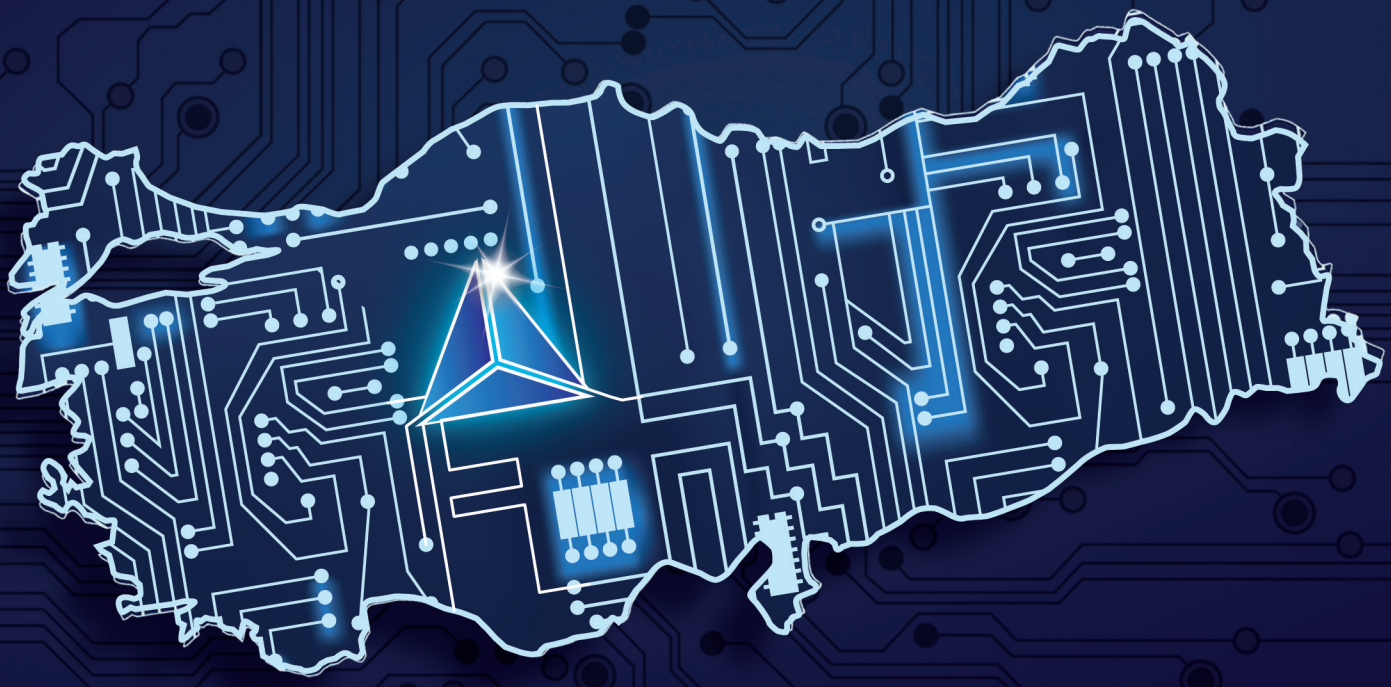
2018 OCAK-MART DÖNEMİ SİBER TEHDİT DURUM RAPORU



STM
MÜHENDİSLİK
TEKNOLOJİ
DANIŞMANLIK

İÇİNDEKİLER

SORUMSUZLUK VE FİKRİ MÜLKİYET HAKKI BEYANI

İşbu eserde/internet sitesinde yer alan veriler/bilgiler ticari amaçlı olmayıp tamamen kamuyu bilgilendirmek amacıyla yayımlanan içeriklerdir. Bu eser/internet sitesinde bulunan veriler/bilgiler tavsiye, reklam ya da iş geliştirme amacına yönelik değildir. STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. işbu eserde/internet sitesinde sunulan verilerin/bilgilerin içeriği, güncelliği ya da doğruluğu konusunda herhangi bir taahhüde girmemekte, kullanıcı veya üçüncü kişilerin bu eserde/internet sitesinde yer alan verilere/bilgilere dayanarak gerçekleştirecekleri eylemlerden ötürü sorumluluk kabul etmemektedir.

Bu eserde/internet sitesinde yer alan bilgilerin her türlü hakkı STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.'ye ve/veya eserde atıf yapılan kişi ve kurumlara aittir. Yazılı izin olmaksızın eserde/internet sitesinde yer alan bilgi, yazı, ifadenin bir kısmı veya tamamı, herhangi bir ortamda hiçbir şekilde yayımlanamaz, çoğaltılamaz, işlenemez.

Giriş

20 Ocak 2018'de Türk Silahlı Kuvvetleri (TSK) tarafından başlatılan "Zeytin Dalı Harekâtı" kapsamında terör örgütleri ile sıcak savaş bağlamında devam eden muharebelerde, TSK'nın sahip olduğu üstünlüğün sabote edilmesi ve algı yanılgısı oluşturulması maksatları ile terör örgütleri ve sempatizanlarının harbin beşinci boyutu olarak nitelendirilen siber savaş yöntemlerini kullanmaya başladıkları tespit edilmiştir. Bu kapsamda sahte haberler üretme, olayları saptırma ve kamu kurumlarına ait olan web sitelerine saldırı gerçekleştirme gibi faaliyetlerde bulunan söz konusu unsurların, bu faaliyetleri algı yönetimi ve kitleleri tahrik etme maksatlarında gerçekleştirdikleri değerlendirilmektedir.

8 Mart 2018 tarihinde, Kuzey Kore orijinli bir grup olarak bilinen "Lazarus Grup" (diğer adı ile "Hidden Cobra") isimli "Siber Suç Örgütü"nün ülkemiz finans sistemine yönelik gerçekleştirmiş olduğu iddia edilen saldırılar tespit edilmiştir. Saldırılarda, grubun en son 2017 yılında görülen "Bankshot" zararlı yazılımının geliştirilmiş bir sürümü ile geri dönüş yaptığı görülmektedir. Bankshot, daha fazla bilgi elde etmek için kurbanın ağına yerleşmek üzere özel olarak tasarlanmış bir zararlı yazılım. Elde edilen veriler, saldırganların bilgi toplamak için bahse konu zararlı yazılımı kullanarak ülkemiz finans sistemlerine yönelik, hedef odaklı bir operasyon planlayabileceği ihtimalini güçlendirmektedir.

Ülkemize yönelik bu ciddi saldırılarla ilgili olarak STM Siber Tehdit İstihbarat Merkezi tarafından gerçekleştirilen analizlerimizin özetlerini raporumuzda bulabilirsiniz.

2017 Ekim-Aralık dönemi raporumuzun 2018 yılı siber tehdit beklentileri başlığı altında yer verdiğimiz hususlardan birisi IoT cihazlarının kullanıldığı Botnet saldırıları olmuştu. 2018 Mart ayında yayımlanan bir raporda[1] Nesnelerin İnterneti (IoT) saldırılarının 2017 yılında, 2016 yılına nazaran %600 arttığı vurgulanırken Çin'in %21 ile birinci, ABD'nin %10,6 ile ikinci, Brezilya'nın da %6,9 ile üçüncü sırada yer aldığı IoT saldırılarına kaynak teşkil eden ülkeler arasında ülkemizin %4,1 ile yedinci sırada yer aldığı belirtiliyor. Bu tehdidin, IoT cihazlarının güvenlikleri tam olarak sağlanmadıkça gündemde kalacağını değerlendiriyoruz. Bununla birlikte saldırganların son dönemde DDos saldırıları için IoT Botnet'lerden çok daha etkin bir yöntem kullandıklarına şahit oluyoruz. Bu saldırı yönteminde, web uygulamalarını ve sitelerini hızlandırmak için tasarlanan ve güvenli olmayan Memcached sunucuları kullanılıyor. Memcached sunucuların zafiyetinden yararlanılan saldırılarla ilgili haberimizi raporumuzda bulabilirsiniz.

2018 yılı için vurguladığımız hususlardan bir diğeri olan kripto para madenciliği de kripto para birimlerindeki değer kayıplarına rağmen gündemdeki yerini koruyor. Kripto para madenciliği güçlü işlemciler ve grafik kartları gerektiriyor ve işlemler oldukça fazla enerji sarfına yol açıyor. Aslında yasa dışı bir faaliyet olmayan kripto para madenciliği, saldırganların değişik yöntemlerle virüs bulaştırdıkları kişisel/kurumsal bilgisayarları veya IoT cihazlarını kullanıcılarının bilgisi dışında ve kendi amaçları doğrultusunda kripto para madenciliğinde kullanmasıyla birlikte sorun olabiliyor. Son dönemde, YouTube üzerindeki reklamların bu tür virüsleri yaymak maksadıyla kullanılması, ilgi çekici bir yöntem olarak gündeme gelmektedir.

2018 Ocak ayı istatistikleri siber saldırıların ardındaki motivasyonun %81,7'sini siber suçların oluşturduğuna işaret ediyor[2]. Ayrıca, siber suçların ekonomik etkisi ile ilgili raporda siber suçların günümüz itibarıyla gelmiş olduğu noktayı özetleyen bilgiler içeriyor[3].

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[2] https://www.hackmageddon.com/2018/02/22/january-2018-cyber-attacks-statistics/

[3] https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=b-b9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-

Rapora göre;

• Siber suçların küresel ekonomiye maliyeti 2014'te yapılan araştırmada 445 milyar ABD Doları iken geçtiğimiz yıl itibarı ile 600 milyar ABD Dolarına yaklaşmış durumda.

• Mülkiyet hakları ve mahrem iş bilgilerinin çalınmasına yönelik suçların siber suçların sebep olduğu maliyetin tüm siber suçların maliyeti içindeki payı en az %25 ve bu hırsızlık askeri teknolojiye ait ise milli güvenliği de tehdit ediyor.

• Bankalar siber suçluların en gözde hedefleri.

• Rusya, Kuzey Kore ve İran finansal kurumlara saldırılarda, Çin ise siber casusluk alanında en aktif ülkeler. Siber suçlarda Rusya ilk sırada Kuzey Kore ikinci sırada yer alıyor.

• Fidye yazılımları 6 bini aşkın çevrimiçi pazar ve hizmeti olarak sunulabilir hale geldiğinden en hızlı büyüyen siber suç aracı.

• İstismar araçları, sipariş usulü zararlı yazılımlar ve kiralık Botnet'ler gibi çok çeşitli araç ve servisler sunan ve büyüyen pazarlarıyla hizmet olarak sunulabilir hale gelen siber suç, gittikçe daha karmaşık bir hale gelmiş durumda.

• Tor ve Bitcoin gibi kripto para birimlerinin anonim olmaları, suç aktörlerinin tanımlanmalarını zorlaştırıyor.

2018 Şubat ayında yayımlanan bir diğer araştırma raporunda[4] ise siber güvenlik olaylarının üçte birden fazlasının oltalama e-postaları veya kurum çalışanlarına gönderilen zararlı yazılım içeren e-posta eklentileri ile başladığını ortaya koyuyor. Bu da araştırma çerçevesinde e-posta kutularının siber güvenlik alanında en zayıf halkayı oluşturması anlamına geliyor. Aslında siber saldırılarda, yaklaşık %21 ile kurumların internet bağlantılı hizmetlerindeki zafiyetlerin istismarı ilk sırada yer alıyor, ancak %18'lik zararlı e-posta eklentileri ve %16 oltalama saldırıları toplamda %34 ile kurumlar için e-posta kaynaklı saldırıların daha büyük bir tehdit oluşturduğunu gösteriyor. Listedeki diğer saldırı tipleri %20 ile iç tehditler, %9 ile kaba kuvvet (brute force) saldırıları olarak belirtiliyor.

Yakın zamandaki gelişmeler, yapay zekâ uygulamalarının zafiyetleri daha etkin tespit ve istismar etme, tespitten kaçınma, operasyonel faaliyetlere destek olma, saldırılara karşı hızlı tepki verebilme gibi alanlarda kullanılabileceğini hatta kullanıldığını gösteriyor. Bu dönem raporumuzda inceleme konusu olarak yapay zekânın siber güvenlikte her geçen gün artan rolünü ele aldık. Makalemizi "Dönem İnceleme Konusu" başlığı altında raporumuzun sonunda bulabilirsiniz.

[4] https://www.helpnetsecurity.com/2018/02/23/weakest-link-security-perimeters/

Siber Tehdit İstihbaratı

Zeytin Dalı Harekâtı ve Terör Kaynaklı Tepkisel Siber Saldırı Analizi

Teknolojik ürünlerin kullanımı yaygınlaştıkça siber güvenlik kavramının önemi ve etkisi küresel çapta artış göstermiş ve bu gelişme sonucunda harbin beşinci boyutu olarak nitelendirilen siber savaş kavramı oluşmuştur. Siber savaşı klasik savaştan ayıran en önemli faktörler:

- İnsan kayıp oranının az olması,
- Yatırım maliyetinin daha düşük olması,
- Oluşturulan silahların birçok hedefe karşı geniş zaman aralığında defalarca kullanılabilmesi,
- Stratejik ve politik olayları etkileyebilmesi,
- Saldırıların maskelenebilmesi,
- Tek taraflı saldırı yapılabilmesi.

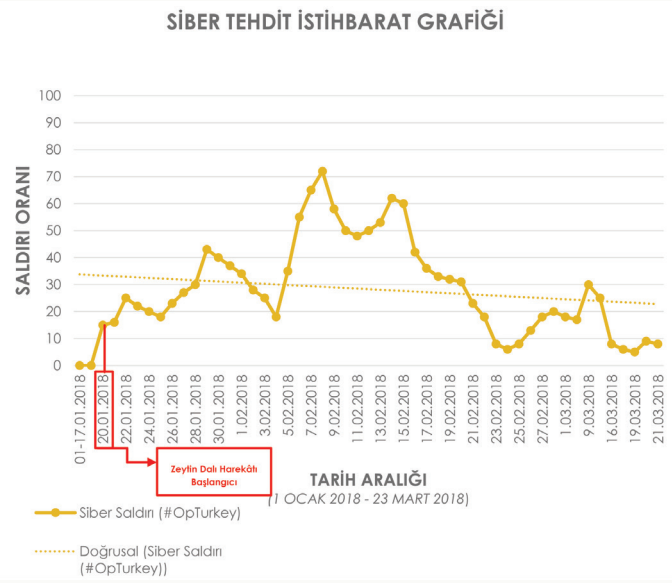
Bahsi geçen bu avantajlar doğrultusunda sürekli ön plana çıkan siber savaş yöntemleri hem askeri hem de sivil kullanıma açık olabildiğinden dolayı bu yöntemleri bilen kişi sayısı azımsanamayacak kadar fazladır. Siber güvenlik ve siber savaş kavramlarında bilgi ve tecrübe edinen kişiler bu yeteneklerini eğitim, profesyonellik, meslek, hobi, merak, illegal ve terör gibi konuların altında kullanabilmektedir.

Dünya genelinde eğitim, hobi, profesyonel hizmet, illegal ve terör amaçlı hareket eden birçok kişi ve grubun varlığı bilinmektedir. Bu grupların kendi motivasyon ve amaçları doğrultusunda hareket ettikleri sürekli olarak basına yansımaktadır. Bu özet, terör amaçlı ve/veya terör motivasyonlu kişi ve grupların gerçekleştirdikleri siber saldırıları Türkiye bazında ele almaktadır.

TSK, 20 Ocak 2018'de başlatmış olduğu Zeytin Dalı Harekâtı sonrasında terör bağlantılı ve/veya motivasyonlu saldırgan gruplar tarafından #OpTurkey etiketi ile ülkemizdeki kamu kurum ve kuruluşlarına siber saldırılar düzenlenmeye başlandığı tespit edilmiştir. Bu saldırıların en temelinde harekât süresince zemin kaybeden terör örgütlerinin; TSK'nın sahip olduğu üstünlüğü sabote etme, kitleleri tahrik etme ve algı yanılması oluşturma amaçlarının olduğu değerlendirilmektedir. #OpTurkey ile başlatılan saldırılarda ağırlıklı olarak sahte haber üretme, propaganda yapma ve kamu kurum ve kuruluşlarına siber saldırı gerçekleştirme faaliyetleri yürütülmektedir.

