[31].

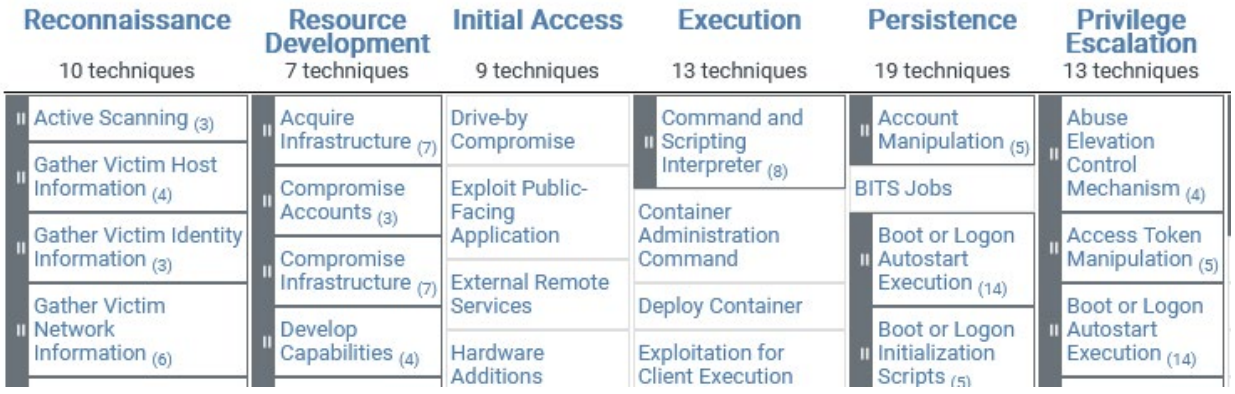
- **Sömürme Aşaması:** Bu aşamada aslında hazırlanan zararlı yazılımı hedef sistemde çalıştırmaya yönelik ilk kapı açılır (bu, teknolojideki bir açıklık da olabilir, başarılı bir oltalama senaryosundan sonra son kullanıcının tehdit aktörünü sisteme dahil etmesi de olabilir.)
- **Yükleme Aşaması:** Sömürü aşamasının hemen ardından, planlama aşamasında planlanan vektöre uygun olarak bir zararlı yazılım ya da atak vektörü hedef sisteme dahil edilir. Tehdit aktörü sisteme girdiğinden ve artık kontrolü ele aldığından, bu saldırı yaşam döngüsünde bir dönüm noktasıdır.
- **Komuta Kontrol Aşaması:** Bu aşamada hedef sistem tamamen veya kısmi olarak ele geçirilmiştir. Bir önceki aşamada sisteme yüklenen zararlı yazılım tehdit aktörünün kontrol ettiği bir komuta sunucusuna haberleşme kanalı açar. Böylelikle tehdit aktörü uzaktan kod çalıştırabilir hâle gelir. Ayrıca ağ boyunca yanal olarak hareket etmek, erişimlerini genişletmek ve gelecek için daha fazla giriş noktası oluşturmak için de çalışabilir. Aynı zamanda kendini izole etmeyi de başarabilir.
- **Eyleme Geçme Aşaması:** Bu aşamada tehdit aktörü, veri hırsızlığı, imha, şifreleme vb. artık amaçlanan hedeflerini gerçekleştirmek için adımlar atarlar.

8.6. MITRE ATT&CK Matrisi

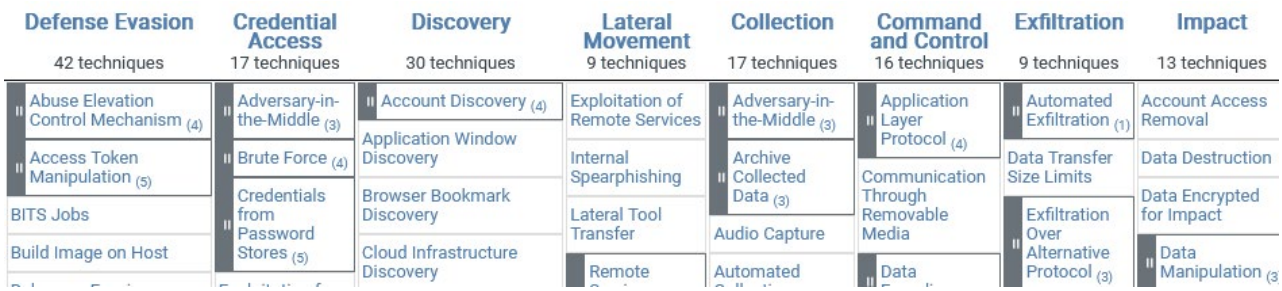
MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) matrisi, belirli bir amacı gerçekleştirmek için tehdit aktörleri tarafından kullanılan teknik, taktik ve prosedürleri içeren bir bilgi tabanıdır. Temel olarak açık kaynak tehdit istihbaratı ve olay müdahalelerin raporlamasının yanı sıra siber güvenlik analistleri ve tehdit avcılarının da katkıda bulunduğu yeni teknikler üzerine araştırmalarla beslenir. Aynı profesyoneller tarafından, tehdit aktörlerinin farklı davranışlarını daha iyi anlamak için kullanılır, böylece tehdit davranışları ön görülebilir, tespit edilebilir ve durdurulabilir.

