DİJİTAL CORONA VİRÜS SİBER TEHDİT İSTİHBARATI İNCELEME RAPORU

19 MART 2020

Dijital Corona Virüs Tehlikesi

Dünya Sağlık Örgütü tarafından pandemi ilan edilen Corona virüsü salgını, insan sağlını etkilediği gibi siber dünya üzerinde dijital sağlığı da etkilemektedir. Corona virüsü haberlerini ve verilerini takip etmek için erişilen internet siteleri, mobil uygulamalar ve masaüstü uygulamalarının bazı örnekleri üzerinde zararlı yazılımlar tespit edilmiştir. Saldırganlar sosyal mühendislik saldırılarında da Corona virüsünden beslenmekte kullanıcıların korku ve heyecan duygularını sömürmektedirler.

Güncel saldırı trendleri arasında bulunan bu durum, güncel zafiyetlerle birleştirildiği durumlarda kişileri ve kurumları zor durumda bırakmaktadır. Güvenilir olmayan kaynaklardan indirilen masaüstü uygulamaları ve mobil uygulamalar vasıtası ile saldırganlar, tüm dünyanın dikkatini toplayan Corona virüs tehlikesinden beslenmektedir.

Corona Virüsü Temalı Zararlı Aktiviteler

Tespit edilen zararlı Corona virüs bilgilendirme web sitelerinin oluşturdukları ağ trafiğinin şüpheli ve zararlı olduğu görülmüştür. Tespit edilen bazı zararlı erişimler aşağıdaki gibidir.

- https://www.corona-virus-map[.]com
- http://coronavirusstatus[.]space/index.php
- https://coronavirus.jhu[.]edu/map.html

Gerçekleştirilen zararlı yazılım analizlerinde de pek çok çalıştırılabilir dosyanın oluşturduğu ağ trafiğinin şüpheli ve zararlı olduğu görülmüştür. Tespit edilen bazı çalıştırılabilirler aşağıdaki gibidir.

Çalıştırılabilir	**Hash Bilgisi**
COVID-19.exe	3633965b6d851f19323b4611e3cbf2408913eb57
GEE CustomersUpdate English Corona 27022020.exe	583f8d29f74f3573181c7514bf1964713f1befbe
FYR_COVID-19.exe	9de3c125694a4395ba120eb555748dd413d792a2
MEDIDAS PREVENTIVAS FRENTE COVID-19.exe	e7ec45dfec38b6771798c9922710df58aa6779bc
Coronavirus (COVID-2019) Safety Measures(2).exe	f058c9ef504284220d39f272e21a85096c46457a
Corona (2)_protected.exe	6570FF5682C334D86E9650DC0241F6EC
Corona-virüs-Map.com.exe	73DA2C02C6F8BFD4662DC84820DCD983
UNICEF COVID-19 APP.exe	E33CA6E0EC223D2B3E958131424EFF4A

İlgili çalıştırılabilir çoğu şüpheli ve zararlı adresler ile iletişim kurduğu ya da güvenli olmayan işlemler gerçekleştirdiği görülmüştür.

Mobil Tehdit: CovidLock

Gerçekleştirilen istihbarat çalışmaları sonucu zararlı fidye yazılımı ile saldırı gerçekleştirilen hacker gruplarının da corona virüsü temasını kullanmaya başladıkları tespit edilmiştir. İşletim sistemlerini hedef alan bu zararlı aynı zamanda mobil telefonları da hedef almaktadır.

Bu tür güncel ve kritik olaylar sırasında kişiler çeşitli korku ve heyecan duygularına kapılmakta ve dikkatleri dağılmaktadır. Kullanıcıların özellikle mobil telefonlarına yükledikleri bazı zararlı mobil uygulamalar sonucu telefondaki veri ve bilgilerinin şifrelenerek fidye istenmesine maruz kaldıkları görülmüştür.

APT ve Dijital Corona Virüsü

Gerçekleştirilen istihbarat çalışmaları sonucu APT36 kampanyasının Corona virüsü temasından da beslendiği görülmüştür. APT36'nın esas olarak Hindistan savunma sanayi, Hindistan hükümetini ve büyükelçiliklerini hedefleyen Pakistan destekli bir tehdit aktörü olduğuna inanılıyor. APT36'nın 2016 yılından itibaren siber espiyonaj düzenlediği düşünülmektedir.

Tespit edilen saldırılar sırasında Corona Virüs temalı sosyal mühendislik saldırılarının düzenlediği ve bu saldırılar sırasında, zararlı makro içeren excel dosyalarının kullanıldığı görülmüştür. "Sağlık Önerisi: Corona Virüs" başlığı ile görüntülenen dosya içerisinde çalışan makro sonrası istemciye CrimsonRAT adı verilen bir RAT varyantı indirildiği ve ilgili RAT zararlısının uzaktan kontrol için kullanıldığı tespit edilmiştir.

Çalışan zararlının aşağıda verilen C2s'ler ile iletişim kurduğu görülmüştür. İlgili dokümanların ve RAT zararlılarının hash bilgileri, C2s bilgileri ile aşağıda verilmiştir.