Gerçekleştirilen siber saldırılarda DDoS[5], Defacement[6], Exploitation[7] ve Spear Phishing[8] yöntemleri tercih ediliyor. İncelenen saldırı sonuçlarında, paylaşılan mesaj ve propaganda cümlelerinin terör örgütlerinin mesaj ve paylaşımları ile birebir örtüştüğü tespit edilmekte ve bu da saldırıların tamamının Zeytin Dalı Harekâtı'na tepki olarak yapıldığı tezini kuvvetlendirmektedir. Bu süreçte saldırıları gerçekleştiren gruplara ek olarak sosyal medyada da saldırı sonuçlarının ve propaganda mesajlarının paylaşılmasını sağlayan birçok aktör tespit edilmiştir. Buna bağlı olarak söz konusu unsurların sosyal medyayı haber ve ifşa ortamı olarak kullandıklarına şahit olunmaktadır.

Tespit edilen saldırıların 1 Ocak - 23 Mart 2018 tarihleri arasında çizmiş olduğu grafikte saldırıların Zeytin Dalı Harekâtı ile senkronize gerçekleştiği net bir şekilde görülmektedir (Şekil 1).



Şekil 1: Siber Tehdit İstihbarat Grafiği

[5] DDoS: Hedef siteye cevap veremeyeceği kadar istek gönderiminde bulunarak sistemi hizmet dışı bırakmak.
[6] Defacement: Hedef sitenin ana sayfasını değiştirmek veya ana sayfa düzenini bozarak mesaj bırakmak.
[7] Exploitation: Hedef sitenin kurulu olduğu sistem üzerindeki açıklığı sömürerek sistemde hak sahibi olmak.
[8] Spear Phishing: Hedef sitenin personeline veya potansiyel kullanıcılarına yönelik aldatma yöntemi ile hassas bilgi elde etmeye çalışmak.

Şekil 1'de görüldüğü üzere Zeytin Dalı Harekâtı'nın başlangıç tarihi ile saldırıların arttığı gözlenmiştir. Saldırı aktörlerinin birden fazla olduğu önceden tespit edildiğinden, saldırı yükünün sabit olmayışı normal bir durum olarak değerlendirilmiş ve saldırı sürecinde oluşan kırılma noktalarına rağmen saldırı sürekliliğinin sabit bir şekilde ilerlediği tespit edilmiştir.

Hidden Cobra Grubu'ndan (LAZARUS) Siber Saldırı Analizi

8 Mart 2018 tarihinde tespit edilen ve "Hidden Cobra Targets Turkish Financial Sector With New Bankshot Implant" başlığı ile yabancı kaynaklarda yer alan, "Türkiye Finans Sektörüne Yönelik Siber Saldırı" başlığı ile de Türk basınında yer alan "Siber Saldırı" iddialarına ilişkin STM Siber Tehdit İstihbarat Merkezi'nde analiz çalışmaları yapıldı.

Kuzey Kore orijinli bir grup olarak bilinen "Lazarus Grup" (diğer adı ile "Hidden Cobra") isimli "Siber Suç Örgütü"nün gerçekleştirmiş olduğu iddia edilen[9] saldırılarda "Bankshot" zararlı yazılımının (malware) bir varyantını kullandığı tahmin edilmektedir. Kullanılan zararlı yazılımının kod benzerliği, hedef alınan sektör (finans sektörü) ve kontrol sunucularının (Botnet veya komuta kontrol) varlığı nedeniyle bu saldırı, küresel finans ağı "SWIFT"e [10] karşı yürütülen "Hidden Cobra"nın önceki saldırıları ile benzerlik göstermektedir.

Ülkemiz finans sistemine yönelik bu saldırıda, en son 2017 yılında görülen "Bankshot" zararlı yazılımının başka bir varyantı ile geri dönüş yaptığı görülmektedir. Bankshot, daha fazla bilgi elde etmek için kurbanın ağına yerleşmek üzere tasarlanmıştır. Çıktılar, bu operasyonun belirli finansal kuruluşlara hedef odaklı planlandığı ihtimalini güçlendirmektedir.

Hedef Odaklı Tehdit (Advanced Persistent Threat) saldırı türünü kullanan grubun izlediği metodoloji ve kullandığı yöntemler ise APT28 (Fancy Bear) ve Snake (Turla veya Uruburos) isimli "Siber Suç Örgütleri" ile benzerlik göstermektedir.

Ülkemizdeki finans kuruluşları, zararlı içerik barındıran bir Microsoft Word belgesini içeren oltalama (spear phishing) yöntemi ile hedeflenmiştir. Bu hedefleme yakın zamanda duyurulmuş olan gömülü bir Adobe Flash istismarını içermektedir. Saldırgan, temelde CVE-2018-4878 zafiyetini istismar etmektedir.

Yukarıda anılan siber casusluk grubuna ait "aktivite sıklıkları", "saldırı yüzeyleri", "saldırı geçmişleri", "saldırılarda kullanılan atak vektörleri" ve bu saldırılara karşı alınacak önlemler ile ilgili analiz aşağıda detaylandırılmıştır.

2014 yılında Amerika'da bulunan "Sony Pictures Entertainment"a yönelik düzenlenen siber casusluk ve 2017 Şubat yılında başlayan WannaCry saldırılarının ilk döneminde "Destover" isimli zararlı bir yazılım kullanıldı. Destover isimli zararlı yazılımının kullanıldığı başka bir saldırı ise Güney Kore Üniversitesi öğrencileri tarafından kurulan "MOFA Dostları" (Dışişleri Bakanlığı Dostu Öğrenciler) grubuna yönelik saldırı idi. Bu saldırılar 2017 yılının sonunda Kuzey Kore Devlet Başkanı "Kim Jong Un"un Kuzey Kore-Güney Kore diyaloğunun geliştirilmesi konuşmasını yaptığı güne kadar, Güney Kore'de işlem gören Kriptopara Değişim Platformlarına (Cryptocurrency Exchange Platform) yönelik saldırılar ile devam etti.

Grubun gerçekleştirdiği tahmin edilen saldırılar aşağıda sıralanmıştır (Tablo 1):

HIDDEN COBRA (LAZARUS) Tarafından Gerçekleştirilen Saldırılar	
1	North Korea Targeted South Korean CrytpoCurrency Users and Exchange in Late 2017 Campaign [5]
2	US Government Publicly Blames North Korea for WannaCry [6]
3	DHS and FBI release Alerts for North Korean-Linked Malware "FALLCHILL" and "VOLGMER"[7]
4	North Korea's DDoS BotNet Infrastructure [8]
5	Lazarus Group linked to attacks on financial organizations in 31 countries.[9]
6	Official Suspects North Korean Connections to Wcrypt attacks.[10]
7	US-CERT assesses Lazarus Group and Guardians of Peace activities as part of HIDDEN COBRA

Tablo 1: Siber Saldırı Grubunun Gerçekleştirdiği Saldırılar

[9] https://securingtomorrow.mcafee.com/mcafee-labs/hidden-cobra-targets-turkish-financial-sector-new-bankshot-implant/

[10] https://securingtomorrow.mcafee.com/mcafee-labs/attacks-swift-banking-system-benefit-insider-knowledge

Hareket kabiliyeti ve saldırı oranı yüksek olan "Hidden Cobra" saldırı grubunun 2017 Aralık ayından bu yana aktif olduğu anlaşılmaktadır. Grubun "Tehdit Aktörü" kartında ise 2013 yılında faal olmaya başladıkları ve son saldırılarını ülkemize yönelik gerçekleştirdikleri bilgisi yer almaktadır.

Yeraltı forum üyeleri kategorisinde değerlendirilen grubun, motivasyon unsuru "finansal" olarak nitelendirilmiştir. Bankalar, kripto para borsaları ve ticari amaçlı zarar verme (Sony Entertainment gibi) hedefli saldırı ve sızma faaliyeti yaptıkları bilinmektedir. Grubun Kuzey Kore Devleti tarafından desteklenen "Devlet Destekli Siber Casusluk Grubu" olduğu tahmin edilmektedir.

Grubun zararlı yazılım geliştirme yeteneğinin ve yeterliliğinin olduğu bilinmektedir. Grup tarafından geliştirildiği değerlendirilen FALLCHILL olarak bilinen zararlı yazılım, bir uzaktan yönetim aracı (RAT) ile bağlantı kurmakta ve son kullanıcıyı komuta ve kontrol sunucusuna bağlamaktadır.

Hidden Cobra, 2016 yılından bu yana havacılık, telekomünikasyon ve finans sektörlerini hedeflemek için FALLCHILL kötü amaçlı yazılımını kullanmaktadır. Bahse konu kötü amaçlı yazılım, saldırganların bir komuta ve kontrol sunucusundan kurban sistemine Proxy üzerinden yayımlayabildikleri çoklu komutlara sahip tam işlevsel bir Uzaktan Erişim Solucanı'dır (RAT).

STM Siber Tehdit İstihbarat Merkezi tarafından kullanılan MISP platformu ile Hidden Cobra'ya ilişkin yapılmış olan tehdit korelasyon grafiği aşağıda sunulmuştur (Şekil 2):

Bu saldırıya ilişkin en net husus, olayın 2 ve 3 Mart 2018'de meydana geldiğini göstermektedir. İmplant şimdiye kadar başka bir sektörde veya ülkede ortaya çıkmadı. Bu saldırı, saldırganların bilgi toplamak için Bankshot zararlısı kullanarak finans sistemlerine yönelik gelecekte bir soygun planlayabileceğini göstermektedir.

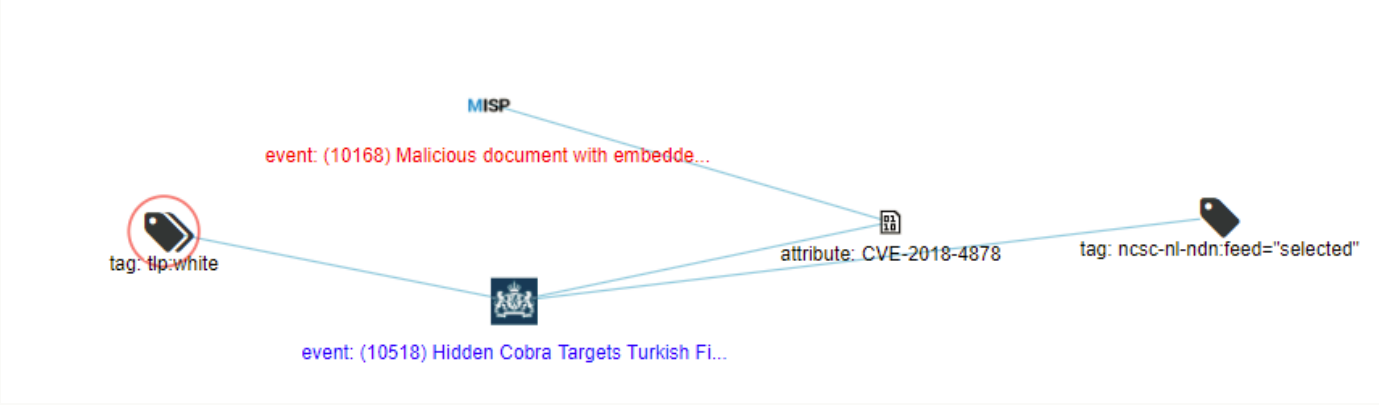
Orijinal Alan Adı: falconcoin.io

Zararlı Alan Adı: falcancoin.io

Kötü amaçlı bir alan adı olan falcancoin.io, 27 Aralık 2017 tarihinde satın alınmıştır. 19 Şubat'ta, kodların görünmeye başlamasından sadece birkaç gün önce güncellenmiştir. Bu kodlar, bir kurbanın sistemine bir saldırganın tam erişim sağlaması için kullanılan bir uzaktan erişim aracı olan Bankshot'ın daha önceki biçimlerinin varyasyonlarıdır.

Hedef Odaklı Saldırı (APT) tehdit vektörleri, Hidden Cobra grubunun gerçekleştirdiği saldırı örneğindeki gibi son kullanıcıları hedef almaktadır. Temelde son kullanıcıyı aldatan bir e-posta ile başlayan saldırılar finans sektöründe kapanması zor olan yaralar açmaya kadar gidebilmektedir.

Kurum ve kuruluşların, her bir son kullanıcı için bilgi güvenliği farkındalığı seviyesini arttıracak eğitimler ve çalışmalar yapması gerekmektedir.



Şekil 2: MISP, Hidden Cobra Korelasyon Grafiği

Almanya Kamu Kurumlarına Yönelik Gerçekleştirilen Siber Saldırı Analizi

27 Şubat 2018 tarihinde başlayan ve Almanya kamu kurumlarına yönelik gerçekleştirilen organize siber saldırılar için birden fazla saldırgan grubun ismi geçmektedir. Rusya merkezli "Sofacy" ve "Fancy Bear" olarak da bilinen "APT28" ile Turla ve Uruburos olarak da bilinen "Snake" gruplarının saldırıları gerçekleştirmiş olabileceği değerlendirilmektedir.

Benzer şekilde aynı grubun "APT28 (Fancy Bear)" 2015 yılında Federal Alman Meclisi'ne yönelik siber saldırılar gerçekleştirdiği bilinmektedir. Grubun kamu kurumları, havacılık, savunma, enerji ve medya sektörlerini hedef aldığı bilinmektedir (Tablo 2). Saldırılardan sorumlu tutulan bir diğer grup ise 2005 yılından beri aktif olarak faaliyet gösteren Turla ve Uruburos olarak da bilinen "Snake" isimli gruptur. Snake'in kamu kurumlarını özellikle de büyükelçilik, askeri kurum, araştırma ve eğitim örgütlerini ve ilaç endüstrisini hedef aldığı bilinmektedir.

yönelik gerekli önlem ve tedbirlerin alınması, son kullanıcıların bilgi güvenliği farkındalığı düzeyinin arttırılması siber istihbarata karşı koyma kapsamında büyük önem arz etmektedir.

APT28;

- 2007 yılından beri aktif olduğu bilinen bir gruptur. Grup kendisini askeri veya kamu kurumları birimlerini hedef alan bir organizasyon olarak tanımlamıştır.
- Aynı zamanda "Sofacy", "Fancy Bear", "Sednit", "Pawn Storm", "TsarTEam", "Swallowtail" ve "Strontium" isimleri ile de anılmaktadır.
- Birçok araştırmacı ve güvenlik uzmanı tarafından araştırılmaktadır. Kamuoyunda bu grubu popüler yapılan saldırılar; Alman Bundestag[11], Fransız kanalı TV5 Monde istasyonu[12] ve 2016 yılında DNC[13]'ye yönelik yapılan saldırılardır.

Son dönem aktivite sıklığı incelendiğinde 28 Şubat ve 1 Mart 2018 tarihlerinde aktivite sıklığının arttığı

Operasyon 1	Operasyon 2	Operasyon 3	Operasyon 4	Operasyon 5	Operasyon 6
DollRussian	Bundestag	TV5 Monde Cyber Attack	EFF Attack	DNC Hack	OpOlympics

Tablo 2: APT28 (Fancy Bear)'in gerçekleştirdiği saldırılar

Yukarıda anılan siber casusluk gruplarının aktivite sıklıkları, saldırı yüzeyleri, saldırı geçmişleri, saldırılarda kullandıkları atak vektörleri ve bu saldırılara karşı alınacak önlemler ile ilgili detaylı analize dayanan bilgiler ışığında;

- Kamu kurumlarına,
- Savunma sektörüne,
- Enerji sektörüne,
- Havacılık sektörüne,
- Eğitim kurumlarına,
- İlaç endüstrisine,
- Medya sektörüne

görülen grubun motivasyonu, saldırı esnasında kullandıkları stratejiler göz önüne alınarak değerlendirilmiştir. Buna göre;

- Grup Rusya ile alakalı olabilecek gizli jeopolitik bilgiye olan ilgisi ile biliniyor. Bu nedenle siber istihbarata karşı koyma kapsamında; kamu kurumları, havacılık, savunma, enerji ve medya sektörünü hedef aldıkları bilinmektedir.
- Grubun topladığı bilgiler ile ilgili finansal bir gelir elde etmek için herhangi bir çabası olduğuna dair bir delil elde edilememiştir. Tehdit vektörü olarak gördüğü hedef/ hedefler üzerinde kalıcı hale gelerek hedefin rutinlerine, sırlarına ve değerli bilgilerine yönelik faaliyet yürütmektedir.