Toplamda 14 taktik vardır:

- **Keşif:** Tehdit aktörlerinin hedef sistemleri için bilgi toplama taktikleri.
- **Kaynak geliştirme**: Tehdit aktörlerinin operasyonları için kullanılacakları zararlı yazılım gibi kaynakları oluşturma taktikleri.
- **İlk erişim:** Tehdit aktörlerinin ağa katılmaya çalışırken uyguladığı taktikler.
- **Uygulama:** Zararlı yazılım veya zararlı kod çalıştırma taktikleri.
- **Kalıcılık**: Tehdit aktörlerinin sistemde kalıcı olma taktikleri.
- **Yetki yükseltme**: Tehdit aktörlerinin sistemde yüksek yetkileri olan kullanıcı bulma veya yaratma taktikleri.
- **Savunma mekanizmalarını atlatma:** Tehdit aktörlerinin sistemde fark edilmeden çalışma taktikleri.
- **Kimlik bilgileri erişimi**: Tehdit aktörlerinin sistemde bulunan hesap isimleri ve/veya parolaları çalma taktikleri.



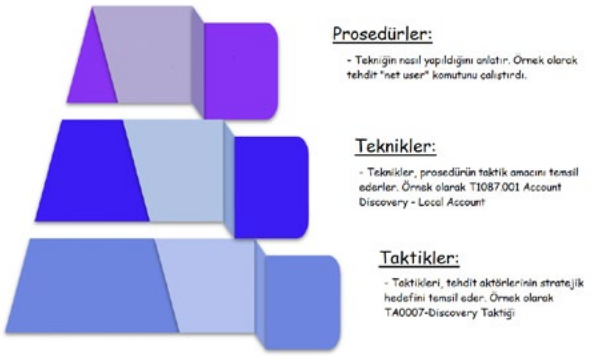
Şekil 14: Mitre Attack matrisi[32].



Şekil 15: Mitre Attack matrisi devamı[32].

- **Araştırma**: Tehdit aktörlerinin sistem hakkında daha detaylı bilgiler (mimaride kullanılan teknolojiler vb) edinme taktikleri.
- **Yanal hareket**: Tehdit aktörlerinin hedef sistemlerin alt sistemleri arasındaki bölme ve kısıtlar arası hareket etme taktikleri.
- **Toplama**: Tehdit aktörlerin sistem doğrultusunda veri toplama taktikleri. Araştırma taktikleri sistem hakkında bilgi sağlarken, toplama taktikleri daha sonra potansiyel atak vektörlerinde kullanılabilecek veriler elde eder. Buna örnek olarak kullanılan kablosuz ağın şifresini elde etmek veya kullanılan veritabanlarından veri toplamak gösterilebilir.
- **Komuta kontrol**: Tehdit aktörlerinin ele geçirilen sistemin uzaktan yönetilebilmesi için gerekli taktikler listelenmiştir.
- **Veri dışarı çıkarma:** Tehdit aktörlerinin sistem dışına veri çıkarma taktikleri.
- **Etki**: Tehdit aktörlerinin ele geçirdikleri verileri/sistemleri maniple etme, kesintiye uğratma veya silme gibi yıkıcı işlem taktikleri.

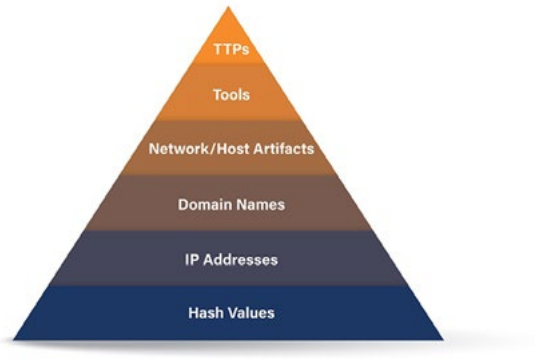
8.7. Teknikler, Taktikler, Prosedürler



Şekil 16: Teknik, Taktik ve Prosedürler[33].

MITRE matrisinde mevcut durumda 193 teknik, 401 de alt teknik bulunmaktadır. Teknik T1087, alt teknik de 001 olarak adlandırılır.

8.8. Acı Piramidi



Şekil 17: Acı Piramidi[34].

Bu şema mavi takımın ağında filtrelediği verileri ve piramidin yukarılarına çıktıkça tehdit aktörlerinin başarıya ulaşma şanslarının çok azalacağını gösterir.

