COVID-19 Salgını

Esnasında Gerçekleşen Sağlık Sektörü Hedefli Siber Olaylar

STM Cyber

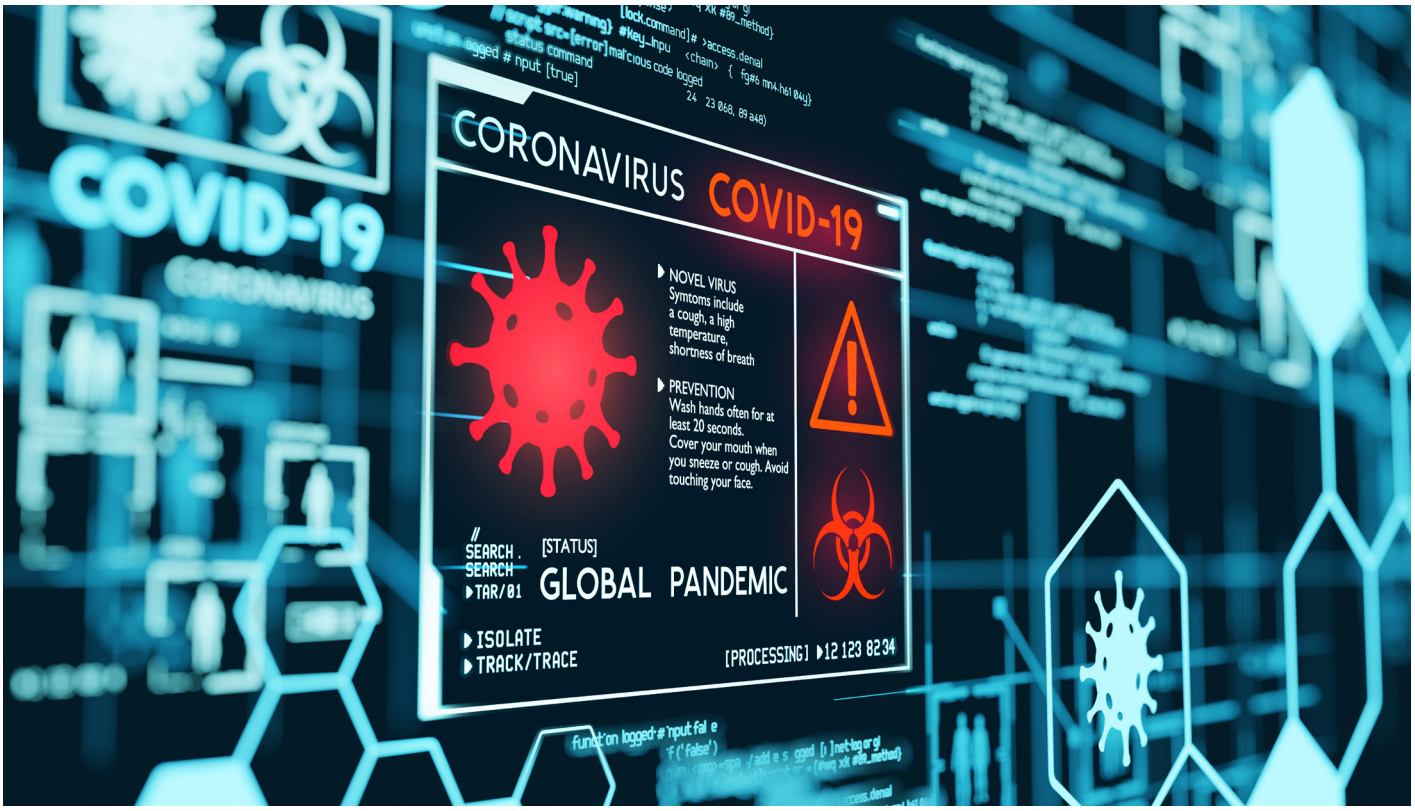
STM

COVID-19 Salgını
Esnasında Gerçekleşen Sağlık Sektörü Hedefli Siber Olaylar

Giriş

Yeni koronavirüs hastalığının (COVID-19) yayılması, birçok sektörün atak yüzeyinde eşi görülmemiş ve ani bir değişikliğe yol açmıştır. Sağlık sektöründe klinikte görev yapmayan birçok personel uzaktan çalışmaya adapte olmak zorunda kalmış ve bu durum güvenlik duruşunda zorunlu bir değişikliğe neden olmuştur. Gözlemlenen en kritik noktalardan biri de koronavirüs ile ilgili alınan yeni alan adı sayısında, üstel bir artış tespit edilmiştir ve günde birkaç bin adet yeni alan adı siber saldırılara zemin hazırlamak maksadıyla oluşturulmaktadır. Bununla birlikte tehdit aktörleri sağlık kurumlarını hem hedefleyen hem de taklit eden kampanyalar yürütmeye devam etmektedir.

Tehdit aktörlerinin COVID-19 pandemisinin etkilerinden dolaylı olarak faydalanmaya çalışacağı da değerlendirilmektedir. Bu büyük olasılıkla, kaynaklarının çoğunu pandemi ile mücadeleye yönlendiren sağlık kuruluşlarının hedeflenmesini içerecektir. Geçtiğimiz aylarda, fidye yazılımı saldırıları ve veri ihlallerinin yanı sıra kişisel verilerin (Personally Identifiable Information - PII), korunan sağlık bilgilerinin (Personal Health Information - PHI) ve yetkisiz ağ erişiminin en göze çarpan özellikleriyle sağlık hizmetlerine yönelik çeşitli tehditler gözlenmiştir. Aşağıda bu olaylardan derlediğimiz haberleri bulabilirsiniz.



Siber Olaylar