Zararlı dokümanlar

- 876939aa0aa157aa2581b74ddfc4cf03893cede542ade22a2d9ac70e2fef1656
- 20da161f0174d2867d2a296d4e2a8ebd2f0c513165de6f2a6f455abcecf78f2a

Crimson RAT

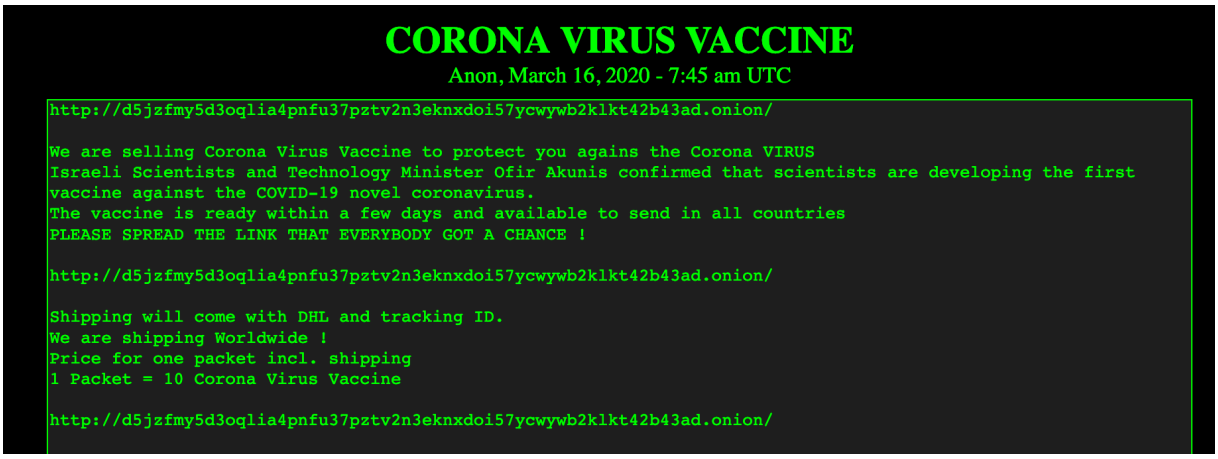
- 0ee399769a6e6e6d444a819ff0ca564ae584760baba93eff766926b1effe0010
- b67d764c981a298fa2bb14ca7faffc68ec30ad34380ad8a92911b2350104e748

C2s

- 107.175.64[.]209
- 64.188.25[.]205

DeepWeb ve Corona Virüsü

DeepWeb üzerinde yapılan araştırmalar sonucu, internetin görülmeyen yüzünde bulunan forum siteleri ve "paste" sayfaları üzerinde de Corona Virüsü ile ilgili sahte kampanyalar görülmüştür. Corona Virüsü aşısının satıldığını, bir paket içerisinde on adet aşının bulunduğunu ve dünyanın her yerine kargo ile gönderilebileceğini iddia eden kişiler DeepWeb gibi platformlarda bulunuyorlar.



Sahte olan bu haberler vasıtası ile bu platformlardaki kişileri hedef alan saldırganlar sosyal mühendislik yapmaktadırlar. Oluşturdukları sahte kampanyalar vasıtası ile kurbanlarından belirli bir parayı bitcoin karşılığında almakta ve ortadan kaybolmaktadırlar.

Bu ve buna benzer birden fazla konu ve başlığın çeşitli DeepWeb sayfalarında bulunduğu görülmüştür.

Dijital Corona Virüsüne Karşı Alınabilecek Önlemler

Kullanıcılar, son günlerde önemli bir durum haline gelen Corona virüsü ile ilgili haber ve bilgilerine ulaşırken dikkatli olmalıdırlar. Böyle bir saldırı karşısında kullanıcılar aşağıdaki işlemleri yapmalıdırlar.

- Spam e-maillere dikkat edilmelidir.
- Buton / Link'in kaynağı incelenmelidir, indirilen dosyalar güvenlik taramalarından geçirilmelidir.
- Masaüstü ve mobil uygulamalar güvenilir kaynaklardan temin edilmelidir
- Zararlı e-posta tespitinde kullanıcıların IT birimine derhal şüpheli e-postaları bildirmeleri gerekmektedir. E-Posta hakkında kurum çalışanlarına bilgilendirme yapılmalıdır.

Kişilerin yanı sıra kurum ve kuruluşlar da bu tür saldırılara karşı dikkatli olmalıdırlar, kurumların alabileceği benzer önlemler aşağıdadır.

- Ağa dahil olan tüm bilgisayarların olası bir zararlı yazılım senaryosuna karşı anti virüs imza veri tabanlarının her zaman güncel tutulması önemlidir.
- Sunucuların spam filtrelerinin kontrol edilmesi, düzenlenmesi, spoofing vb. metotlara karşı hazırlıklı olunması gerekmektedir.
- Kurum çapında, kullanıcılara farkındalık eğitimleri verilmeli ve bilgilendirme e-postaları atmalılardır.


CATCH PROBE
Security Intelligence Center Orchestration
CYBER
THREAT
INTELLIGENCE
PLATFORM
www.catchprobe.com
www.intelprobe.com.tr
info@intelprobe.com.tr
Adres :
Mutlukent Mah.
Fesleğen Sk. No:9
Çankaya - ANKARA
Tel :
+90 312 225 10 93
Fax:
+90 312 225 10 99
INTEL
PROBE
INTELLIGENCE & ANALYTICS