Örnek olarak tehdit aktörü bir zararlı yazılım kullansın. Eğer mavi takım sistemlerinde bu zararlı yazılımın özet değeri için bir önlem aldı ise tehdit aktörleri kodlarında en ufak bir değişiklik bile yapsa bu önlemi atlatacaktır. Ama mavi takım bu zararlı yazılımı kullanan tehditlerin genel olarak teknik, taktik ve prosedürlerini takip ediyorsa ve bu doğrultuda sistemlerini izliyorsa tehdit aktörlerinin başarıya ulaşma şansı ciddi şekilde azalır.

8.9. Kırmızı Takım Çalışmalarını Simüle Eden Uygulamalar

Tehdit aktörlerinin teknik, taktik ve prosedürleri simüle edilip sonucunda üretilen alarmlar çalışılarak, mavi takımın bu yöntemleri sistemlerinde izlemesine, bunlara göre kurallar yazarak sistemi filtrelemesine yardımcı olacak açık kaynak uygulamalar vardır. Bunlar;

- Caldera: https://github.com/mitre/caldera
- Atomic Red: https://atomicredteam.io/
- Purple Team ATT&CK Automation: https://github.com/praetorian-inc/purple-team-attack-automation

DÖNEM KONUSU

9. CB DDO BİG Rehberi Uyumluluk Denetimi

9.1. Bilgi ve İletişim Güvenliği Rehberi

Kamu kurumları ile Ulusal Siber Güvenlik Stratejisinde belirlenen kritik altyapı sistemleri barındırmakta olan sektörlerin (elektronik haberleşme, enerji, finans, ulaştırma, su yönetimi ve kritik kamu hizmetleri) uyması gereken Bilgi ve İletişim Güvenliği tedbirlerini içeren 2019/12 sayılı Cumhurbaşkanlığı Genelgesi 06.07.2019 tarihinde yayınlanmıştır.

Genelge ile; güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği; bütünlüğü ya da erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amaçlanmıştır. Bu çerçevede, ulusal ve uluslararası standartlar ve bilgi güvenliği kriterleri doğrultusunda kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren “Bilgi ve İletişim Güvenliği Rehberi” Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda hazırlanmış ve 24.07.2020 tarihinde onaylanmıştır.

9.2. Bilgi ve İletişim Güveliği Denetim Rehberi

Kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerin 27 Temmuz 2020’den itibaren 24 aylık

Şekil 18: Bilgi ve İletişim Güvenliği Rehberi[35].

bir uyum süresi içinde Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci'nin ve belirlenen güvenlik tedbirlerinin uyum önlemlerini yerine getirmesi beklenmektedir.

Rehber kapsamında kurum ve kuruluşlar tarafından yürütülen faaliyetlerin ve alınan tedbirlerin etkinliğini değerlendirmek amacıyla yılda en az bir kez denetime tabi tutulması gerekmektedir.

Denetçilere yol göstermesi amacıyla Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından denetim sürecinde uyulması gereken usul ve esasları içeren Bilgi ve İletişim Güvenliği Denetim Rehberi hazırlanmıştır.

Şekil 18: Bilgi ve İletişim Güvenliği Denetim Rehberi[36].

Denetim Rehberi'nin denetimin planlanması, yürütülmesi ve raporlanması süreçlerinde kurumlara ve denetçilere kılavuz olması hedeflenmiştir. Rehber; Denetim Çalışmalarına Hazırlık, Denetim Metodolojisinin Belirlenmesi ve Denetim Sonuçlarının Raporlanması şeklinde üç ana bölümden oluşmaktadır.

9.3. Denetim Çalışmalarına Hazırlık

BİG Rehberi kapsamında yer alan denetim faaliyetlerinin öncelikli olarak kurumların iç denetim birimlerinde görev alan ve bilgi teknolojileri alanında denetim tecrübesi olan iç denetçiler tarafından gerçekleştirilmesi esas alınmaktadır.

İç denetim birimi bulunmadığı ya da iç denetim ekibinin yeterli yetkinlikte olmadığı durumlarda ise kurum içi diğer personel, diğer kamu kurum ve kuruluşlarından görevlendirilecek personel ya da hizmet alımı yoluyla denetim gerçekleştirilebilecektir.

Kurumun hizmet alım yoluna gitmesi durumunda bu hizmetin, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda Türk Standartları Enstitüsü (TSE) ve TÜBİTAK BİLGEM işbirliği ile yürütülen "Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Sağlayan Personel ve Firma Belgelendirme" programı kapsamında yetkilendirilmiş firmalardan alınması gerekmektedir.

9.4. Bilgi ve İletişim Güvenliği Denetim Metodolojisi

Uyum denetiminde temel hedef Rehber Uygulama Sürecinin Etkinliğinin ve Varlık Gruplarına Uygulanan Tedbirlerin Etkinliğinin ölçülmesidir. Bu hedef doğrultusunda oluşturulacak denetim metodolojisi denetimin planlanması, denetim prosedürlerinin uygulanması ve denetim sonuçlarının raporlanması olmak üzere üç ana süreci içermektedir.

a) Denetimin planlanması; denetime ilişkin yol haritasının oluşturulması evresidir. Bu evrede denetim ekibinin belirlenmesi, kurumun anlaşılması, denetim kapsamının belirlenmesi ve denetim stratejisi ve denetim programının oluşturulması çalışmaları yürütülmektedir.