[11] https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigate-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag
[12] https://blog.trendmicro.com/tv5-monde-russia-and-the-cybercaliphate/
[13] https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

• Hareket vektörü değerlendirildiğinde; grubun siyasi kararlar, kamuoyu ya da coğrafi konuları etkilemek için kullanılabilecek stratejik devlet bilgilerini toplamak için faaliyet yürütüldüğü değerlendirilmektedir.

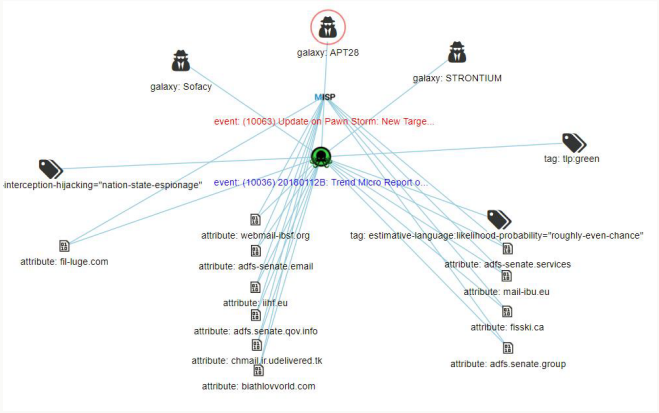
APT28'in Microsoft Windows, Linux ve Apple işletim sistemlerine yönelik zararlı geliştirme yetenekleri olduğu da bilinmektedir. Ayrıca zararlı yazılımları kapalı devre ağlara yönelik olarak USB Sürücü yoluyla hedefleme yeteneğine sahiptirler.

Windows işletim sistemlerine yönelik olan araçları çoğunlukla arka kapı ve bilgi toplayıcılardır (Backdoor and Information Gathering Tools). Bu zararlıların yetenekleri arasında tuş vuruş kaydetme yeteneği (keylogger) ile cihazları Botnet komuta kontrol sunucularına bağlamak gösterilebilir.

APT28 tarafından geliştirilen ve kullanılan zararlı yazılımlar (APT28'e ait olduğu bilinen zararlı yazılımlar);

[*] OLDBAIT	[*] CHOPSTICK
[*] XAgen	[*] Winexe,
[*] WinIDS	[*] Fooze
[*] Komplex	[*] DealersChoice
[*] USBStealer	[*] Sedkit
[*] Sofacy	[*] CORESHELL
[*] XTunnel	[*] SOURFACE
[*] DownRange	[*] Sedreco Dropper
[*] Downdelph	[*] Sednit
[*] HideDrv (Rootkit)	[*] Grizzly Steppe

MISP Computer Incident Response Center'dan alınan "İstihbarat Raporu"na göre ise grubun oltalama amaçlı kullanılacak olan domain'leri bitcoin ile satın aldığı tespit edilmiştir.



Şekil 3: MISP CIRC Tehdit Modelleme

Şekil 3'te yer alan bilgiler, kurum / kuruluşların karşılaşabileceği siber saldırı vektörlerine etkin karşı koyma yeteneklerinin arttırılması için yürütülen "Siber Tehdit İstihbaratı" çalışması ile elde edilmiştir. Hedef Odaklı Saldırı vektörlerinin kurum ve kuruluşlarda tespit edilme süresinin ortalama 240 gün olduğu düşünüldüğünde "Siber Tehdit İstihbaratı" sağladığı proaktif hizmet sayesinde kurum/kuruluşlarda "güvenlik farkındalığını" yüksek tutmaktadır.

Yukarıda yer alan bilgiler doğrultusunda APT28 (Fancy Bear) ve Snake (Turla, Uruburos) isimli grupların; kamu kurumları, savunma sektörü, enerji sektörü, havacılık sektörü, eğitim kurumları, ilaç endüstrisi ve medya sektörüne yönelik "Siber Casusluk" faaliyetleri düzenledikleri anlaşılmaktadır.

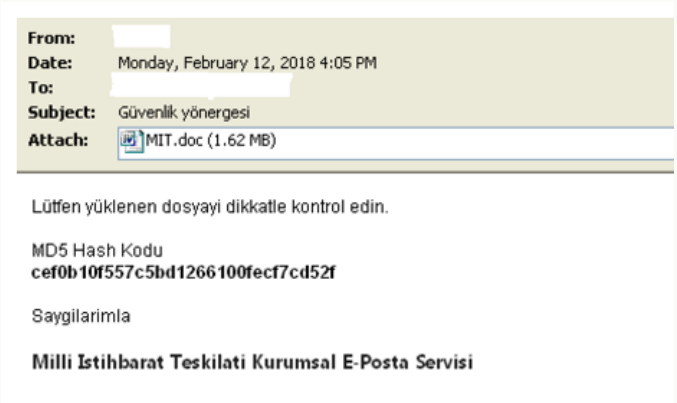
Grupların kuruldukları günden bugüne aktivite sıklıkları, kullandıkları metodoloji ve zararlı yazılımlarının istismar ettiği benzer zafiyetler ile iki grubun da "Rusya" merkezli olması nedeniyle "Siber Casusluk" operasyonlarını birlikte yürütme ihtimalleri veya eşgüdümlü olarak hareket etme ihtimalleri bulunmaktadır.

Siber Saldırılar

Oltalama Saldırısı Muddywater

2018 Ocak ile Mart ayları arasında Orta Doğu ve Orta Asya'daki işletmeleri hedef alan ve başta Türkiye, Pakistan ve Tacikistan olmak üzere birçok ülkenin kritik sanayi tesisini hedef alan yeni bir saldırı tespit edildi. Saldırıların arkasında İranlı bilgisayar korsanlarının görev aldığı Temp.Zagros adındaki grup olduğu düşünülüyor. TEMP.Zagros, ilk olarak 2017'de tespit edilmiş ve bilgisayar korsanları, çeşitli ülkelerde çeşitli sektörleri hedef alan oltalama saldırıları ile isimlerini duyurmuşlardı[14].

Saldırılardan etkilenen ülkelerin başında Türkiye olduğu ifade ediliyor. Saldırı vektörü olarak e-posta eki olarak gönderilen makro tabanlı dokümanlar olduğu düşünülüyor. Şekil 4'te Türkiye'deki kullanıcıları hedef alan örnek bir e-posta gösterilmiştir. Türkçe yazılmış içerikle TSK'dan gönderildiği iddia edilen bir belge de Şekil 5'te gösterilmiştir[15].



Şekil 4: Türkiye'deki kullanıcıları hedef alan bir e-posta

Yapılan gözlemler, saldırı tekniklerinin daha önce Orta Asya ve Orta Doğu coğrafyasını tehdit eden saldırılarda kullanılan MuddyWater ile benzerlik gösterdiğini ortaya koymuş durumda. Orta Doğu coğrafyasında geniş bir alanı etkileyen MuddyWater, özellikle hükümetlere bağlı kurumları hedef almıştı. Saldırganların tek seferlik saldırı modelini izlemektense büyük olasılıkla ülkelere ve kritik tesislere karşı siber casusluk aktivitelerini

Şekil 5: TSK'dan gönderildiği iddia edilen bir belge

sürdürmeye devam etmeleri bekleniyor[16]. Saldırganlar, kullanıcılar üzerinden sosyal mühendislik faaliyeti gerçekleştirip kullanıcıların söz konusu dosyayı tıklamasını sağlayarak klasörde yer alan zararlı yazılımı harekete geçiriyorlar. Araştırmalara göre zararlı yazılımlar, dokümanın içinde gömülü olarak yer alıyor. Zararlı yazılım, bir VBS dosyasını ve bir INI dosyasını bırakan makro tabanlı bir doküman kullanıyor. INI dosyası, WScript.exe kullanılarak yürütme sırasında VBS dosyası tarafından oluşturulan komut satırı kullanılarak yürütülecek Base64 kodlu PowerShell komutunu içeriyor. Saldırganlar bu şekilde hedef üzerinde istedikleri komutları çalıştırabiliyorlar.

[14] http://securityaffairs.co/wordpress/70453/hacking/temp-zagros-phishing.html
[15] https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html
[16] https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

Bu saldırılar, TEMP.Zagros grubunun en yeni kod yürütme ve kalıcılık mekanizma teknikleriyle güncel kaldığını ve kötü amaçlı yazılımlarını güncellemek için bu teknikleri hızla kullanabileceklerini veya eki tıklamamaları gerekiyor. Bu nedenle farkındalık eğitimleriyle toplumun her kesimine yayılan "siber güvenlik bilinci"nin oluşturulmasında fayda görülmektedir.

SHA256 Hash	Dosya Adı
76e9988dad0278998861717c774227bf94112db548946ef617bfaa262cb5e338	Invest in Turkey.doc
6edc067fc2301d7a972a654b3a07398d9c8cbe7bb38d1165b80ba4a13805e5ac	Güvenlik yönergesi. .doc
18479a93fc2d5acd7d71d596f27a5834b2b236b44219bb08f6ca06cf760b74f6	Türkiye Cumhuriyeti Kimlik Kartı.doc
3da24cd3af9a383b731ce178b03c68a813ab30f4c7c8dfbc823a32816b9406fb	Turkish Armed Forces.doc
cee801b7a901eb69cd166325ed3770daffcd9edd8113a961a94c8b9ddf318c88	KEGM-CyberAttack.doc
1ee9649a2f9b2c8e0df318519e2f8b4641fd790a118445d7a0c0b3c02b1ba942	IL-1801.doc
aa60c1fae6a0ef3b9863f710e46f0a7407cf0feffa240b9a4661a4e8884ac627	kiyiemniyeti.doc
c87799cce6d65158da97aa31a5160a0a6b6dd5a89dea312604cc66ed5e976cc9	egm-1.doc
18cf5795c2208d330bd297c18445a9e25238dd7f28a1a6ef55e2a9239f5748cd	Güvenlik Yönergesi.doc
153117aa54492ca955b540ac0a8c21c1be98e9f7dd8636a36d73581ec1ddcf58	MIT.doc
d07d4e71927cab4f251bcc216f560674c5fb783add9c9f956d3fc457153be025	Güvenlik Yönergesi.doc
af5f102f0597db9f5e98068724e31d68b8f7c23baeea536790c50db587421102	Güvenlik Yönergesi.doc
5550615affe077ddf66954edf132824e4f1fe16b3228e087942b0cad0721a6af	NA
3d96811de7419a8c090a671d001a85f2b1875243e5b38e6f927d9877d0ff9b0c	Güneydoğu Anadolu Projesinde .doc

Şekil 6: Zararlı yazılıma ait tehdit göstergeleri

göstermektedir. Birden fazla gizlenme ve kalıcılık tekniğini kullanarak tersine mühendislik süreçlerini engelleme ve aynı zamanda güvenlik ürünleri tarafından tespit edilememe yeteneği kazandıkları değerlendirilmektedir. Zararlı yazılıma ait ülkemize yönelik tehdit göstergeleri Şekil 6'da açıklanmıştır[17].

Son kullanıcılar, siber saldırganlar tarafından en fazla tercih edilen saldırı yöntemi olan sosyal mühendislik yöntemleriyle kendilerine gelen mesajları ayırt edemeyebiliyorlar. Bu noktada kendilerine sunulan içerikleri iyi ya da kötü olarak ayırt etme konusunda zorluk yaşıyorlar. Özellikle kamu ya da üretim gibi kritik altyapıları hedef alan saldırılar önemli zarara, kimlik hırsızlıklarına neden olabiliyorlar.

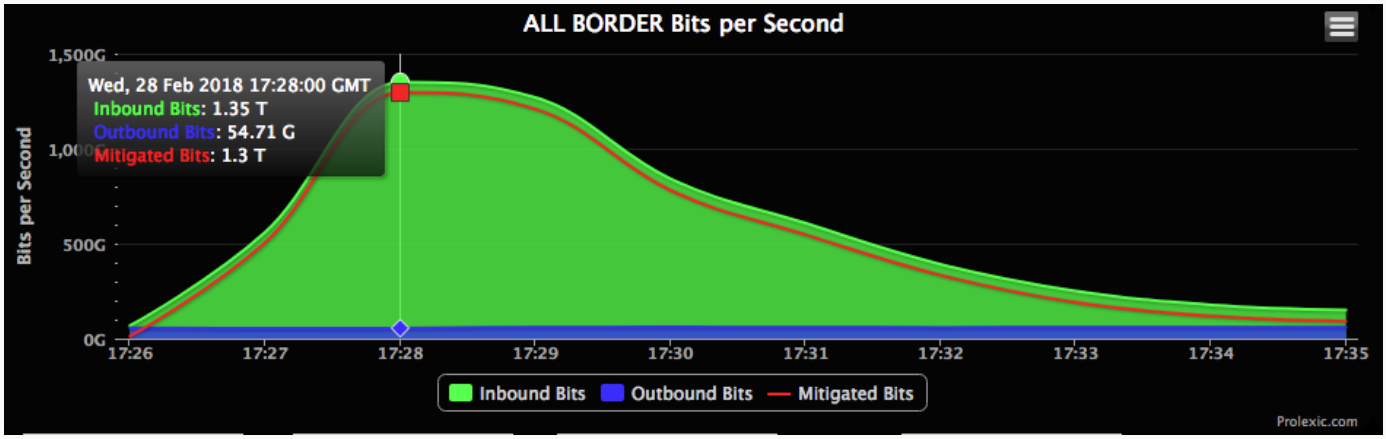
Kullanıcıların neden bu tür e-postalar aldıklarını dikkate almaları ve gerçek olduklarından emin oluncaya kadar genel olarak herhangi bir bağlantıyı

Memcached Sunucuları Kullanarak Dağıtık Hizmet Dışı Bırakma Saldırıları

Kod deposu olarak bilinen GitHub, 28 Şubat 2018 tarihinde bugüne kadar kaydedilen en büyük DDos saldırısına uğradı. Şekil 7'de görüldüğü gibi 1.35 Tpbs veri akışına maruz kalan web sitesi bir süre hizmet veremedi[18]. Saldırganlar, ilk defa DDoS saldırılarında Botnet kullanmadan bu denli güçlü ve rekor sayılan bir saldırı gerçekleştirdiler. Bu yapılan saldırı, şimdiye kadar görülen en büyük DDoS saldırısı olarak değerlendirildi, Mirai Botneti ve daha önce en büyük DDoS saldırısı olduğu açıklanan 2016 Eylül saldırılarının iki katından daha büyük bir saldırı olarak tarihe geçti[19].

Bu saldırıdan sadece dört gün sonra yeni rekor 1,7 Tbps'ye yükseldi[20]. DDoS saldırısı hafifletme hizmeti sunan bir siber güvenlik şirketi tarafından,

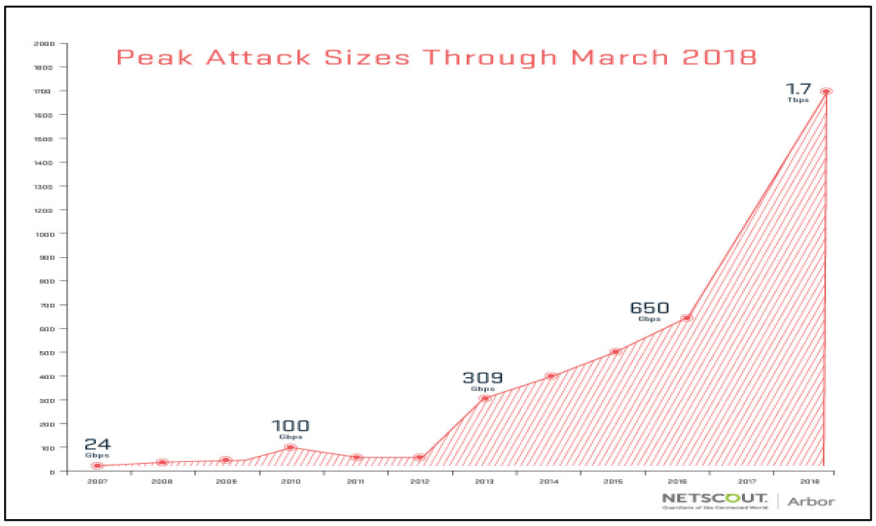
[17] Indicators of Compromise- Macro based Documents and Hashes https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html
[18] https://blogs.akamai.com/2018/03/memcached-fueled-13-tbps-attacks.html
[19] https://thehackernews.com/2018/03/biggest-ddos-attack-github.html
[20] https://www.hackread.com/worlds-largest-ddos-attack-us-firm-suffers-1-7-tbps-of-ddos-attack/



Şekil 7: GitHub Saldırı Hacmi

ABD merkezli bir müşterisinin, Şekil 8'de görüldüğü gibi saniyede 1,7 Tbps'lik veri akışının yaşandığı bir DDoS saldırısına maruz kaldığı açıklandı[21]. Yapılan açıklamaya göre son saldırı da, Github saldırısını oluşturan aynı memcached yansıtma/büyütme saldırı vektörüne dayanıyordu. 1,7 Tbps'ye ulaşan saldırının yöneldiği ABD'li şirkette, yeterli güvenceler sayesinde herhangi bir kesinti yaşanmadığını da bildirdi.