- Hammersmith Medicines Research (HMR), Londra merkezli İngiliz aşı araştırma ve geliştirme merkezine siber saldırı gerçekleşmiştir. Saldırganların (The Maze ransomware group) hedef firmanın tüm bilgisayar sistemlerini fidye yazılımları ile kapatma girişimi başarısız olmuştur. Saldırgan grup, bilgisayarları kapatma girişimlerinin başarısız olmasının ardından ilgili şirketten fidye talebinde bulunmuş, fidye ödemesi talebinin reddedilmesi üzerine şirket hastalarının kişisel ve medikal bilgilerini içeren yaklaşık 2,300 dosyayı dark webde yayınlamıştır. Bu durum söz konusu siber saldırının ilk etapta başarısız sonuçlanmış gibi görünse de aslında hedefine ulaştığını göstermektedir. Saldırgan grubunun bu girişimi COVID-19 pandemisi sırasında hiçbir sağlık kuruluşuna saldırmama sözü vermesinin ardından sadece birkaç gün sonra gerçekleştirmesi dikkat çekmektedir. HMR şirketinin BT yetkilileri sızan bilgilerin geçmiş 8-20 yıl aralığında olduğunu belirtmektedir. Sızan bilgiler; medikal anketleri, pasaport bilgilerini, sürücü belgelerini ve sosyal güvenlik numaralarını içermektedir. Saldırgan grup, girişimin şirkete 14 Mart tarihinde fidye yazılımları ile yapıldığını doğrulamıştır. [1]

- Benzer şekilde INTERPOL'ün Siber Füzyon Merkezi'ndeki Siber Suçlar Olay Müdahale ekibi, sağlık sektöründeki kilit kuruluşlara karşı yapılan fidye yazılımı saldırılarının sayısında önemli bir artış tespit etmiştir. Siber suçluların hastaneleri ve tıbbi hizmetleri sekteye uğratmak için fidye yazılımlarını kullandığı belirtilmiştir. [2]