   Denetim ekibinin BİG Denetim Rehberinde belirtilen koşulları karşılaması gerekir. Ekip, Denetim Rehberi ekinde yer alan EK-A Denetim Ekibi Bilgisi formu ile kayıt altına alınmalıdır.

   Kurumların bilgi barındıran tüm varlıkları Rehber uyum sürecine dahil edilmiş ve varlık grupları altında toplanmış olmalıdır. Denetim kapsamı ise risk odaklı denetim yaklaşımı ve önemlilik kriterleri esas alınarak varlık grupları ana başlıkları ile ilişkili en az bir varlık grubunun dahil edilmesi ile oluşturulmalıdır. Belirlenen denetim kapsamı Denetim Rehberinde yer alan EK-B Varlık Grupları ve Denetim Kapsamı formu ile kayıt altına alınmalıdır.

Kurumun anlaşılmasının ve denetim kapsamının belirlenmesinin ardından etkinlik değerlendirmelerinin nasıl gerçekleştirileceğine yönelik denetim başlangıç ve bitiş tarihi, denetim ekibi, denetim sürecinde görüşülmesi planlanan kurum personeli bilgileri gibi unsurları içeren denetim stratejisi belirlenmelidir. Daha sonra denetimin ana hedefleri olan Rehber uygulama sürecinin ve varlık gruplarına uygulanan tedbirlerin etkinliğinin değerlendirilmesi amacıyla gerçekleştirilecek çalışmaları içeren denetim programı oluşturulmalıdır. Program, denetim ekibi tarafından Denetim Koordinatörü liderliğinde Denetim Rehberi EK-C'de yer alan Denetim Programı formu ile kayıt altına alınmalıdır.

b) Denetim Prosedürlerinin Uygulanması; denetim kapsamında yer alan varlık gruplarına yönelik güvenlik tedbirlerinin etkinliğinin değerlendirilme evresidir. BİG Rehberinde tedbirlere yönelik belirtilen denetim yöntem önerileri de referans alınarak denetim gerçekleştirilir. Denetçinin çalışmaları, kanıtları ve değerlendirmeleri Denetim Rehberi EK-D'de yer alan Çalışma Formu ile kayıt altına alınır.

   Rehber Uygulama Sürecinin Etkinliğinin değerlendirilmesi sürecinde Denetim Rehberi EK-E'de yer alan Rehber Uygulama Süreci Etkinlik Durumu Formundaki sorular ile gerçekleştirilerek kayıt altına alınır.

   Denetim kapsamında yer alan varlık gruplarına uygulanan güvenlik tedbirlerinin etkinliğinin değerlendirilmesinde Rehberde yer alan soru önerileri kullanılarak denetimler gerçekleştirilebilir. Varlık gruplarına uygulanan güvenlik tedbirlerinin etkinliğinin değerlendirilmesi sırasında varlıklara yönelik örneklem seçim yöntemi kullanılabilecektir. Denetçi denetim sonuçlarını Denetim Rehberi EK-F'de yer alan Tedbir Etkinlik Durumu tablosunda kayıt altına almalıdır.

   Denetimin tamamlanmasının ardından denetimde tespit edilen bulgulara ilişkin mutabakat sağlanması amacıyla denetim ekibi ve denetime katılan kurum personeli ve yöneticileriyle kapanış toplantısı yapılır ve sonuçlar tutanak ile kayıt altına alınır.

c) Denetim Raporunun Hazırlanması; denetim metodolojisine ve yapılan programa uygun olarak tamamlanan denetimin kurumun ilgili birimlerine süreç/denetim sonucu hakkında bilgilendirme yapılması amacıyla Denetim Rehberinde ana hatları çizilmiş olan raporun hazırlanma evresidir.

   Hazırlanan denetim raporunun her sayfası denetçiler tarafından güvenli elektronik imza ile imzalanarak nihai hâline getirilir ve belirlenen gizlilik derecesi gerekliliklerine uygun olarak kuruma teslim edilir.