Her iki saldırıda da ortak olarak web uygulamalarını ve sitelerini hızlandırmak için tasarlanan, güvenli olmayan Memcached sunucularının kullanılması gösteriyor ki kimlik doğrulama gerektirmeyen sunucular, hedeflenen bir hizmette trafiği yükseltmek için yansıtıcı olarak kötü amaçla kullanılabiliyorlar.



Şekil 8: Arbor Networks Raporu Saldırı Hacmi

Memcached Nedir?

Memcached, nesnelerin belleğe kaydedilmesine ve çok sayıda açık bağlantıyla çalışacak şekilde tasarlanmasına olanak tanıyan açık kaynaklı ve kolayca dağıtılabilen, dağıtılmış önbelleğe alma (cache) sistemidir. Sorguları ram üzerinde önbellekler ve bir sonraki çağırılışında verinin hızlı dönülmesini, haliyle de performans artırımı ve sunucu yükünün hafiflemesini sağlar. Memcached sunucu, (Transport Control Protocol) TCP veya (User Datagram Protocol) UDP bağlantı noktası 11211 üzerinden çalışmaktadır.

Memcached Açığını Saldırganlar Nasıl Kullanır?

Saldırılar UDP paketlerin 11211 portu üzerinden gönderilmesiyle gerçekleştirilmektedir. Memcached açığından faydalanılarak yapılan saldırı tipine literatürde "amplification attacks" denilmektedir. Saldırgan, DDoS amaçlı kullanabileceği sunucuyu tespit ederek ilgili porttan sunucuya sahte UDP paket gönderir. Sunucu gelen bu paketi bilmediği için

[21] https://www.arbornetworks.com/blog/asert/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/

reddettiğine dair karşı bir paket hazırlar. Saldırı süreci de böylelikle başlamış olur. Saldırgan, saldırı yapılmasını istediği IP adresi üzerinden (spoof) istek gönderip Memcached kullanan ve 11211 portu açık sunucudan buraya cevap dönülmesini sağlar. Böylelikle DDoS trafiği başlamış olur. Ayrıca amplification saldırılarında, 1'e 5000 hatta 1'e 51000 etkisinde saldırı yapılabilir. Yani 10 byte'lık bir isteğe 510 KB yanıt gönderilebilir. Saldırganların DDoS saldırısında kullandığı Memcrashed-DDoS expolit koduna dipnotta belirttiğimiz bağlantıdan ulaşabilirsiniz[22].

Bu olay benzeri durumlara karşı savunma yapabilmek için öneriler şu şekilde sıralanıyor:

• Memcached localden dinletip çalıştırılması. Eğer dışarıdan bir IP'nin bu port ve servise ulaşması gerekmiyorsa:

- Metin editörüyle (vi, nano veya vim)/etc/sysconfig/memcached dosyasını açın. (CentOS için.)

- OPTIONS="" parametresini bulun.

- OPTIONS="-l 127.0.0.1" olarak güncelleyin.

- memcached servisini restart edin.

netstat -ntlp komutunu çalıştırıp memcached servisinin 127.0.0.1 dinlediğinden emin olun. (0.0.0.0) olmamalı.

• Eğer tüm servisler aynı sunucudaysa memcached, socket bazlı da çalıştırabiliyor ve bu yöntem daha performanslı oluyor. Bunun için yine OPTIONS parametresinin aşağıdaki şekilde güncellenmesi ve servisin yeniden başlatılması gerekiyor.

OPTIONS="-s /tmp/memcached.socket"

• Memcached'e bug fix içeren bir güncelleme yayımlandı ve UDP portu varsayılan "disable" olarak değiştirildi. Konuyla ilgili dokümana dipnotta belirttiğimiz bağlantıdan erişebilirsiniz[23].

Slingshot Casus Yazılımı

Araştırmacılar tarafından, Orta Doğu ve Afrika'da 2012'den Şubat 2018'e kadar siber casusluk için kullanılan gelişmiş bir tehdidi tespit edildi. Bu konuda yayımlanan raporda;

• Slingshot'ın keşfedilmesiyle birlikte oldukça esnek ve iyi tasarlanmış bir siber casusluk platformu ortaya koymak için bir araya getirilmiş birçok bileşeni olan bir çalışmanın olduğu diğer bir karmaşık ekosistemin ortaya çıktığını,

• Oldukça gelişmiş olan bu yazılımın, her çeşit soruna teknik bir bakış açısıyla ve genellikle oldukça zekice yollarla çözüm getiren, hassas şekilde düşünülerek eski ve yeni bileşenleri bir araya getiren, uzun vadeli olarak tasarlanmış, sağlam kaynaklara sahip üst seviyede bir aktörün hazırladığı bir sistem olarak karşımıza çıktığını görüyoruz[24]. 'Slingshot' adını verilen zararlı yazılım kurbanların bilgisayarlarına, ele geçirilmiş yönlendiriciler üzerinden bulaşıyor. Çekirdek (kernel) modunda çalışabilen yazılım, kurbanın bilgisayarının tüm kontrolünü elinde bulundurabiliyor. Şimdiye kadar Türkiye ile birlikte Kenya, Yemen, Afganistan, Libya, Kongo, Ürdün, Irak, Sudan, Somali ve Tanzanya'da Slingshot ve ilgili modüllerden etkilenen 100 civarında kurban tespit edildi. Kurbanlar genelde kurum ve kuruluşlardan ziyade bireysel kullanıcılardan oluşuyor, ancak aralarında bazı devlet kurum ve kuruluşlarının da yer aldığı belirtiliyor[25]. En çok etkilenen ülkelerin ise Kenya ve Yemen olduğu değerlendiriliyor.

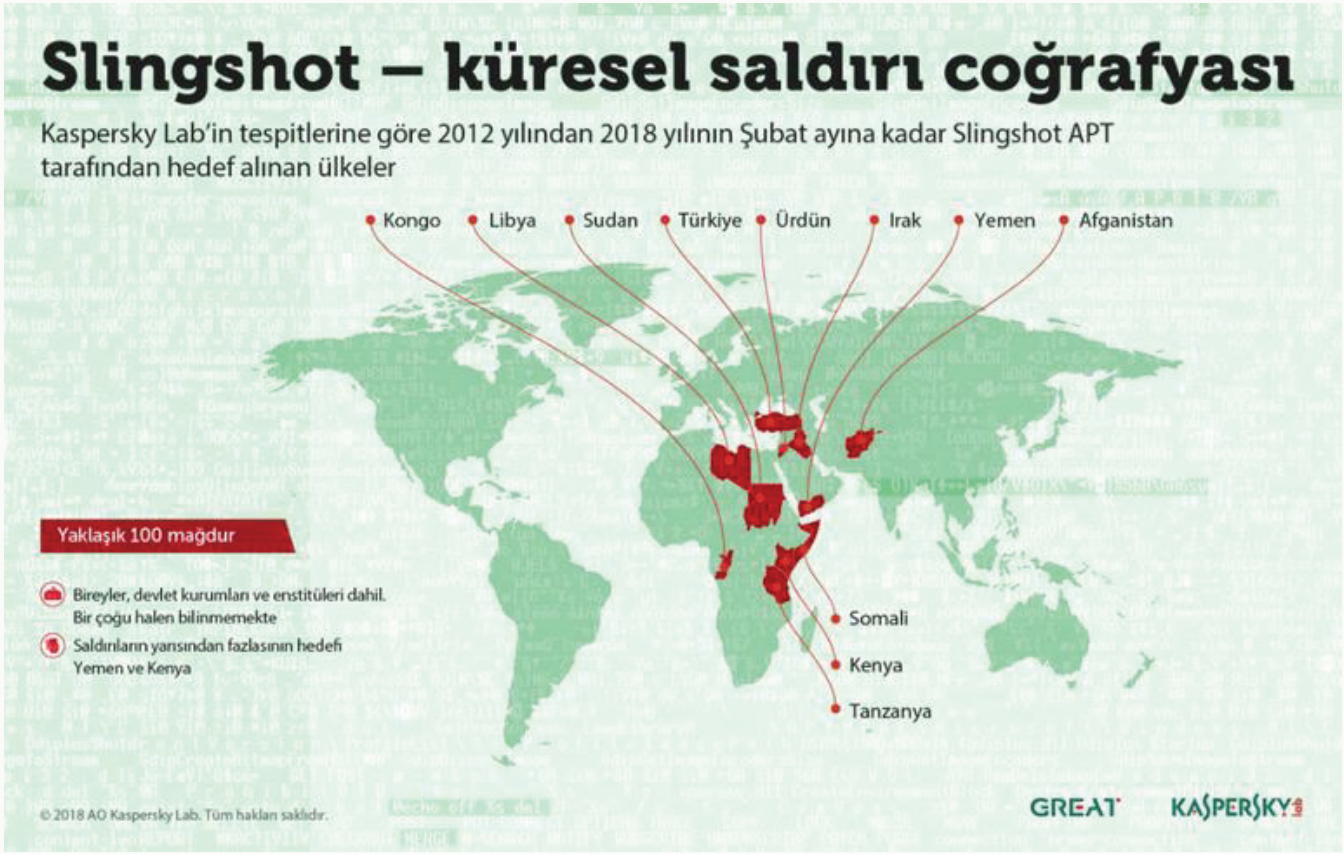
Slingshot'ın ilk çıktığı zamanlarda hedeflerine nasıl nüfus ettiği henüz tam olarak bilinmiyor. Bununla birlikte birkaç olayda Slingshot'ı yönetenlerin Litvanya'da üretilen MikroTik adlı modemlere erişim sağladıkları ve modeme zararlı bir kod enjekte ettikleri biliniyor. Modem tekniğinin detayları bilinmemekle birlikte modemin dosya sisteminden dinamik bağlantı kütüphanesi dosyalarının indirilmesi için MikroTik'in kullandığı 'Winbox' adlı konfigürasyonun kullanıldığı düşünülüyor. Bu dosyalardan ipv4.dll adlı dosyanın, Slingshot'ın

[22] https://github.com/649/Memcrashed-DDoS-Exploit/

[23] https://github.com/memcached/memcached/wiki/ReleaseNotes156

[24] https://s3-eu-west-1.amazonaws.com/khub-media/wp-content/uploads/sites/43/2018/03/09133534/The-Slingshot-APT_report_ENG_final.pdf

[25] https://thehackernews.com/2018/03/slingshot-router-hacking.html

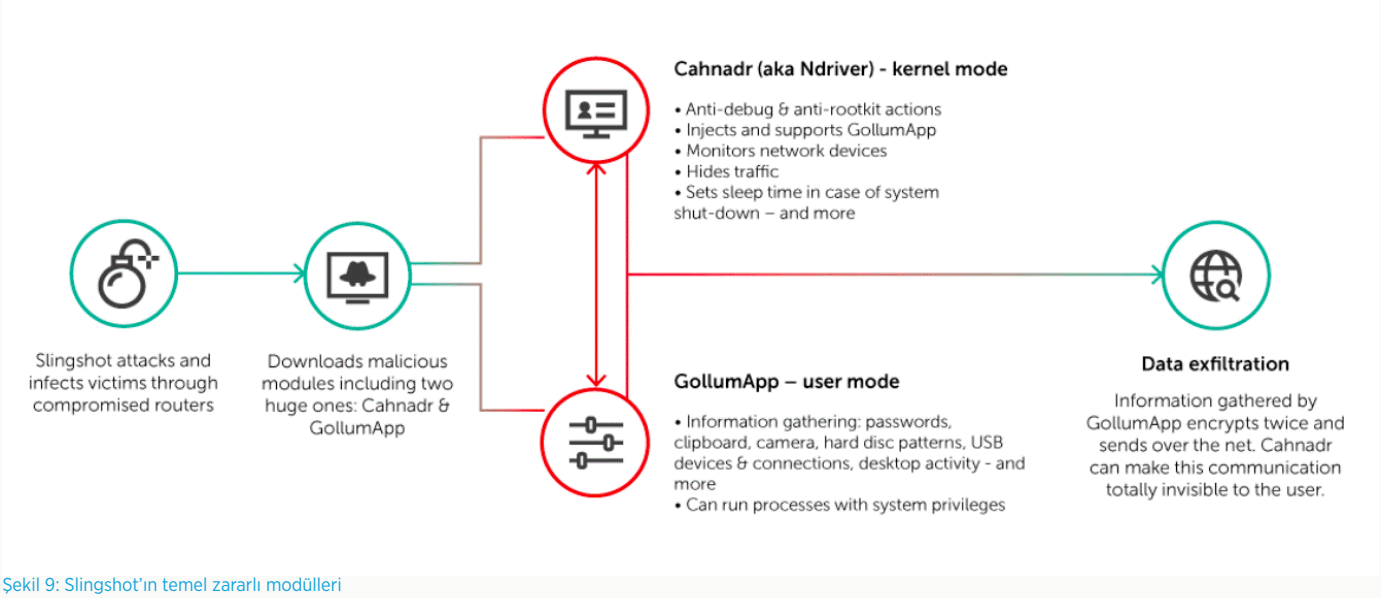


geliştiricileri tarafından oluşturulmuş zararlı bir indirme ajanı olduğu söyleniyor. Winbox, ipv4. dll dosyasını hedef bilgisayara aktararak hafızaya yüklüyor ve çalıştırıyor.

Slingshot operasyonu, araştırmacıların yazılan karakterleri kaydeden şüpheli bir programı fark edip kodun başka bir yerde kullanılıp kullanılmadığını görmek için davranışsal tespit işareti oluşturmasının ardından keşfedildi. Bu yöntemin kullanılmasıyla sistem klasöründe scesrv.dll adlı şüpheli bir dosyanın yer aldığı bir bilgisayar tespit edildi. Araştırmacılar incelemeyi derinleştirmeye karar verdiler. Dosya analiz edildiğinde yasal gibi gözükse de aslında scesrv.dll modülünde zararlı kodlar bulunduğu görüldü. Bu arşiv, sistem ayrıcalıklarına sahip 'services.exe' ile birlikte yüklendiğinden aynı yetkileri elde ediyordu.

Slingshot'ın en çok dikkat çeken özelliği, çok yaygın olmayan saldırı yöntemlerini kullanması. Daha fazla kurban keşfedildikçe çoğunda yazılımın ele geçirilmiş yönlendiricilerden bulaştığı görüldü. Slingshot'ın arkasındaki grubun saldırı sırasında yönlendiricileri ele geçirip, içine zararlı bir dinamik bağlantı arşivi yerleştirdiği belirlendi. Bu arşiv aslında diğer zararlı bileşenlerin indirilmesini sağlıyordu. Bir sistem yöneticisi yönlendiriciyi yapılandırmak için giriş yaptığında, yönlendiricinin yönetim yazılımı zararlı modülü sistem yöneticisinin bilgisayarına indirip çalıştırıyor. Yönlendiricilerin nasıl ele geçirildiği ve yapılan operasyonun bu denli nasıl genişlediği hakkında ise henüz net bilgiler elde edilmiş değil[26]. Zararlı yazılımın bulaşmasının ardından, Slingshot kurbanın cihazına çok sayıda modül yüklüyor. Bunlar arasında iki adet çok büyük ve güçlü modül bulunuyor: Cahnadr (çekirdek) ve GollumApp (kullanıcı) (Şekil 9). Bağlı bu iki modül; bilgi toplama, kalıcılık, trafik gizliliği ve toplanan verilerin dışarı sızdırılması konusunda işlevsel olarak birbirlerine yardımcı olduğu değerlendiriliyor.