- Dünya Sağlık Örgütü'nün COVID-19 pandemisi esnasında en çok göz önünde bulunan kurumlardan olması üzerine saldırganların ilk hedeflerinden birisi haline gelmiştir. DSÖ aldıkları saldırıların, COVID-19 krizinin başlamasından bu yana 2 katından fazlasına çıktığını belirtmiştir. DarkHotel adındaki saldırgan grubu DSÖ çalışanlarına giriş (login) ekranı gibi görünen oltalama sayfaları göndererek şifre çalma girişiminde bulunmuşlardır fakat bu girişim başarısız olmuştur. [3]

- Çek Cumhuriyeti'nin sahip olduğu en büyük COVID-19 test merkezlerinden birisi olan Brno University Hospital 12 ve 13 Mart tarihlerinde aldığı büyük bir siber saldırı sonucunda tüm bilgisayar sistemlerini acil kapatma kararı almıştır. Alınan bu karardan sonra sisteme yeni kayıt girişi yapamayacakları için hastane yönetimi yeni gelen tüm hastaları başka hastanelere yönlendirmek zorunda kalmıştır. Aynı şekilde hastane içerisindeki tüm ameliyatlar bu sebeple iptal edilmiştir. Sağlık çalışanları hastalarla ilgili tüm notları manuel olarak yazmaya ve hastane içinde iletmeye başlamışlardır. Bu durumun süreçleri çok yavaşlattığı ve dolaylı yoldan hastaların hayatını tehlikeye attığı belirtilmektedir. [4]

- Amerikan Sağlık ve İnsan Hizmetleri Departmanı (The U.S. Department of Health and Human Services – HHS) COVID-19'a karşı verdiği mücadeleyi yavaşlatmak ve halka yanlış bilgi ve haberler yayılmasını amaçlayan, ciddi yoğunlukta siber saldırı aldığını belirtmektedir. HHS sözcüsü Caitlin Oakley yaptığı açıklamada, siber güvenlik sistemlerine yapılan saldırıların, tehdit ve zafiyetleri tespit etmek amacıyla risk tabanlı olarak sürekli izlendiğini ve son günlerde alınan saldırı sayılarında ciddi miktarda artış olduğunu belirtmiştir. Bu sebeple BT birimlerinde bu süreç için ekstra güvenlik önlemleri hazırladıklarını ve tümleşik yapıyı koruyacaklarını açıklamışlardır. Aynı zamanda bu süreç içerisinde dağıtılan sahte haberleri yalanlamak adına Ulusal Güvenlik Konseyi (National Security Council – NSC) resmi Twitter hesabından bir açıklama yapmıştır. Bahsi geçen tweet içeriğinde halk arasında mesaj yoluyla yayılan ulusal karantinaya gidileceği yönünde söylenti ve yazıların sahte olduğunu, ulusal bir karantinanın söz konusu olmadığını belirtmektedir. [5]

- Facebook'ta bulunan National Cyber Security Services grubunda paylaşılan bir bilgide tehdit aktörlerinin, yönlendiricilerin (router) DNS ayarlarını ele geçirip değiştirerek zararlı COVID-19 uygulamalarını yaydıklarını tespit ettiklerini belirtmişlerdir. Bunun COVID-19 esnasında çıkan yeni bir siber saldırı tipi olduğunu ve web tarayıcıların sahte olan COVID-19 uygulamalarına karşı uyarılar verdiğini göstermişlerdir. Bu uygulamaların genellikle Dünya Sağlık Örgütü tarafından sunuluyormuş gibi gösterilip aslında tehlikeli bir kişisel veri çalma yazılımı olan "Oski Information-stealing malware" olduğu belirtilmektedir. Bu zararlı yazılım çalıştığında kurbanın bilgisayarındaki tarayıcı çerezlerini, tarayıcı geçmişini, tarayıcı ödeme bilgilerini, kaydedilmiş giriş kimlik bilgilerini (şifreler dahil), kripto para cüzdanlarını, metin dosyalarını, tarayıcı otomatik doldurma bilgilerini, Authy iki faktörlü kimlik doğrulama veri tabanlarını çalmak ve uygulamaya zararlı bulaştığı sırada masaüstünün bir ekran görüntüsünü almak gibi risk derecesi çok kritik olan işlemleri gerçekleştirebilmektedir. Facebook grubu kendi kullanıcılarını bu tehdide karşı uyarmıştır. [6]