Denetim Raporlarının Dijital Dönüşüm Ofisine Gönderilmesi

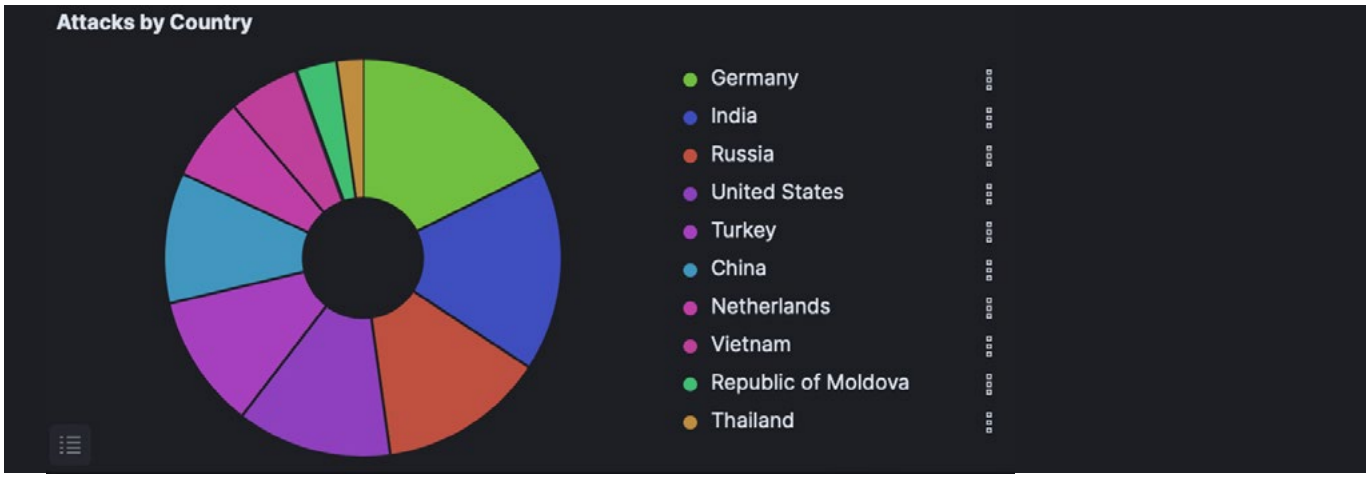
Denetim raporunun aşağıda yer verilen bölümleri denetim raporunun oluşturulma tarihinden itibaren en geç iki aylık süre içinde, 5070 sayılı Elektronik İmza Kanunu hükümlerine göre oluşturulan güvenli elektronik imza ile Üst Yönetici veya Üst Yöneticinin yetkilendirdiği personel tarafından imzalanarak DDO'ya iletilir[37].

- EK-A Denetim Ekibi Bilgisi
- EK-B Varlık Grupları ve Denetim Kapsamı
- EK-E Rehber Uygulama Süreci Etkinlik Durumu
- EK-F Tedbir Etkinlik Durumu
- EK-H Denetim Görüşü

HONEYPOT VERİLERİ

Bu rapor üç ay içinde Honeypot sensörlerimizden topladığımız verilerle oluşturulmuştur. En çok saldırı toplanan ülkeler, portlar, en çok denenen parolalar ve kullanıcı isimleri gibi veriler azalan sırada listelenerek inceleme için sunulmuştur.

Ekim, Kasım ve Aralık ayları boyunca Honeypot sensörlerimize toplam 3.777.008 saldırı gelmiştir.



Şekil 20: Gelen saldırıların ülkelere göre dağılımı.

Saldırın Geldiği Ülke	Saldırı Sayısı
Almanya	451.319
Hindistan	423.026
Rusya	345.961
ABD	322.576
Türkiye	278.855
Çin	271.227
Hollanda	174.696
Vietnam	145.992
Moldova	84.079
Tayland	57.000

Tablo 3: En çok saldırı gelen ülkeler ve saldırı sayıları.

Toplanan veriler incelendiğinde, en çok saldırı gelen ülkenin Almanya olduğu, sonrasında Hindistan, Rusya, ABD ve Türkiye'nin onu takip ettiği görülmektedir.

Saldırılan Port	Saldırı Sayısı
445 – SMB	1.315.205
23 – TELNET	295.649
5900 - VNC	287.506
3389 - RDP	280.152
25 - SMTP	208.830
22 - SSH	79.877
1433 – MSSQL	23.290
8080 - HTTP-ALT	16.885
7547 - tr069	8.195
5555 - MS-CRM	6.284

Tablo 4: En çok saldırı gelen portlar, bu portları kullanan servisler ve saldırı sayıları.

Yukarıdaki tablo incelendiğinde, en çok saldırının SMB servisinin kullandığı port 445'e geldiği görülmektedir. SMB servisi, sunucuların paylaşılan dosyalar ve yazıcılar için kullandığı servis olduğundan, bu servisin diğer

Denenen Parola	Denenme Sayısı
admin	9.085
123456	3.613
(boş)	2.599
nproc	2.111
password	1.916
12345	1.525
guest	1.134
1234	1.020
root	979
123	946

Tablo 5: SSH ve RDP honeypotlarımız üzerinde en çok denenen parolalar ve deneme sayıları.