[26] https://www.secplicity.org/2018/03/13/sophisticated-slingshot-attack-daily-security-byte/



Şekil 9: Slingshot'ın temel zararlı modülleri

Slingshot'ın siber casusluk amacıyla kullanıldığı düşünülüyor. Yapılan analizlerde yazılımın; ekran görüntüleri, klavye verileri, ağ verileri, parolalar, USB bağlantıları, diğer masaüstü aktiviteleri ve pano verilerini toplayabildiği anlaşıldı. Zaten yazılımın kernel erişiminin olması istediği her şeyi çalabileceği anlamına geliyor. Slingshot'ın bugüne kadar yalnızca en gelişmiş saldırılarda gördüğümüz kernel modu modülleri gibi birçok araç ve yöntem kullanan oldukça karmaşık bir tehdit olduğu, yazılımın sahip olduğu işlevlerin saldırganlar için çok değerli olduğu ve bunun da Slingshot'ın neden yaklaşık altı yıldır kullanıldığını gösterdiği vurgulanıyor.

Bu ve benzeri durumlara karşı savunma yapabilmek için önerilerimiz şu şekilde:

- Mikrotik yönlendiricileri kullananların, bilinen açıklardan korunmak için en kısa sürede yazılımlarını son sürüme yükseltmeleri. Mikrotik Winbox artık yönlendiriciden kullanıcı bilgisayarına hiçbir şey indirilmesine izin vermiyor.

- Hedef odaklı saldırıları önleyen teknolojilere ve tehdit istihbaratı özelliğine sahip kurumsal düzeyde bir güvenlik çözümü kullanılması. Bu çözümler, ağdaki anormallikleri analiz edip siber güvenlik ekiplerinin tüm ağı görebilmesini ve otomatik tepki vermesini sağlayarak gelişmiş hedefli saldırıları yakalayabiliyor.

- Güvenlik ekiplerinin en son tehdit istihbaratı verilerine erişmelerinin sağlanması. Bu sayede, hedefli saldırıları önlemeleri için sızıntı belirtileri (IOC), YARA ve özel gelişmiş tehdit raporlaması gibi araçların sistemlerde kullanılması faydalı olacaktır.

Arka Kapı İçeren BitTorrent Yazılımındaki Tehlike

2018 Mart ayının ilk haftasında MediaGet olarak adlandırılan BitTorrent istemcisinin arka kapı içeren bir varyasyonu nedeniyle yaklaşık yarım milyon bilgisayara zararlı yazılım bulaştığı tespit edildi[27].

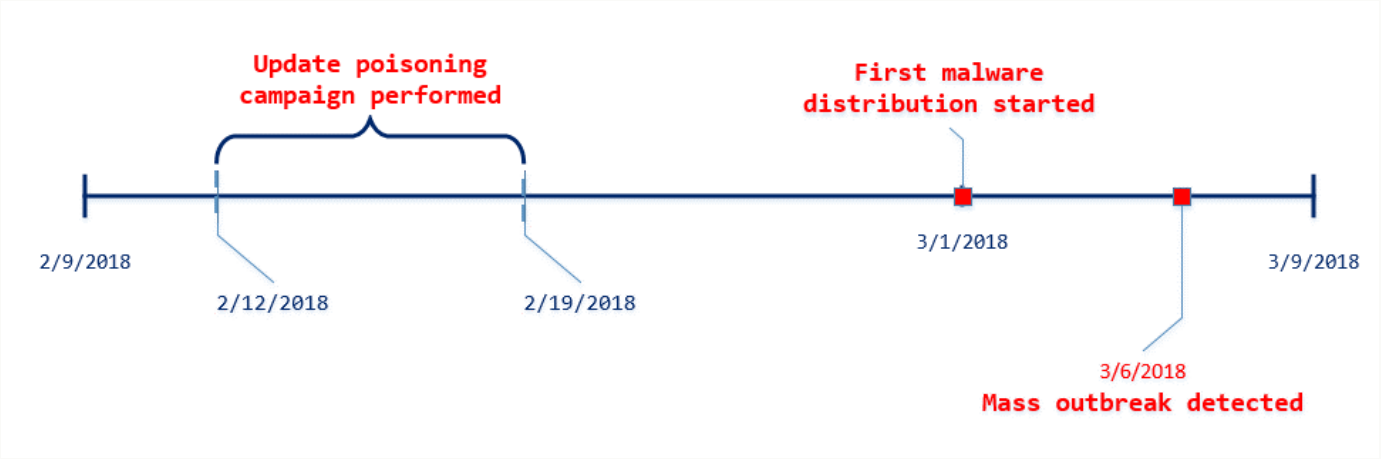
Dufoil'in bir varyasyonu olduğu belirtilen kötü amaçlı yazılım, bulaştığı Windows bilgisayarlara kripto para madenciliği ile ilgili bir program yüklüyor ve kurbanların işlemcisini kullanarak Electroneum kripto parası madenciliği için istismar ediyor.

6 Mart 2018'de Türkiye, Rusya ve Ukrayna'daki bilgisayarları etkileyen saldırının, Microsoft Windows Defender araştırma bölümü tarafından keşfedildiği ve ciddi bir zarara yol açmadan önce engellendiği belirtiliyor, ancak saldırının 12 saat içerisinde nasıl bu kadar büyük bir kitleye erişebildiğini anlatan bir açıklamanın yapılmadığı görülüyor.

Yapılan detaylı araştırmalar sonucunda saldırının MediaGet BitTorrent yazılımının güncelleme mekanizmasını hedef alarak yapıldığı belirtildi.

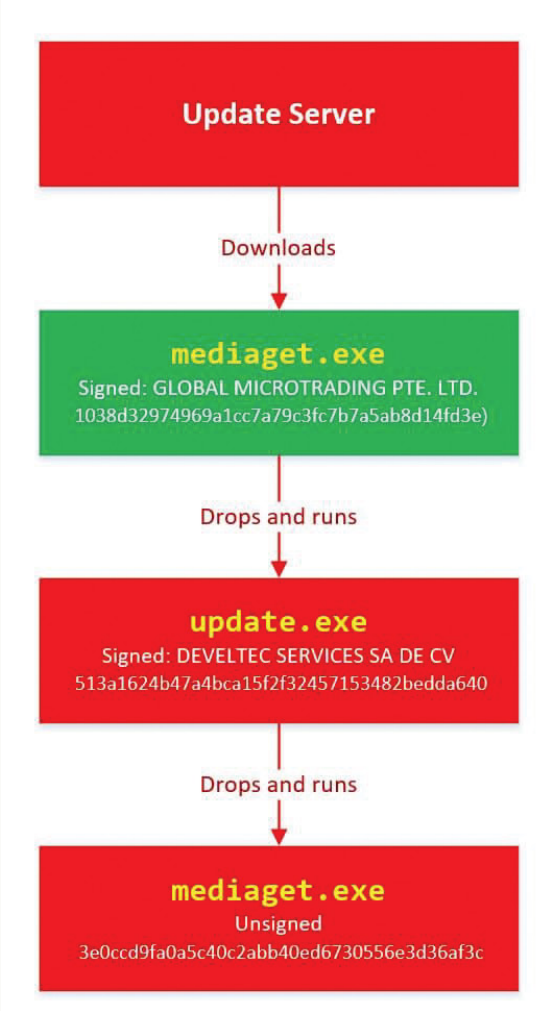
İmzalı mediaget.exe, update.exe programını indiriyor ve yeni mediaget.exe'yi indirmesini sağlamak için çalıştırıyor. Böylece kurbanın bilgisayarına orijinali ile aynı özelliklere sahip olan

[27] https://thehackernews.com/2018/03/windows-malware-hacking.html



ve arka kapı içeren yazılım indirilmiş oluyor.

Arka kapı içeren zararlı BitTorrent yazılımı, merkezi olmayan Namecoin ağ altyapısında bulunan komuta kontrol sunucusuna bağlanıyor. Daha sonra komuta kontrol sunucusunda Coinminer bileşenini indiriyor ve kurbanların bilgisayarını kullanarak saldırganlar için kripto para madenciliği yapıyor.



Saldırganların ayrıca komuta kontrol sunucuları aracılığıyla kurbanların bilgisayarlarına uzak URL adreslerinden zararlı yazılım indirebildiği de ifade ediliyor. update.exe dosyasını imzalayan MediaGet'in de saldırının kurbanı olduğunu düşünülüyor. Bu durum, saldırganların update.exe dosyasını farklı bir sertifika ile imzaladığını ve sahte sertifikanın MediaGet tarafından başarılı bir şekilde doğrulandığını gösteriyor.

Virüs bulaşmış BitTorrent istemcisinin Windows Defender AV tarafından Trojan:Win32/Modimer.A olarak tespit edildiği ve ikilik sayı düzeninde orijinal MediaGet ile %98 benzerlik gösterdiği belirtiliyor.

Windows Defender yazılımının kullandığı davranışsal izleme ve makine öğrenmesi teknikleri bu büyük zararlı yazılım harekâtının tespit edilmesinde ve engellenmesinde önemli rol oynuyor.

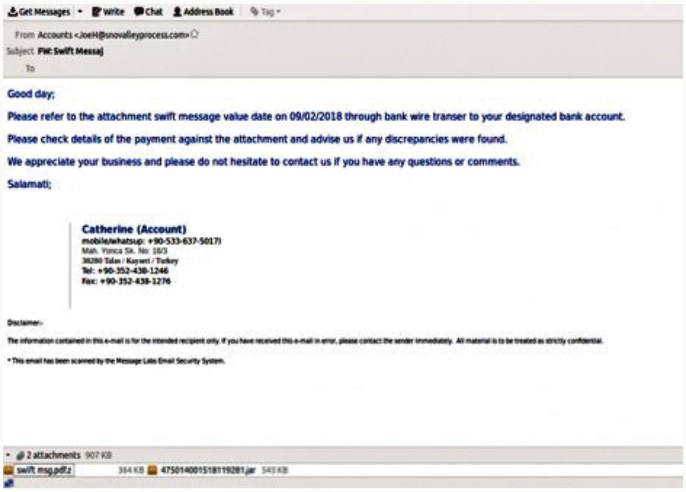
Windows 10, Windows 8.1 ve Windows 7'de Microsoft Security Essentials ya da Windows Defender AV çalıştıran kullanıcıların bu saldırıdan etkilenmediği biliniyor.

SWIFT Oltalama Saldırısı

2018 Şubat ayının başlarında bankalar arası para transfer sistemi olan SWIFT'i hedef alan yeni bir oltalama saldırısı keşfedildi. Daha önceki saldırılardan farklı olarak bu saldırıda, kurbanların kredi kartı bilgilerinin çalınmasının yanı sıra, kullanıcıların cihazları Adwind RAT adı verilen bir uzaktan erişim aracı ile enfekte oluyor.

2015 yılında keşfedilen Adwind RAT Android, macOS, Linux ve Windows cihazları etkiliyordu.

Yapılan son oltalama saldırısında ise zararlı yazılımın Windows tabanlı cihazları hedef aldığı belirtiliyor[28]. Saldırılarda kullanılan e-postalarda, kullanıcılara hesaplarından bir havale işlemi başlatıldığı ve detayların e-posta ekinde bulunduğu söyleniyor.



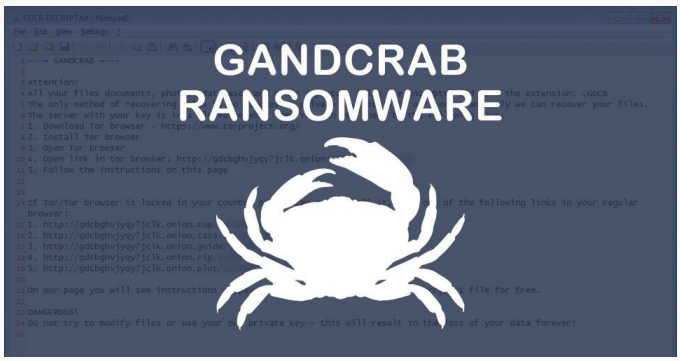
Kurbanların e-posta içerisinde bulunan eklentiye tıklaması ile birlikte eklenti içerisinde bulunan Adwind zararlı yazılımı kurbanın cihazına bulaşıyor.

Zararlı yazılım sistem kayıt defterini değiştiriyor, antivirüs kurulumunu kontrol ediyor ve var ise süreçlerini öldürmeye çalışıyor. Cihaza zararlı yürütülebilir dosyalar yüklüyor (anti-adwire, forensic, monitoring) ve daha sonra Tor ağındaki bir alan adı ile bağlantı kuruyor.

Zararlı yazılım ayrıca Windows Geri Yükleme seçeneğini devre dışı bırakmaya çalışıyor ve kullanıcı farkında olmadan bir program kurmayı engelleyen "Kullanıcı Hesap Denetimi" özelliğini kapatıyor.

Saldırının 9 Şubat 2018 tarihinde gerçekleştirildiği, dokuz saat sürdüğü ve Türkiye ile birlikte Kıbrıs ve Hollanda'yı etkilediği belirtiliyor.

Bu tür saldırılardan kaçınmak için bilinmeyen kaynaklardan gelen e-postalar açılmamalı, e-posta içerisindeki bağlantılara tıklanmamalı ve eklentiler indirilmemeli/açılmamalıdır. İndirilen eklentilerin taranarak zararlı aktivite barındırmadığından emin olunmalı.



GandCrab Fidye Yazılımı

2018 Şubat ayının başında Rus siber saldırı topluluğu tarafından Dark Web üzerinde reklamı yapılan GandCrab adında bir fidye yazılımı keşfedildi.

Çoğu Avrupa'da olmak üzere yaklaşık 50,000 bilgisayara bulaştığı tahmin edilen fidye yazılımının dağıtımı için RIG ve GrandSoft istismar kitlerinden faydalanılıyor. Yazılım sisteme enfekte olduğunda ödeme yapılmazsa ödenmesi gereken tutar iki katına çıkıyor. Ödemenin Dash kripto para ile yapılmasına izin veriliyor ve hizmet, .bit alan adını içeren bir sunucu tarafından sağlanıyor.

Fidye yazılımının yönetici konsoluna Tor ağı üzerinden erişilebiliyor. Konsol, zararlı yazılım kişiselleştirmesine izin veren (fidye miktarı, bireysel botlar vb.) kullanıcı dostu bir arayüze sahip.

GandCrab yazılımcıları, üyelerine teknik destek ve güncelleme sunmalarının yanı sıra fidye yazılımının antivirüsler tarafından algılanmasının nasıl engelleneceğini anlatan bir video yayımlamış.

Fidye yazılımının Dark Web üzerinde yapılan reklamında aşağıdaki maddeler dikkat çekiyor[29]:

[28] https://www.hackread.com/wire-bank-transfer-malware-phishing-email-hits-swift-banking-system/
[29] http://securityaffairs.co/wordpress/68636/malware/gandcrab-raas.html

• Olası alıcılardan fidye yazılımından elde edilen kârın 60'a 40 olarak bölündüğünü belirten "ortak program"a katılmaları beklenmektedir.

• Büyük ortaklar paylarını %70'e çıkarabilir.

• Hizmet olarak sunulan fidye yazılımı için ortaklara teknik destek ve güncelleme sunulmaktadır.

• Ortaklar, Bağımsız Devletler Topluluğu ülkelerini (Azerbaycan, Ermenistan, Beyaz Rusya, Kazakistan, Kırgızistan, Moldova, Rusya, Tacikistan, Türkmenistan, Özbekistan ve Ukrayna) hedef olarak seçemezler. Bu kuralı ihlal edenlerin hesapları silinir.

• Ortaklar, sınırlı sayıdaki fidye yazılımını kullanmak için başvuruda bulunmalıdırlar. Saldırıdan yaklaşık

bir ay sonra, Romanya polisi, Europol ve Organize Suç ve Terörle Mücadele Dairesi (DIICOT) ile birlikte fidye yazılımının şifresini çözen ücretsiz bir araç piyasaya sürüldü[30].

Şifre çözücünün bilinen tüm GandCrab sürümleri için işe yaradığı iddia edilse de birkaç kullanıcı ve güvenlik araştırmacısı uygulama ile ilgili bazı problemlerin olduğunu bildirdi. Bu tür durumlarda kullanıcıların yazılımın resmi dokümantasyonuna bakmaları gerekiyor.