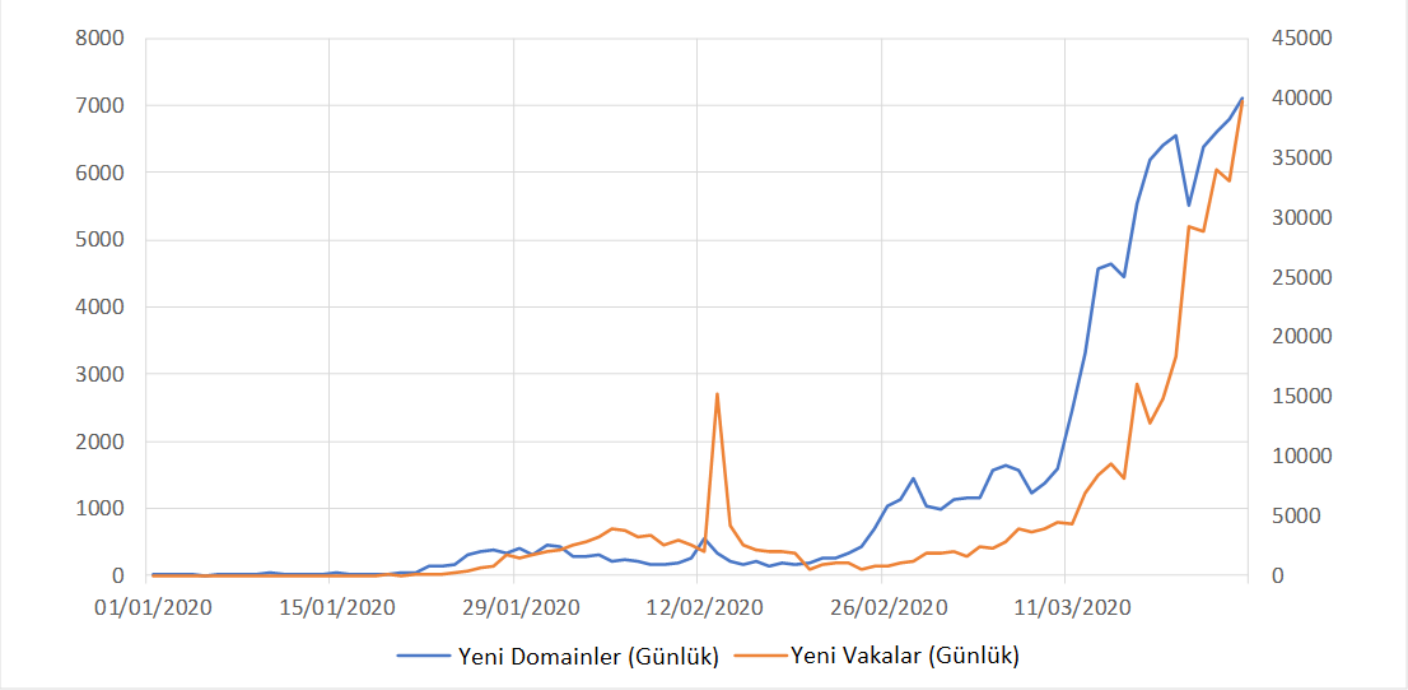
- Hizmet tabanlı servis (Access-as-a-service) olarak çalışan bazı siber suç gruplarının Emotet zararlı yazılımını kullanarak hedef kuruluşlara ağ erişimi sağladıkları görülmüştür. Aynı şekilde zararlı fidye yazılımı kullanan grupların "Sodinokibi" ve "Ragnarok" gibi bazı zararlı yazılımların sanal özel ağ (VPN) ürünlerindeki zafiyetleri kullanarak ağlara ilk erişim sağladıkları tespit edilmiştir. Güncel durumda sayıları ciddi miktarda artmış olan uzaktan çalışan ve klinikte yer almayan sağlık çalışanlarının bu VPN ürünlerini kullandıkları düşünülerek saldırganlar tarafından hedef alındıkları öngörülmektedir. Saldırganların bu VPN uygulamalarındaki zafiyetleri kullanarak ilk erişimi sağladıktan sonra domain kontrolörüne erişimi amaçladıkları, ardından fidye yazılımları kurmayı amaçladıkları tespit edilmiştir. Bunun için açık kaynaklı zafiyet-istismarı sonrası araçları olan Powershell Empire, Cobalt Strike ve PSExec gibi bazı sistem yöneticisi araçlarını kullandıkları görülmüştür. Bu bağlamda tespit edilen 4 tane aktif C2 (Command and Control) sunucusunun yüksek ihtimalle sağlık sektörünü hedef alan Cobalt Strike ve Powershell Empire kullanan alan adları mevcuttur.