servislere kıyasla çok daha fazla saldırı alması beklenen bir durum olarak değerlendirilmektedir. SMB'yi sırasıyla TELNET, VNC ve RDP servisleri takip etmektedir. Son iki en çok saldırı alan port bu çeyrekte de dikkat çekmektedir. "tr069" servisi, "CPE WAN Management Protocol (CWMP)" isimli protokolü 7547 portu üzerinden kullanan bir servistir. DEFCON22 etkinliğinde de sunulmuş olmak üzere internet ortamında bilinen exploitleri mevcuttur. "MS-CRM" servisi ise SoftEther VPN, HP OpenView, HP Data Protector, McAfee EndPoint Encryption Database Server, SAP gibi bilinen uygulamalarda kullanılmakla birlikte trojanların arka kapısı olarak kullanılabilen ve 5555 portu üzerinden kullanılan bir servistir. Bu iki porta gelen saldırıların sayılarının beklenenin çok üzerinde olması bu servislere yapılan saldırılarda bir artış olacağının göstergesi olabilir.

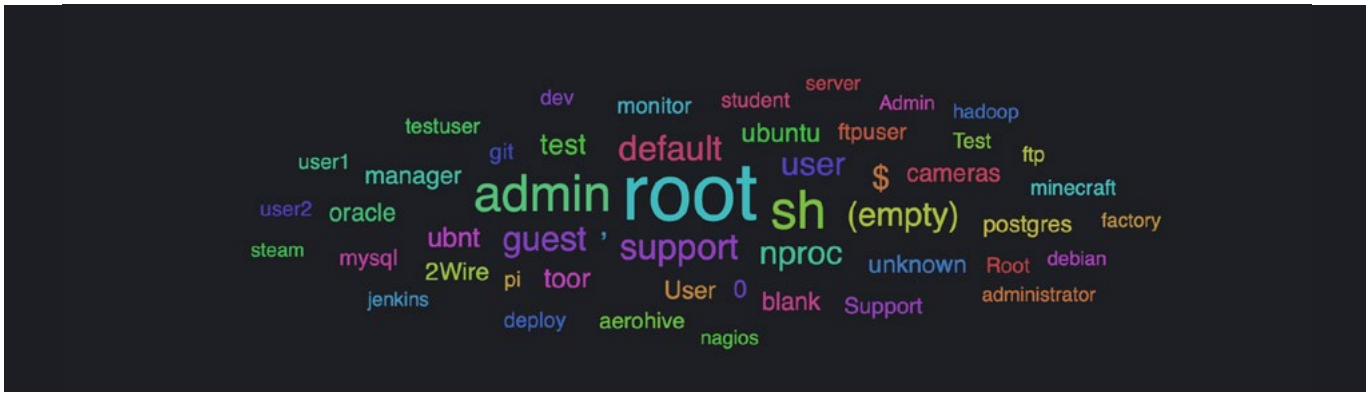
Denenen parolalar incelendiğinde, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan admin, root, password gibi kelimeler gözlemlenmektedir. Bu parolaların test süreci tamamlanır tamamlanmaz değiştirilmesi ve karmaşık, 12-16 karakterli, özel karakter içeren parolalarla değiştirilmesi analistlerimiz tarafından tavsiye edilmektedir. Ayrıca kolay hatırlanması ve girilmesi için herhangi bir harf, karakter içermeden sadece sıralı sayılar ile oluşturulmuş parolaları kullanmaktan kaçınılmalıdır.

Şekil 21: Parola etiket bulutu.

Denenen Kullanıcı Adı	Denenme Sayısı
root	37.179
sh	12.334
admin	10.151
support	3.039
guest	2.683
default	2.643
(boş)	2.090
nproc	2.053
user	2.045
$	1.792

Tablo 6: SSH ve RDP honeypotlarımız üzerinde en çok denenen kullanıcı adları ve deneme sayıları.

Denenen kullanıcı adları incelendiğinde, geçen çeyreğe oranla daha fazla deneme yapıldığı ilk olarak dikkat çekmektedir. Yeni kurulmuş olan sistemlerin sıklıkla kullandığı root, admin, user gibi kullanıcı adlarının saldırganlar tarafından tercih edildiği görülmektedir. Kurulumu tamamlanan servislerin ve yönetim panellerinin kullanıcı adlarının en kısa zamanda değiştirilmesi ve kurulan sistemlerin kendi isimlerinin kullanılmaması (örn. ubuntu, postgres, oracle, testuser) tavsiye edilmektedir.



Şekil 22: Kullanıcı adı etiket bulutu.

KAYNAKÇA

[1] S. Morgan, «Cybercrime To Cost The World $10.5 Trillion Annually By 2025,» [Çevrimiçi]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[2] D. Granger, «Karmen Ransomware Variant Introduced by Russian Hacker,» 2017. [Çevrimiçi]. Available: https://www.recordedfuture.com/karmen-ransomware-variant/.

[3] A. Hevner, «Design science in information systems research. MIS Quarterly,» 2004. [Çevrimiçi].

[4] J. Jian, Organized Cyber-Racketeering: Exploring the Role of Internet Technology in Organized Cybercrime Syndicates Using a Grounded Theory Approach, 2020.