İzlanda'da Kripto Para Madenciliği Amaçlı Bilgisayar Hırsızlığı

Özellikle bitcoin ve diğer kripto para birimlerine yönelik madencilik faaliyetleri için tasarlanmış 600'e yakın yüksek kapasiteli bilgisayar İzlanda veri merkezlerinden çalındı. Yapılan tahminlere göre bilgisayarların değeri 2 milyon ABD Dolarını buluyor. Çalınanlar arasında bilgisayarların yanı sıra 600 adet grafik kartı, 100 adet işlemci, 100 adet güç kaynağı, 100 adet anakart ve 100 adet bellek bulunuyor.

İzlanda'nın yaşadığı en büyük soygun vakalarından olan bahse konu hırsızlığın 2017 Aralık ayı sonları ile 2018 Ocak ayı başlarında gerçekleştirildiği değerlendiriliyor[31] ancak soyguncuların izlerinin sürülebilmesi amacıyla konunun halka duyurulması 2018 Mart ayı başlarında yapıldı.

Suçluların kâr amacıyla bugüne kadar kripto para borsalarına saldırdıkları, madencilik zararlı yazılımı ve fidye yazılımı yaydıkları hatta fidye için kripto para yatırımcılarını kaçırdıkları ve bir bitcoin borsasını soymayı denedikleri belirtiliyor.

İzlanda, enerji tüketen sunucuların soğutulmasına yardımcı olan soğuk iklimi ve ucuz elektrik fiyatları nedeniyle kripto para madenciliği firmalarının veri

[30] http://securityaffairs.co/wordpress/69694/malware/gandcrab-ransomware-decryptor.html

[31] https://thehackernews.com/2018/03/bitcoin-mining-computers.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1694.gh0ao08pqk.111a

merkezleri için cazip bir ülke konumunda. Ülkede üretilen enerjinin hemen hemen tamamı jeotermal ve hidroelektrik gibi yenilenebilir kaynaklardan elde ediliyor.

Polisin, saldırganların çaldıkları bilgisayarları devreye almış olmaları ümidiyle ülke çapında yüksek enerji harcanan bölgelerde inceleme yaptığı, aynı zamanda enerji kullanımındaki ani yükselmeleri tespit edip anormalliklerin kendilerine bildirilmesi amacıyla internet servis sağlayıcılar ve elektrik sektöründe çalışanlarla da irtibat halinde çalıştığı ifade ediliyor.

POS Cihazlarından Kart Bilgileri Çalınabiliyor

POS (Point-of-sale) cihazlarından, özgün bir tekniğe dayalı olarak ödeme yapılan kart bilgilerini çalan yeni bir zararlı yazılım türü keşfedildi.

UDPoS olarak adlandırılan bu yeni zararlı yazılım, kart bilgilerini aktarmak için daha önceki POS zararlı yazılımlarının kullandığı HTTP yerine UDP Domain Name System (DNS) trafiğini kullanıyor ve adını da buradan alıyor[32].

Zararlı yazılım örneğinin, beklenenin aksine bu tür komuta kontrol sunucularının yoğun olduğu ABD,

Çin, Kore, Türkiye veya Rusya yerine İsviçre'de konuşlu bir komuta kontrol sunucusu ile bağlantılı olduğu ortaya çıkmış durumda. Sunucuda gerçek zararlı yazılımını içeren ve kendi kendine açılabilen bir zip arşivi olan taşıyıcı dosyası bulunmakta.

Alışılmamış DNS sorgularıyla bilgi aktarımı yapmasının yanında, UDPoS kendisini yasal bir uzaktan masaüstü kontrol uygulaması olan LogMeln'in güncellemesi olarak gösteriyor ve böylece çalınan kart bilgilerinin transferi esnasında güvenlik duvarları ve diğer güvenlik kontrollerinden kaçınmaya çalışıyor. Burada not edilmesi gereken bir husus da zararlı yazılımın sadece LogMeln kullanan daha eski POS sistemlerini hedef alması.

Zararlı yazılımın hâlihazırda kredi veya banka kart bilgilerinin çalınması maksadıyla kullanıldığına yönelik bir kanıt yok, ancak yapılan testler yazılımın kendisinden beklenen fonksiyonları yerine getirebilecek kabiliyette olduğunu gösteriyor. Kaldı ki tehdide yönelik araştırmalar esnasında zararlı yazılım örneğinin haberleştiği komuta kontrol sunuculardan birisinin aktif olduğunun ortaya çıkması, uzmanların gerçek zararlı yazılımın komuta kontrol sunucuları ile iletişim kurabileceğinin bir kanıtı olarak görülüyor.

Bu arada LogMeln tarafından yapılan açıklamada, uygulamalarının ele geçirilmediği, yamaların, güncellemelerin güvenli olarak dağıtılacağı, kullanıcılarından bir ek ile veya bağlantı yoluyla güncelleme yapmalarının istenmeyeceği konusu vurgulandı.

Uzmanlara göre bu tür bir zararlı yazılımla mücadelenin zorlukları bulunuyor, çünkü hemen hemen tüm şirketlerin TCP ve UDP tabanlı iletişimi izlemek ve filtrelemek için güvenlik duvarları ve diğer koruma tedbirleri varken, DNS'in hâlâ saldırganlara sızmak için bir fırsat bırakacak şekilde farklı ele alındığı ifade ediliyor.

[32] https://thehackernews.com/2018/02/pos-malware-dns.html

Zararlı Yazılım Analizi

Kripto Para Madenciliği Yapan Android Zararlısı ADB.Miner

ADB.Miner 2018 Şubat ayında ortaya çıkan, bulaştığı Android tabanlı cihazlara Monero kripto para madenciliği yaptıran bir zararlı.

Android işletim sistemi bulunan cihazlar arasında port 5555 üzerinde çalışan Android Debug Bridge (ADB — Android cihazların durum yönetiminin yapılabildiği bir arayüz) özelliği açık olan cihazları hedef alıyor. Bulaştığı cihazları bot ağına ekleyen ADB.Miner, bu cihazlar üzerinden kripto para madenciliği yapıyor.

Agresif bir yayılma şekli benimseyen ADB.Miner, bir solucan zararlısı gibi yayılma eğilimi gösteriyor. Bulaştığı cihazlar üzerinden internet taraması yapan ADB.Miner, 5555 portunu açık bulduğu başka cihazlara bulaştığı cihaz üzerinden yayılıyor. İnternet taramalarının takip edildiği sistemlerde, 5555 portunu içeren tarama verilerinde ciddi bir artış gözlemleniyor.

İnternet ortamında en çok taranan portlar arasında ilk 10'da yer almayan 5555 portu, ADB.Miner zararlısının ortaya çıkmasıyla birlikte ilk 5'de yerini almış bulunuyor (Şekil 10). [33]

ADB.Miner;

- Yayılmak için Mirai zararlısının kaynak kodlarını kullanıyor.
- Mirai'nin kaynak kodlarını kullanan ilk Android zararlısı olarak karşımıza çıkıyor. Android zararlısı, Mirai'nin IoT ve ağ cihazlarını tespit etmek amacıyla kullandığı kaynak kodunun bazı kısımlarını içerisinde barındırıyor.
- Monero madenciliği yaptırdığı cihazlardan elde ettiği kripto paraları "44XT4KvmobTQfeWa6P-CQF5RDosr2MLWm43AsaE3o5iNRXXTfDbYk2VP-HTVedTQHZyfXNzMn8YYF2466d3FSDT7gJS8gd-HAr" adresine yolluyor.

Ayrıca, ADB.Miner Android zararlısının yayılmak için her hangi bir zafiyeti istismar etmediğini belirtmekte fayda var. ADB özelliği Android cihazlar içerisinde varsayılan olarak kapalı gelmektedir. ADB özelliğinin kullanılması için üretici ya da kullanıcı tarafından açılmış olması gerekiyor. Özellikle rootlanmış Android cihazlarda sıkça karşılaşılan bu durum cihazlarımızın ADB.Miner gibi zararlılara maruz kalmasına sebep olabilir. Evlerimizdeki Android tabanlı cihazlar için de geçerli olabileceğinden port 5555'i açık cihazların tespitinin yapılmasında, eğer kullanılıyorsa güvenlik duvarı yardımı ile dışarıdan erişime kapatılmasında, eğer kullanılmıyorsa da ilgili servisin kapatılmasında fayda bulunuyor.

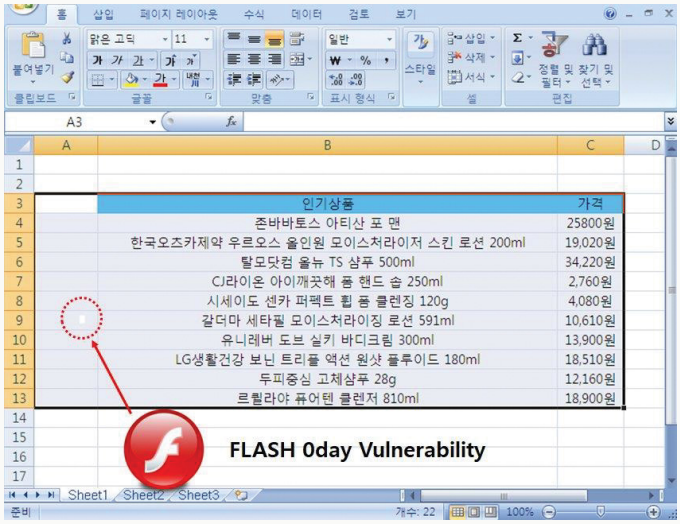
	dstport	Uniq ...	Scan volume by...	Total ...	Scan volume by...
1	23	415k		127M	
2	1433	18.5k		75.2M	
3	5555	78.6k		41.4M	
4	22	42.7k		30.4M	
5	445	86.8k		16.5M	
6	3306	2.65k		9.78M	
7	3389	15.6k		7.94M	
8	8080	63.5k		5.77M	
9	2323	134k		5.72M	
10	81	53.2k		4.27M	

Şekil 10: ADB.Miner sonrası alınan bir en çok taranan port örneklemesi

[33] http://scan.netlab.360.com

Adobe Flash Player Uzaktan Komut Çalıştırma Zafiyeti

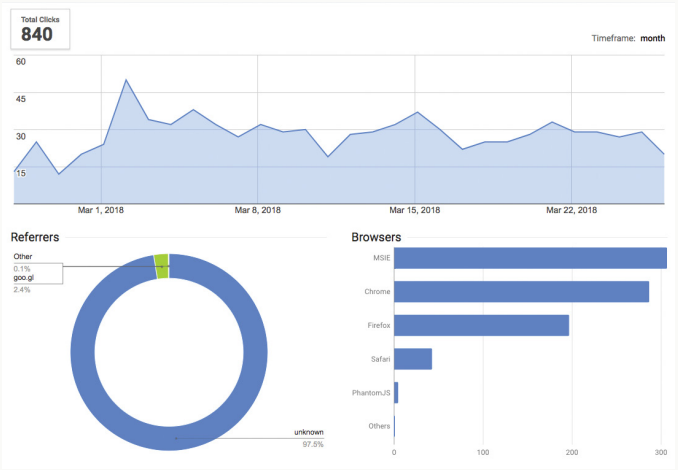
31 Ocak 2018 tarihinde Güney Kore CERT biriminin yayımladığı raporda[34] ortaya çıkan uzaktan komut çalıştırma zafiyeti (CVE-2018-4878), hem tarayıcılar hem de Office dokümanları üzerinden çalışarak sistemleri etkileyebiliyor. Zafiyet, Adobe firması tarafından 1 Şubat 2018'de duyuruldu[35], fakat yaması ancak bir hafta sonra yayımlanabildi.



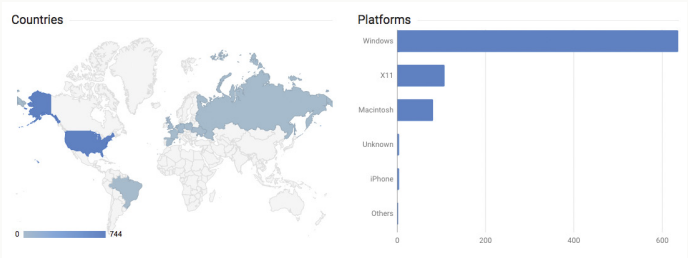
Zafiyetin 2017 Kasım ayı ortalarından beri Kuzey Kore'nin desteklediği saldırganlar tarafından kullanıldığı ve saldırganların asıl hedefinin Kuzey Kore üzerine çalışan Güney Koreli araştırmacılar olduğu ifade ediliyor. Sömürü kodu içeren Excel dokümanı çeşitli oltalama e-postaları ile bu araştırmacılara gönderiliyor. Bu dönemde zararlı kod içeren bu tür Excel dokümanları çoğu güvenlik ürünü tarafından tespit edilememiş durumda.

Zafiyet herkes tarafından bilinir hale geldikten sonra birçok grup tarafından kullanılmaya başlandı. Son olarak Türkiye'deki finans sektörünü hedef alan Hidden Cobra grubu tarafından da kullanıldı. Hidden Cobra, altkoin anlaşması konulu Sözleşme.docx isimli bir dosya ile sosyal mühendislik yöntemleri ile bu zafiyeti sömürdü. Zararlı kod içeren bu dosya açıldığında sisteme dll dosyalarını indirip çalıştırarak bu şekilde komuta kontrol merkezi ile bağlantı kuruyor.

Bu zafiyetle yapılan başka bir saldırıda da yine özel olarak hazırlanmış Word dokümanı ile kısaltılmış adresler[36] kullanıldı. Bu kısaltılmış adresler sayesinde saldırıdan hangi bölgeden kaç kişinin etkilendiği görülebiliyor. Aşağıdaki grafiklerde beş adresten sadece bir tanesine 2018 Mart ayında 840 kişinin tıkladığı ve bu kişilerin çoğunun da Windows işletim sistemi ve Internet Explorer tarayıcısı kullandığı görülüyor (Şekil 11 ve Şekil 12). Ayrıca az da olsa Avrupa ve Rusya'dan bağlanılsa da en çok bağlantı Amerika'dan gerçekleşmiş görünüyor.[36]



Şekil 11: Adobe Flash Player zafiyeti ile son dönemde yapılmış bir saldırıya ait tıklanma ve tarayıcı bilgileri



Şekil 12: Adobe Flash Player zafiyeti ile son dönemde yapılmış bir saldırıya ait ülke ve platform bilgileri

Bu tip sıfırıncı gün (0-day) açıklarından korunabilmek için sosyal mühendislik saldırılarına dikkat edilmesi, gelen e-postaların içeriğine ve gönderen adreslerine çok dikkat edilmesi ayrıca indirilen dokümanların hepsinin korumalı görünümde açılması gerekiyor. Güvenilmeyen web sitelerine girilmemesi ve alan adlarında kullanılan unicode karakterlere karşı dikkatli olunması da önem arz ediyor.

[34] https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=26998

[35] https://helpx.adobe.com/security/products/flash-player/apsa18-01.html

[36] Kullanılan kısaltılmış linkler: goo[.]gl/okCYMJ, goo[.]gl/4rHQkh, goo[.]gl/GA8sBY, goo[.]gl/H1EHRG, goo[.]gl/JnYb7s

Teknolojik Gelişmeler

Nereye Bakıyor Bu Drone'lar?

Drone'ların gerek askeri gerek sivil kullanımları giderek artıyor. Görüntü amaçlı kullanımın giderek artması paralelinde mahremiyet sorunları da ön plana çıkarıyor. Güçlü görüntü sistemleri ile donatılan drone'ların casusluk faaliyetinde kullanıldığı bir gerçek, ancak drone ve kontrolör arasındaki trafik şifreli olduğu için drone'un gerçek amacının uzaktan anlaşılması çok zor.

Protocol) adı verilen güvenli bir protokolle iletildiği gibi üzerine Wi-Fi sinyallerinin taşındığı katmanın güvenliği (WPA2) de eklenince içeriğin analiz edilmesi neredeyse imkânsız hale geliyor. Makalede anlatılan teknik ise yıllar önce geliştirilen görüntü sıkıştırma tekniklerinden bir tanesine dayanıyor. Hareketli görüntüler sabit görüntülerden çok daha fazla trafik üretiyor. Bu sebeple görüntü iletilirken her bir karenin bir önceki kareye göre farklı piksellerin yer aldığı Delta-frame adı verilen bir kare yollanıyor. Böylece sabit görüntüler çok daha az bant genişliğine ihtiyaç duyuyor. Araştırmacıların kullandığı teknik de buna dayanıyor. Şifreli trafiğin içeriği görülemese de görüntüdeki ufak değişiklikler yan-kanal analizi verilen yöntemle ayırt edilebiliyor.