Tablo 1'de bu potansiyel C2 sunucularının adreslerini ve alan adlarını bulabilirsiniz. Bu bilinen suç örgütlerinin dışında bazı tehdit aktörlerinin COVID-19 esnasında ağ erişimi sattığı tespit edilmiştir. 12 Mart 2020 tarihinde "wazawaka" isimli tehdit aktörü yaklaşık gelirinin 2 milyar dolar olduğunu belirttiği ve spesifik olarak adını vermediği bir özel Amerikan sağlık kuruluşuna erişim sattığını söylemektedir. Aynı şekilde "JamBou" isimli tehdit aktörünün içerisinde 1,900 Amerikan sağlık personelinin kişisel verilerinin bulunduğu veri tabanını 8 Şubat 2020 tarihinde satışa sunduğu görülmüştür.

IP	Araç Ailesi	Alakalı Alan Adı
54.157.197[.]203	Cobalt Strike	plasticsurgeryall[.]com
54.188.166[.]98	Cobalt Strike	bannerhealhcare[.]com
3.89.128[.]232	Cobalt Strike	mothershiphttp.manipayhospital[.]org
63.142.252[.]21	Powershell Empire	saintmarys-reno[.]com

Tablo 1 Sağlık sektörünü hedefleyen potansiyel C2 sunucuları

COVID-19 süresince tespit edilen koronavirüs ile alakalı yeni alınan alan adlarında ciddi bir artış görülmektedir. Bu alan adları tehdit aktörleri tarafından hızlıca yayılmaktadır ve COVID-19 ile alakalı kötü amaçlı bir ortam yaratılmaya çalışılmaktadır. Bu bağlamda günlük olarak yaklaşık 6,000 koronavirüs bağlantılı alan adı kaydı gözlemlenmiştir. Bu sayı Şubat ayının başından bu yana onaylanan vaka sayısının artışıyla doğru orantılı olarak artmaktadır ve koronavirüs bağlantılı alan adları ile vaka sayılarının arasında güçlü bir ilişki tespit edilmiştir. Şüpheli alan adları kullanılarak sağlık sektörüne gerçekleştirilen bazı saldırılar aşağıda listelenmiştir.