[5] M. Goncharov, «Criminal hideouts for lease: Bulletproof hosting services. Forward- Looking Threat Research (FTR) Team, A TrendLabsSM Research Paper,» 2015.

[6] T. a. P. M. Smith, «Towards a Taxonomy for Classifying Knowledge on Ransomware as a Service (RaaS) Specializations,» %1 içinde *DESRIST 2022*, 2022.

[7] R. Broadhurst, Organizations and cybercrime, 2013.

[8] E. a. T. H. Leukfeldt, «Examining the social organization practices of cybercriminals in the Netherlands online and offline,» *International journal of offender therapy and comparative criminology,* pp. 522-538, 2020.

[9] «Combatting Cyber Attacks on the High Seas,» [Çevrimiçi]. Available: https://www.lockheedmartin.com/en-ca/features/dream-job-cyber.html. [Erişildi: 07 12 2022].

[10] «Maritime cyber security,» [Çevrimiçi]. Available: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html. [Erişildi: 07 12 2022].

[11] Deniz GÜLER, Ahmet YILDIZ, İzgi SAVAŞ,Feramuz AŞKIN, Yeni Deniz Güvenliği Ekosistemi Ve Doğu Akdeniz, TASAM, 2019, pp. 420-421.

[12] «MSC Confirms Malware Attack Caused Website Outage,» [Çevrimiçi]. Available: https://www.seatrade-maritime.com/containers/. [Erişildi: 07 12 2022].

[13] «Cyber Attack Targets Iranian Port near Strait of Hormuz,» [Çevrimiçi]. Available: https://www.jpost.com/breaking-news/cyberattack-targets-iranian-port-near-strait-of-hormuz-627616 . [Erişildi: 07 12 2022].

[14] «HMM Hit by Cyber Attack,» [Çevrimiçi]. Available: : https://www.offshore-energy.biz/hmm-hit-by-cyber-attack/. [Erişildi: 07 12 2022].

[15] «Compliance does not equal security or effective risk management,» [Çevrimiçi]. Available: https://www.rivieramm.com/news-content-hub/news-content-hub/compliance-does-not-equal-security-or-effective-risk-management-60830. [Erişildi: 07 12 2022].

[16] B. Ç. Soner ÇELİK, « GİRİŞ,» *GÜNCEL SİBER GÜVENLİK TEHDİTLERİ: FİDYE YAZILIMLAR,* p. 107, 2018.

[17] B. Security. [Çevrimiçi]. Available: https://www.bgasecurity.com/2021/11/ransomware-saldirilarini-nasil-tespit-edebilirsiniz/.

[18] Y. K., «FİDYE ZARARLISI (RANSOMWARE) ÇEŞİTLERİ, KORUNMA YOLLARI, GÜNCEL İSTATİSTİKLER VE FAYDALI BİLGİLER (2022),» 2022.

[19] T. Meskauskas, «Pcrisk,» 13 December 2022. [Çevrimiçi]. Available: https://www.pcrisk.com/removal-guides/25292-axlocker-ransomware.

[20] B. Toulas, «New ransomware encrypts files, then steals your Discord account,» 20 kasım 2022.

[21] T. Perrin ve M. Marlinspike, «The Double Ratchet Algorithm,» 20 11 2016. [Çevrimiçi]. Available: https://signal.org/docs/specifications/doubleratchet/.

[22] The Matrix.org Foundation CIC, «Matrix Specification,» 17 November 2022. [Çevrimiçi]. Available: https://spec.matrix.org/v1.5/.

[23] G. Hillenius, «German armed forces testing open source chat,» 16 01 2020. [Çevrimiçi]. Available: https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/matrix-pilot-bwmessenger.

[24] M. R. Albrecht, S. Celi, B. Dowling ve D. Jones, «Practically-exploitable Cryptographic Vulnerabilities in Matrix,» 2022.

[25] «ReMark,» [Çevrimiçi]. Available: https://remark.ae/hard-disk-shredding-data-wiping/. [Erişildi: December 2022].

[26] «blancco.hu,» [Çevrimiçi]. Available: https://blancco.hu/esettanulmany/az-adattorles-kezelese-a-vallalatoknal/. [Erişildi: 30 December 2022].

[27] U. G. A. Office, «https://www.gao.gov/,» 9 October 2018. [Çevrimiçi]. Available: https://www.gao.gov/products/gao-19-128. [Erişildi: 28 December 2022].

[28] O. o. t. U. S. o. D. F. A. a. Technology, «DEFENSE SCIENCE BOARD TASK FORCE ON DEFENSE SOFTWARE,» Department of Defense RESEARCH & ENGINEERING ENTERPRISE, Washington, D.C. 20301-3140, 2000.

[29] «The Hacker News,» 4 November 2022. [Çevrimiçi]. Available: https://thehackernews.com/2022/10/proxynotshell-new-proxyhell.html .