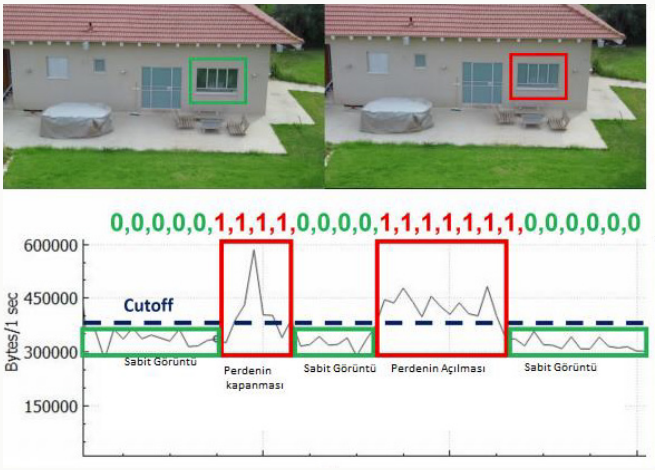
Şekil 13: Sol tarafta kırmızı kare içerisinde tespit edilen bir Dron. Casusluk amaçlı ortadaki sarı çerçeveli pencerenin görüntülenmesini ya da sağdaki mavi çerçeveli özçekim amaçlı kullanımını ayırt edebilmek mümkün mü?

Son yıllarda drone'ları tespit etme, sınıflandırma hatta uçmasını engelleme gibi yetenekler içeren anti-drone teknikleri gelişmeye devam ediyor ancak üzerinizdeki bir drone'u tespit etseniz bile yukarıdan çok büyük bir alanı gözetleyebileceğinden hedefin gerçekten siz olup olmadığını anlamanız neredeyse imkânsızdı, ta ki içlerinde RSA'in mucitlerinden Adi Shamir'in de yer aldığı Ben Gurion Üniversitesi araştırmacıları şifreli trafik üzerinden drone'ların sizi gözetleyip gözetlemediklerini anlayan yeni bir teknik geliştirene kadar[37].

Drone ve kontrolör arasındaki video trafiği FPV (First Person View) adlı kanal üzerinden iletiliyor. Aktarılan görüntü SRTP (Secure Real-Time Transport

Teknik kısaca şu şekilde özetlenebilir: Araştırmacılar drone ve kontrolör arasındaki trafiği kayıt ediyor. Standart antenlerle 45 metreden kayıt yapılabiliyor. Daha profesyonel antenlerle 1,5 km'ye kadar kayıt yapılabildiğini de belirtiliyor. Daha sonra gözetlenen pencerelerde perdeyi kaldırıp indirerek görüntüde ufak bir değişiklik meydana getiriliyor. Bu değişiklik ufak da olsa bir trafikte bir artış meydana getiriyor. Kaydedilen trafikte bu değişiklik tespit edilip (Şekil 14) drone'un gerçekten o evi gözetlediği de anlaşılmış oluyor. Bu çalışan prototipin gerekli optimizasyonlarla casus drone'ların tespiti için yüksek güvenlik gerektiren yerleşkelere uygulanacak hâle geleceği değerlendiriliyor. Ve drone'lar ile anti-drone teknikleri arasındaki savaş da olanca hızıyla devam edeceğe benziyor.

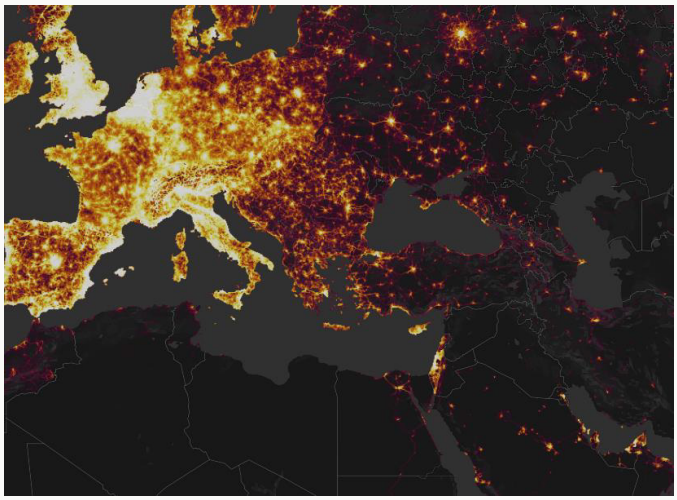
[37] Game of Drones - Detecting Streamed POI from Encrypted FPV Channel (https://arxiv.org/pdf/1801.03074.pdf)



Şekil 14: Perdenin açılıp kapanmasının trafik boyutunda yarattığı farkların tespiti

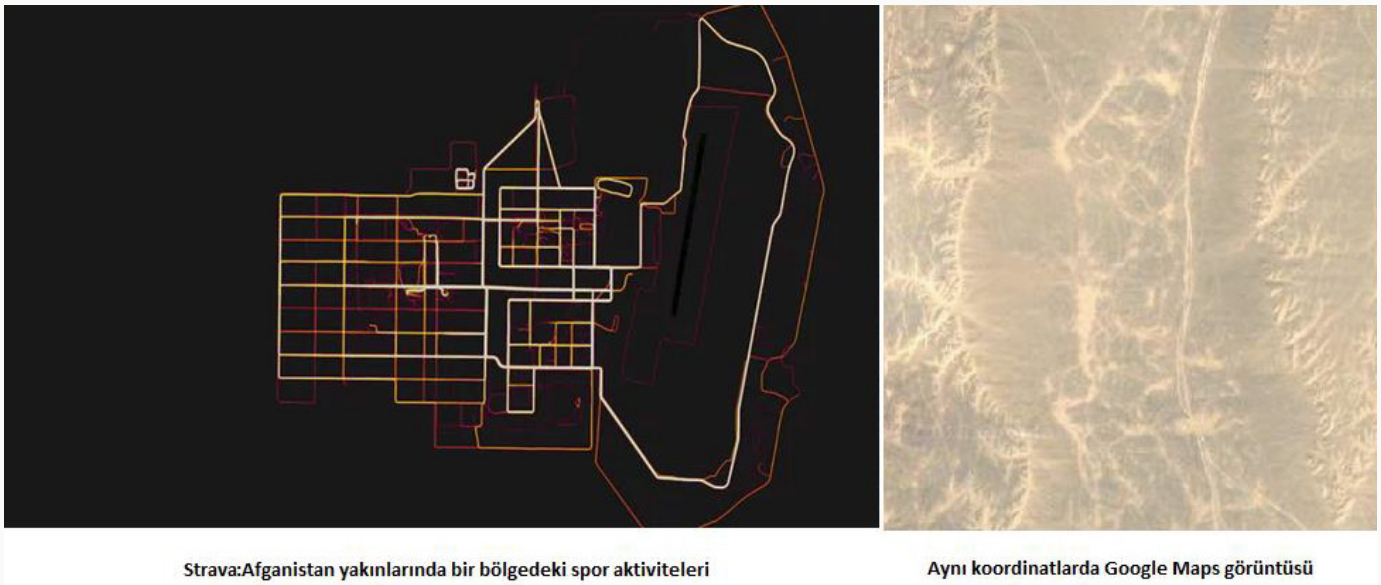
Sporcuların Isı Haritası ve Askeri Üslerin Yerleri!

Strava, koşu ve bisiklet sporları ile uğraşanların aktivitelerini paylaştığı, verilerini tuttuğu bir uygulama olarak kullanılmaktadır. Uygulama sahipleri, 2017 Kasım ayında ellerindeki verilerden elde ettiği bir dünya ısı haritası yayımladı. Üç trilyondan fazla GPS noktası içeren haritada yoğun spor yapılan alanları bulabiliyor ve spor yapan insanların izledikleri rotayı görebiliyorsunuz (Şekil 15) ancak bu verilerin bir de güvenlik boyutu var. Güvenlik analisti Tobias Schneider[38] yaptığı detaylı incelemelerde haritanın gizli askeri üslerin yerini tespit edebilecek kadar zengin bir veri içerdiğini ortaya koydu. Özellikle Amerikan ve İngiliz askerleri arasında yaygın olarak kullanılan uygulama sebebiyle Afganistan, Cibuti ve Suriye gibi bölgelerdeki üsler haritadan tespit edilebiliyor. Haritaların yayımlanmasından sonra birçok kullanıcı sosyal medyadan ilginç bulduğu aktiviteleri yayımladı.



Şekil 15: Strava ısı haritasından bir bölüm

Bir diğer örnekte de (Şekil 16) Afganistan yakınlarında tespit edilen bir aktivite yoğunluğu görülüyor. Koşu rotalarının muntazam yapısı buranın eğitim alanı vb. bir yerleşke olduğu izlenimini uyandırıyor, ancak aynı koordinatlarda Google Maps gibi uygulamalar neredeyse hiçbir şey göstermiyor. Strava, gelen tepkiler üzerine bazı aktiviteleri haritadan kaldırmış gözüküyor. Uygulama sahipleri büyük verinin işlenmesi üzerine muazzam bir iş yaptıklarını iddia ederken işin mahremiyet tarafıyla hiç ilgilenmemiş gözüküyorlar!



Şekil 16: Strava aktiviteleri

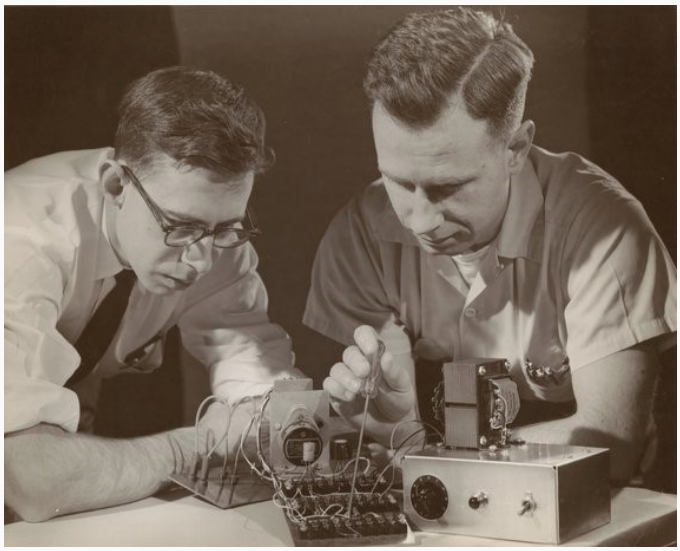
[38] https://twitter.com/tobiaschneider/status/957319340394799104

Dönem İnceleme Konusu

Yapay Zekâ ve Siber Güvenlik

Yapay Zekâ ve Makine Öğrenmesi Nedir?

Modern yapay zekânın tarihsel süreçte ilk ortaya çıkışı 1956 yılında Dartmouth Koleji'nde John McCarthy ve arkadaşları tarafından düzenlenen Yapay Zekâ Yaz Okulu olarak kabul edilmektedir.



Şekil 17: Frank Roseblatt ve Mark I makinası (1959)

Ardından Frank Rosenblatt tarafından ortaya atılan Perceptron öğrenme kuralı ve farklı şekilleri ayırt etmeyi öğrenen Mark I makinası (Şekil 17) ile önemli bir kilometre taşını aşan yapay zekâ alanındaki çalışmalar, yapay zekânın gündelik problemlerin çözümü için kullanılabileceğini göstermiştir.

Daha sonra 1960'lı yılların başında Minsky ve Peppert, Perceptron algoritmasının bazı problemleri çözmek için yetersiz olduğunu göstermiş, bu gelişme yapay zekâya olan ilginin azalmasına ve yapay sinir ağlarının önemini yitirmesine sebep olmuştur. 2000'li yılların başında üretilen veri miktarının ve işlemci kapasitesinin artmasıyla birlikte derin sinir ağlarının nesne tanıma, ses tanıma ve makine tercümesi gibi farklı problemler üzerinde ardı ardına daha önce görülmemiş başarılar sağlaması yapay zekâya olan ilgiyi tekrar körüklemiştir. Bütün bu gelişmeler yapay zekâ ve makine öğrenmesinin akademik uygulamaların yanı sıra endüstriyel anlamda ne kadar önemli olduğunu göstermesi açısından son derece dikkat çekici olmuş, dolayısıyla bu alana yapılan yatırımların artmasını sağlamıştır.

Günümüzde devletler ve şirketler yapay zekâ ve makine öğrenmesi alanlarına her geçen gün daha fazla yatırım yapmakta, yapay zekânın ekonomik anlamda yaratacağı katma değerden olabildiğince fazla pay almaya çalışmaktadırlar. Bununla birlikte yapay zekânın ekonomik getirilerinin yanı sıra teknolojik anlamda tüm dünyada çok ciddi değişikliklere yol açması beklenmektedir.

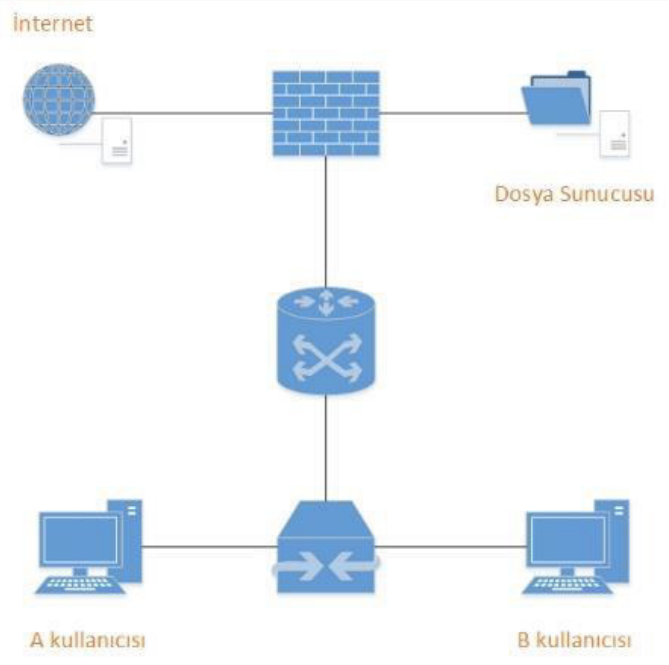
Yapay zekânın savunma, eğitim, sağlık, finans gibi pek çok farklı alanda çok büyük değişiklere yol açması, bununla birlikte bu değişikliklerin belki de en önemlilerinin bilgi güvenliği alanında yaşanması beklenmektedir. Bu kapsamda, günümüzde siber güvenlik kapsamında insan gücüne dayalı yöntemlerle gerçekleştirilen saldırıların ve savunma yöntemlerinin yerini yapay zekâ tabanlı daha güvenilir yaklaşımlara bırakacağı öngörülmektedir. Pek çok saldırının yapay zekâ temelli gerçekleştirileceği ve bunlara karşı yalnızca insan gücüyle savunma gerçekleştirmenin imkânsız hale geleceği, dolayısıyla savunma yöntemlerinin de yapay zekâ ile desteklenmesi gerektiği son derece açıktır.

Yakın zamanda bu alandaki gelişmeler yapay zekânın siber güvenlik anlamında her geçen gün daha fazla önem kazanmakta olduğunu tekrar tekrar göstermiştir. Yakın zamanda yapılan tahminler önümüzdeki beş yıl içerisinde siber güvenlik alanında yapay zekâ harcamalarının 18 milyar ABD Dolarını bulacağını öngörmektedir[39].

Yapay Zekâ ve Siber Savunma

Büyük kurumsal ortamlarda siber güvenlik faaliyetlerinin yürütülmesindeki en büyük sıkıntılardan bir tanesi yeterli operasyonel iş gücünün olmayışıdır. Aşağıdaki diyagramda

[39] https://www.cisomag.com/ai-cybersecurity-market-reach-18-2-billion-2023/



görülen oldukça ufak bir ağda iki farklı kullanıcının farklı servislere erişip birbirlerine erişememeleri isteği için bile anahtarlama (switch), yönlendirici (router) ve güvenlik duvarlarında (firewall) ayrı ayrı kurallar girilmesi gerekiyor. Hele ki tüm bu cihazların yönetimi ayrı kişi veya gruplardaysa bu işlemin operasyonel yükü çok daha ağırlaşıyor. Bu örnekten yola çıkarak siber saldırıya uğrayan çok büyük bir ağda acil olarak müdahale edilmesi gereken durumları göz önünde bulundurursak durumun vahameti çok daha iyi anlaşılabilir.

İşte tüm bu süreçleri otomatize etmek için ortaya atılan IBNS (Intent-Based Network Systems) fikri siber güvenlik dünyasını son zamanlarda heyecanlandıran gelişmelerden bir tanesidir. Konsept, özetle tüm ağ cihazlarının birbirinden haberdar olması, ağdaki kritik değişiklikleri birbirleri ile paylaşabilmesi, var olan tehditleri tanımlayıp otomatik politika girmesi ve belki de en önemlisi de çok karmaşık kurallar yerine tek cümlelik emirleri makine öğrenmesi ile tüm ağdaki cihazlarda uygulanabilecek kurallara çevirebilmesi özelliklerini taşıyor. Sistem istenen durum ile ağın güncel durumunu sürekli karşılaştırarak uygulanan kuralları matematiksel yöntemlerle doğruluyor. Yani yukarıda verdiğimiz örnekteki durumda, "A kullanıcısı sadece internete, B kullanıcısı internet ve dosya sunucusuna erişebilsin" gibi bir cümle ile komut verdiğimizde, sistem otomatikman anahtarlama cihazı üzerinde farklı sanal ağlar yaratıp yönlendirici ve güvenlik duvarında otomatik olarak kuralları giriyor. Hızla müdahale edilmesi gereken büyük çaplı saldırılarda güvenlik operatörlerinin iş yükünü önemli ölçüde alacak olan bu yöntem makine öğrenmesinin siber savunma amaçlı kullanımına oldukça iyi bir örnek olarak karşımıza çıkıyor[40].

Yapay zekâ ve siber savunmada kullanımı konusunda bir diğer örnek ise Cambridge Üniversitesi matematikçileri tarafından geliştirilip ürüne dönüştürülen ve eş zamanlı olarak ağ trafiğindeki tüm anomalileri tespit edebilen bir yazılımdır. Mevcuttaki saldırı tespit ve önleme sistemlerinin (IPS/IDS) en zayıf yanı sizi bilinen saldırılara karşı koruyabilmesidir. Bu yöntem ise ağ trafiğini izleyerek herhangi bir kural ya da imzaya bağlı olmadan "gözetimsiz makine öğrenmesi" yöntemleri ile bilinen/bilinmeyen tüm tehditlere karşı gerçek zamanlı koruma yapabiliyor. Sistem gelişmiş hedef odaklı saldırılardan içeriden yapılan kötü niyetli saldırılara kadar her çeşit saldırıyı ayırt edip önleyebiliyor. Makine öğrenmesi yöntemleri ile beraber kullanılan "Recursive Bayesian Estimation" teorisinin çok yakın gelecekte imza tabanlı IPS/IDS sistemlerinin yerine geçebileceğini söyleyebiliriz[41].

Benzer şekilde klasik imza tabanlı anti-virüslerin yerine yapay zekâ temelli çözümlerin ilk örnekleri görülmeye başlandı. Yüz binlerce zararlı yazılım örneği ile eğitilen bu sistemler, gerçek zamanlı olarak bir dosyanın zararlı olup olmadığını anlıyor. İstemci üzerinde çalışan ufak boyutlardaki bir ajan (40-60 MB) yardımıyla herhangi bir bulut ya da imza tabanlı olmayan ve tamamen izole çalışabilen bu sistemlerin bilinen ya da bilinmeyen tüm zararlılara karşı 100 ms altında bir cevap süresi ile koruma sağladığı iddia ediliyor. İmza tabanlı olmadığından dolayı herhangi bir imza güncellemesi ya da günlük tarama vs. gerektirmeyen bu sistemler klasik antivirüs sistemlerinin tespit etmekte zorlandığı sadece hafızada çalışıp diske bir veri yazmayan

[40] https://www.networkworld.com/article/3201958/lan-wan/why-ciscos-new-intent-based-networking-could-be-a-big-deal.html
[41] https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/

uygulama ve işlemleri dahi tespit edebiliyor.

Aşağıdaki testte, altı adet değişik antivirüs yüklü sistem, son sürümlerine ve imza veri tabanına güncellenmiş. Daha sonra internet bağlantıları kesilip bir hafta beklendikten sonra, o hafta ortaya çıkan yeni zararlı yazılımlar bulaştırılmaya çalışılmış. Görüldüğü üzere yapay zekâ kullanan sistem yeni zararlıları yakalamada çok daha başarılı davranıyor[42].

Yapay Zekâ ve Siber Saldırılar

Şekil 18: Yeni zararlı yazılımların yakalanma oranları

Ne yazık ki yapay zekânın sadece iyi niyetli kişilerin kullanımında olacağı oldukça iyimser bir yaklaşım olurdu. Nitekim güncel bir akademik çalışma yapay zekânın kötü niyetli kullanım senaryolarını gerçeğe bir adım daha yaklaştırdı[43]. New York Teknoloji Enstitüsü'nden araştırmacılar derin öğrenme yöntemleri ile mevcut parola kırma araçlarından çok daha verimli çalışan bir yöntem önerdiler.

GAN (Generative Adverserial Network) tabanlı yaklaşımlar ile iki farklı derin sinir ağı aynı anda eğitilmekte ve bir model gerçek gibi duran örnekler üretmeyi öğrenirken diğer bir model ise bu örneklerin gerçek olup olmadığını ayrıştırmaya çalışmaktadır. GAN tabanlı yaklaşımlar özellikle siber güvenlik anlamında saldırı ve savunma için kullanım alanı olması açısından son derece önemli bir yere sahip.

Mevcut parola kırma araçlarından "Hashcat" ve "John The Ripper" sözlük saldırısı ile parola kırabildiği gibi mevcutta kullandığı sözlüğü kullanıcı tarafından tanımlanan bazı kurallar ile genişletebilme özelliklerine sahip. Örneğin birleştirme kuralı ile sözlükte ayrı ayrı yer alan "parola" ve "123456" sözcükleriyle "parola123456" şeklinde bir parola da denenebiliyor. İyi tanımlanan kurallar ile "password" parolasından "p4s5w0rd" parolasını elde edebilmek mümkün, ancak mevcut parola kalıpları üzerinde çok yoğun araştırmalar gerekiyor[44]. İlk paragrafta bahsedilen makalede, araştırmacılar 2010 yılında sızan "RockYou" veri tabanındaki parolaların bir kısmı ile eğittikleri yapay zekâ modelinin daha sonra veri tabanının tamamının %47'sini doğru olarak üretebildiğini görmüş. Bu oran yukarıda bahsedilen insan yardımı ile girilen kurallar ile üretilen parolalardan iki katı daha başarılı gözüküyor. Şüphesiz ki eldeki veri büyüdükçe bu başarım oranı artacak ve belki de insanoğlunun kullanabileceği tüm parolalar yakın gelecekte yapay zekâ tarafından hâlihazırda biliniyor olacak.

Karşı Saldırılar

Siber güvenlikte yapay zekâ alanında son yıllarda oldukça önem kazanan bir diğer konu da makine öğrenmesi tabanlı sistemlere yapılan düşmanca saldırılardır. Bu konu yapay zekânın gündelik hayatta yoğun bir şekilde kullanılmaya başlanması ile birlikte son derece önem kazanmıştır. Özellikle derin öğrenme tabanlı yöntemlerin yaygın bir şekilde kullanılması ve pek çok sistemin bu sistemlere bağlı çalışması ile birlikte bu sistemlerin kandırılması ve kötü niyetli kullanılma ihtimali son derece düşündürücüdür. Son zamanlarda kara kutu saldırılar ile oldukça etkileyici saldırılar düzenlenebilmektedir. Örneğin yakın zamanda sınıflandırıcı tabanlı bir yapay zekâ sisteminin gördüğü silah fotoğrafını bir helikopter gibi sınıflandırması sağlanmış, bu sistemlerin güvenliğinin de tehdit altında olduğu gösterilmiştir. Bir diğer saldırı yöntemi ise makine öğrenmesi modellerine kara kutu saldırısı düzenlenerek var olan modelin ürettiği etiketlerin

[42] https://pages.cylance.com/rs/524-DOM-989/images/AV-TEST_Advanced_Threat_Prevention_Test_Report_Feb_2017_v2.pdf

[43] https://arxiv.org/pdf/1709.00440.pdf

[44] https://www.researchgate.net/publication/276113338_Cracking_More_Password_Hashes_With_Patterns

kullanılması suretiyle makinenin ne öğrendiğinin kopyalanması sağlanmış dolayısıyla bu modelin bir kopyası oluşturularak gerçek modele bu model üzerinden nasıl saldırı düzenlenebileceği ile ilgili bir zafiyet oluşturulabildiği gösterilmiştir.

Şekil 19: Fiziksel örnekler ile sınıflandırıcıların kandırılması mümkün. Sınıflandırıcı dur işareti yerine dur levhası üzerine çizilmiş şişeleri algılamaktadır.

Son yıllarda sürücüsüz araçların kullanımı giderek yaygınlaşmıştır. Önümüzdeki birkaç yıl içerisinde sürücüsüz araçların tüm dünyada giderek daha yaygın hâle geleceği öngörülmektedir. Sürücüsüz araçlara yapılacak saldırılar bu açıdan oldukça önem arz etmektedir. Yakın zamanda yapılan bir araştırmada birbirinin aynı gibi görünen "DUR" işaretlerinden birisini makinenin "DUR" şeklinde algılayabildiği, diğerini de "DEVAM" şeklinde algılayacak şekilde saldırı düzenlenebileceği gösterilmiştir[45]. Şekil 19'da da benzer bir saldırı ile sınıflandırıcının "DUR" levhasını tanımasına levha üzerine çizilen şişe resimleri ile engel olunuyor[46]. Dolayısıyla sürücüsüz aracın durması gerekirken yoluna devam etmesine sebep olmak mümkün. Bu da özellikle sürücüsüz araçların saldırganlar tarafından kandırılıp kötü niyetli şekilde yönlendirilmesine imkân sağlayabilir. Üstelik bu saldırıların önemli kısmının kara kutu saldırılar olduğu ve saldırganların yapay zekâ modellerine erişimleri olmadığının altını çizmek gerek. Saldırganların makine öğrenmesi algoritmalarının üzerinde eğitildiği verilere sahip olması ya da modelin mimarisi hakkında bilgi sahibi olması durumunda yapay zekânın nasıl karar verip hareket edeceğini öğrenip buna uygun saldırılar tasarlamak da mümkün olabilir.

Gelecekteki Olası Senaryolar ve Sonuç

Uzmanlara göre yapay zekânın kullanıldığı zararlı yazılımlar yakın gelecekte siber güvenlik dünyasının karşılaşacağı en büyük sorunlardan bir tanesi olacak. Bulunduğu ortamı anlayabilecek bu zararlı yazılımlar bir insan gibi saldırı öncesi izleme, bilgi toplama, sessiz kalma ve hatta güvenlik ürünlerini atlatma gibi kararları bulunduğu platforma göre şekillendirecek. Otonom olarak çalışacak bu yazılımlar adaptif bir şekilde bir önceki saldırının başarı durumuna göre yeni taktikler deneyebilecek. Yerleştiği ortamı sürekli izleyerek uygulamaların, cihazların ve trafik akışının davranışlarını izleyecek ve tespit edilemediği sürece daha da zeki hâle gelecekler[47]. Diğer taraftan durum o kadar da umutsuz değil. Zira savunma amaçlı yapay zekânın kullanımı artarak devam edecek. Araştırmacılar, yapay zekânın kod geliştirme ve test safhasında devreye girerek olası zafiyetleri baştan önleyebileceğini düşünüyor. Ayrıca yıllardır büyük bir sorun olan yama yönetiminde yapay zekânın kullanılmasıyla yama öncesi test işlemleri ve yamanın başka bir uygulamada sorun yaratıp yaratmayacağı gibi büyük çaba gerektiren işlerin çok daha hızlı ve sorunsuz yürümesi muhtemel olacak[48].

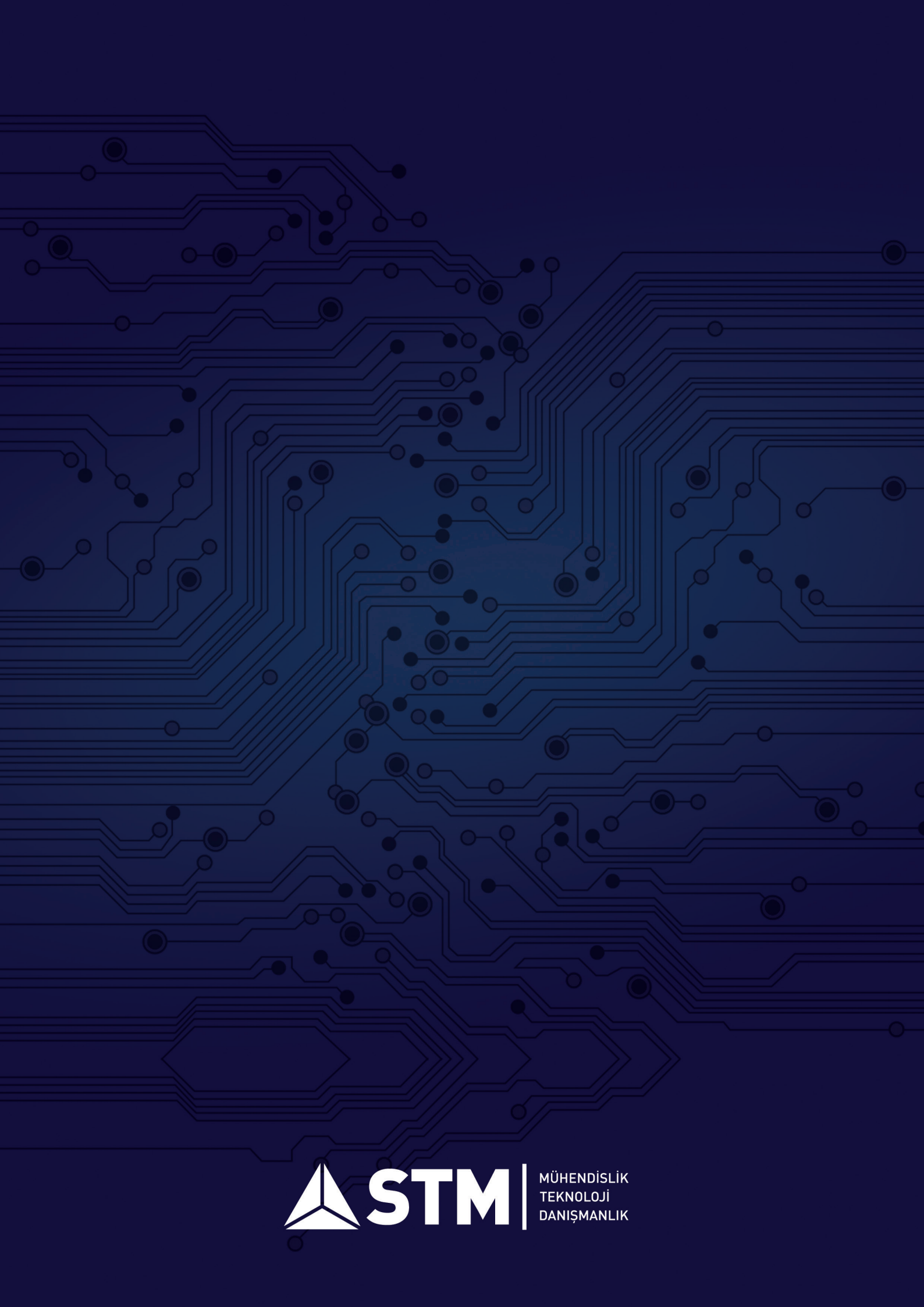
Görülen o ki yapay zekânın siber güvenlik sistemlerine entegrasyonu ve kötü niyetli kullanımı, sürekli bir bilek güreşi hâlinde olacak.

[45] Practical Black-Box Attacks against Machine Learning

[46] Note on Attacking Object Detectors with Adversarial Stickers

[47] https://www.darkreading.com/threat-intelligence/artificial-intelligence-cybersecurity-friend-or-foe-/a/d-id/1328838

[48] https://www.darkreading.com/attacks-breaches/how-ai-can-help-prevent-data-breaches-in-2018-and-beyond/a/d-id/1330263


STM
MÜHENDİSLİK
TEKNOLOJİ
DANIŞMANLIK