- 20 Mart 2020'de abuse.ch görevlileri DSÖ (Dünya Sağlık Örgütü)'ne Nanocore RAT (Remote Access Trojan) zararlı yazılımı göndermek amacıyla yapılan saldırıyı tespit etmişlerdir.
- Aynı şekilde Public Health Agency of Canada'ya Ursnif zararlı yazılımı ile saldırılmaya çalışılmış ve ABD Sağlık Departmanı'na DanaBot zararlısı kullanılarak koronavirüs haritası e-posta aracılığıyla gönderilmiştir.
- 13 Mart 2020 tarihinde Vancouver General Hospital'da COVID-19 temalı kimlik çalma girişimi tespit edilmiştir.
- 11 Mart 2020 tarihinde e-posta sahteciliği (spoofing) kullanılarak, sağlık teknolojisi şirketi olan CipherHealth'in e-posta hesaplarından DSÖ'ye oltalama mailleri gönderilmiştir. E-posta içerisinde bulunan CipherHealth alan adı bağlantısının stpl.ca bağlantısına kimlik bilgileri çalma amacıyla doğrudan yönlendirildiği tespit edilmiştir.
- 16 Mart 2020 tarihinde kullanıcılardan bilgisayarlarını COVID-19'a karşı tedavi geliştirilme sürecinde işlem gücü bağışlamayı teklif eden "Folding@home" projesinin altında RedLine Stealer zararlısı olan bir kandırmaca olduğu tespit edilmiştir.
- 23 Mart 2020 tarihinde ABD'nin Sağlık ve İnsani Hizmetler Departmanı (HHS)'nın web sayfası olan hhs.gov üzerinden saldırganlar açık yönlendirmeyle hesaplara oltalama e-postaları göndermişlerdir. Bu e-postaların içinde bulunan bağlantı ile indirme yapan kişilere Raccoon Stealer zararlısı yüklendiği tespit edilmiştir.

- Türkiye'yi hedef alan odaklı saldırılarda kullanılmak üzere alınmış bazı alan adları tespit edilmiştir. Bunların tamamının oltalama amaçlı kullanıldığı ile ilgili bir kanıt olmasa da potansiyel riskli olarak değerlendirilmiştir. Ayrıntılar **Tablo 2**'de belirtilmiştir.
- 12 Mart 2020 tarihinde KrebsonSecurity isimli firma, Johns Hopkins Üniversitesi tarafından yapılan COVID-19 takip haritalarının saldırganlar tarafından kötüye kullanıldığını tespit etmiştir. Reason Security ve MalwareBytes şirketleri de kötüye kullanılan bu sitelerde AZORult zararlı yazılımını tespit etmişlerdir. İnternet üzerinde listelenen COVID-19 takip haritalarının web sitelerine gömülen bu zararlı yazılımın sayısının oldukça yüksek olduğu görülmüştür.

Alan Adı	Kayıt Tarihi	Durumu	Kara Liste
coronavirusturkiye.net	2/1/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkiye.blog	3/16/2020	Kullanılmıyor	Listelenmemiş
coronavirus-turkey.ru	4/4/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkiye.website	2/26/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkey.xyz	4/12/2020	Şüpheli	Listelenmiş
coronavirusturkiye.online	2/26/2020	Kullanılmıyor	Listelenmemiş
coronavirus-turkey.online	4/4/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkiye.xyz	2/1/2020	Kullanılmıyor	Listelenmemiş
coronavirusuturkiye.xyz	2/27/2020	Kullanılıyor – COVID-19 Haritası – Şüpheli	Listelenmemiş
coronavirus-v-turkey.online	4/5/2020	Kullanılıyor Şüpheli	Listelenmiş
coronavirus-v-turkey.ru	4/5/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkey.site	4/12/2020	Kullanılıyor – Boş Sayfa – Şüpheli	Listelenmiş
coronavirusturkiye.site	3/15/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkey.club	4/12/2020	Kullanılıyor – Boş Sayfa – Şüpheli	Listelenmiş

Tablo 2 Olası oltalama sayfaları (Türkiye)

Sonuç

Tehdit aktörleri COVID-19 pandemisinden hem doğrudan kimlik avı dolandırıcılığı, hem de zararlı yazılımları ve sosyal mühendislik taktiklerini kullanarak faydalanmaktadır. Sağlık sektörü, bu tehditlerin son dönemde birleştiği noktadır. Devlet destekli bazı tehdit aktörlerinin de özellikle aşı ve ilaç şirketlerini hedef alıyor olması da konunun ulusal bir tehdit olarak değerlendirilip önlemlerin bu çerçevede alınmasını gerektirmektedir.

Bu süreçte hastalık ile ilgili verilerin, ulusal ve uluslararası makamların resmi web sitelerinden takibi sağlanmalı ve bunun haricindeki kaynaklara şüpheli gözüyle bakılmalıdır. İndirilen uygulamalarda da benzer şekilde davranılmalı ve güvenilir kaynaklar haricinde indirme işlemi yapılmamalıdır. Son kullanıcıların dikkat etmesi gereken bir diğer konu ise medikal ürün dolandırıcılığıdır. Açılan sahte e-ticaret sitelerinden yapılacak alışverişlerde kredi kartı bilgilerinin çalınması dâhil birçok risk ile karşı karşıya olunduğuna dikkat edilmelidir. Bundan dolayı yapılacak alışverişlerde güvenilir kaynaklardan alışveriş yapılmalı ve web sitesine güvenli bağlantı yapıldığından emin olunmalıdır. Kurumlar uzaktan çalışma sürecinde benzer tehditlerden korunma amacıyla uzak bağlantı için kullandıkları yöntemlerin güvenlik durumunu gözden geçirmeli ve çok faktörlü doğrulama mekanizmalarından yaralanmalıdırlar.

Bu raporda tanımlanan tehditleri azaltmak ve ortaya çıkan yeni tehditlerden haberdar olabilmek için STM Siber Füzyon Merkezi hizmetleri kapsamında sağlanan tehdit istihbaratları ve tehlike göstergelerinin (Indicators of Compromise - IoC) takip edilmesini önermekteyiz.

Kaynakça

[1]	B. Goodwin, «Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack,» ComputerWeekly, 22 03 2020. [Çevrimiçi]. Available: https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus. [Erişildi: 01 04 2020].
[2]	«Cybercriminals targeting critical healthcare institutions with ransomware,» Interpol, 04 04 2020. [Çevrimiçi]. Available: https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware. [Erişildi: 07 04 2020].
[3]	N. Eddy, «WHO, coronavirus testing lab hit by hackers as opportunistic attacks ramp up,» 24 03 2020. [Çevrimiçi]. Available: https://www.healthcareitnews.com/news/who-coronavirus-testing-lab-hit-hackers-opportunistic-attacks-ramp. [Erişildi: 01 04 2020].
[4]	S. Porter, «Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak,» HealcareITNews, 19 03 2020. [Çevrimiçi]. Available: https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak. [Erişildi: 01 04 2020].
[5]	M. Miliard, «UPDATED: HHS fends off cyberattack as it fights coronavirus,» HealtcareITNews, 16 03 2020. [Çevrimiçi]. Available: https://www.healthcareitnews.com/news/updated-hhs-fends-cyberattack-it-fights-coronavirus. [Erişildi: 01 04 2020].
[6]	«#Hackers Hijack Routers' #DNS to Spread #Malicious #COVID-19 Apps.,» National Cyber Security Services, 30 03 2020. [Çevrimiçi]. Available: https://www.facebook.com/ncybersec/posts/1447748678729185?__xts__%5B0%5D=68.ARD3W-G7M1XszDItuE61LoNUrLgA5Tk6mDfrc73NwBHH5tMHQ9J4tkLY3upZEFnRZ6QzghXDiChbQg66VMyTh0Y-W4DKD6uTd8mQ54IYK-K8PMIDcGV0C9tnSI5F7lpQWN9ZBWqcWdb81Drpindmclr3wEdzLrmS83a9tWRuQlOOTyQ-5w_V. [Erişildi: 01 04 2020].