[30] S. Özeren ve H. C. Yücel, 8 November 2022. [Çevrimiçi]. Available: https://www.picussecurity.com/resource/blog/proxynotshellcve-2022-41040-and-cve-2022-41082-exploits-explained.

[31] F. Cosio, «Brierandthron.com,» 10 January 2022. [Çevrimiçi]. Available: https://www.brierandthorn.com/post/spot-the-difference-mitre-framework-vs-lockheed-martin-kill-chain-cyber-kill-chain.

[32] «Mitre Attack Navigator,» Mitre, [Çevrimiçi]. Available: https://mitre-attack.github.io/attack-navigator/. [Erişildi: 2022 December 30].

[33] C. Peacock, «Summiting the Phramid of Pain,» CSNP, 18 July 2022. [Çevrimiçi]. Available: https://www.csnp.org/post/summiting-the-pyramid-of-pain. [Erişildi: 30 December 2022].

[34] Netsurion, «Threat Intelligence and The Pyramid of Pain,» Netsurşon, [Çevrimiçi]. Available: https://www.netsurion.com/articles/the-pyramid-of-pain. [Erişildi: 30 December 2022].

[35] T. C. C. D. D. Ofisi, «Türkiye Cumhuriyeri Cumhurbaşkanlığı Dijital Dönüşüm Ofisi,» Temmuz 2020. [Çevrimiçi]. Available: https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf.

[36] T. C. D. D. Ofisi, «Cumhurbaşkanlığı Dijital Dönüşüm Ofisi,» Ekim 2021. [Çevrimiçi]. Available: https://cbddo.gov.tr/SharedFolderServer/Projeler/File/BG_Denetim_Rehberi.pdf.

[37] C. D. D. Ofisi, «Bilgi ve İletişim Güvenliği Denetim Rehberi,» [Çevrimiçi]. Available: https://cbddo.gov.tr/SharedFolderServer/Projeler/File/BG_Denetim_Rehberi.pdf.

[38] D. GOODIN, «Researchers devise iPhone malware that runs even when device is turned off,» 2022.

[39] J. Classen, R. Reith, A. Heinrich ve M. Hollick, «Evil Never Sleeps:When Wireless Malware Stays On After Turning Off iPhones,» Mayıs 2022.

[40] A. Support, «Use Low Power Mode to save battery life on your iPhone or iPad».

[41] J. Han, A. J. Chung, P. Tague, «PitchIn: eavesdropping via intelligible speech reconstruction using non-acoustic sensor fusion,» %1 içinde *Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks*, 2017.

[42] L.Zhang,P.H.Pathak,M.Wu,Y.Zhao,P.Mohapatr, «Accelword: Energy efficient hotword detection through accelerometer,» %1 içinde *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, 2015.

[43] S.A.Anand, N.Saxena, «Speechless:Analyzingthethreattospeech privacy from smartphone motion sensors,» %1 içinde *2018 IEEE Symposium on Security and Privacy*, 2018.

[44] Y. Michalevsky, D. Boneh, G. Nakibly, «Gyrophone: Recognizing speech from gyroscope signals,» %1 içinde *23rd USENIX Security Symposium*, 2014.

[45] Z.Ba,T.Zheng,X.Zhang,Z.Qin,B.Li,X.Liu,K.Ren, «Learning- based practical smartphone eavesdropping with built-in accelerometer,» %1 içinde *NDSS*, 2020.

[46] Fortinet, «https://www.fortinet.com/blog/threat-research/analysis-of-follina-zero-day,» [Çevrimiçi].

[47] Microsoft, «https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/,» [Çevrimiçi].

[48] NIST, National Vulnerability Database, «https://nvd.nist.gov/vuln/detail/CVE-2022-30190,» [Çevrimiçi].

[49] Bleeping Computer, https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2022-patch-tuesday-fixes-1-zero-day-55-flaws/.

[50] L. a. V. R. Jeffery, «Why ransomware attacks are on the rise — and what can be done to stop them,» 2021. [Çevrimiçi]. Available: https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them.

[51] B. M. M. a. S. S. Al-rimy, «Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security,,» 2018. [Çevrimiçi].

[52] H. a. N. A. R. Puat, «Ransomware as a service and public awareness. PalArch's Journal of Archaeology of Egypt/Egyptology,» 2020. [Çevrimiçi].

[53] M. Simmonds, «How businesses can navigate the growing tide of ransomware attacks. Computer Fraud & Security,» 2017. [Çevrimiçi].

[54] 16 November 2022. [Çevrimiçi]. Available: https://www.zerodayinitiative.com/blog/2022/11/14/control-your-types-or-get-pwned-remote-code-execution-in-exchange-powershell-backend.

[55] [Çevrimiçi]. Available: https://www.pcrisk.com/removal-guides/25292-axlocker-ransomware.

[56] «Crowd Strike,» 23 March 2017. [Çevrimiçi]. Available: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf.

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech