Covid-19 Aşı Geliştirme Çalışmalarına Yönelik Siber Tehditler

STM Cyber

STM

Dünya çapında halihazırda 900.000'den fazla kişinin ölümüne neden olan ve günlük hayatı alt üst eden koronavirüse karşı bir aşı geliştirmek için yoğun bir uluslararası yarış sürüyor. 155'ten fazla kurum, özel şirket, üniversite aşı geliştirme aşamasında ve aşılar yavaş yavaş insanlar üzerinde test edilmeye başlandı. Bazı aşılar, insanları hasta etmeden bir bağışıklık tepkisi oluşturmak için koronavirüsü taklit edecek başka bir yaygın virüsü değiştirerek çalışıyor. Oxford ve AstraZeneca'nın araştırması, koronavirüsü taklit eden bir patojene dayanıyor. Rusya Sağlık Bakanlığının da, bu patojeni taklit edecek bir aşı üzerinde çalışmakta olduğu ve testlerin Oxford araştırmacıları kadar ileri düzeyde olmadığı da ABD basınında yer almaktadır[1].

Amerikan, İngiliz ve Kanada hükümetleri, bilgisayar korsanlarının koronavirüs aşısı araştırmasını çalmaya çalıştıklarını iddia etmişlerdir. Amerika'da 2016 yılında Demokrat Parti 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.

1- https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html

Cozy Bear tehdit aktör grubunun, kötü amaçlı yazılım kullanarak aşı geliştirmekte olan devlet ve ona bağlı kuruluşları hedef aldığı iddia edilmektedir. Saldırının kurum çalışanlarının parolalarını ve diğer kimlik bilgilerini ele geçirmek için kandırmaya yönelik sahte e-postalar göndererek (phishing ve spear phishing) aşı araştırmasına ve tıbbi tedarik zinciriyle ilgili bilgilere erişim sağlamak için yapıldığı düşünülmektedir. Bunlara ek olarak Cozy Bear grubunun elinde bulunan belli başlı statik IP'lere zafiyet taraması yaptığı ve bulduğu açıklıkları sömürme çalışmaları yaptığı da 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 sömürülerinden sonra saldırganlar tarafından ele geçirildikleri düşünülen parolalar ile ilgili kuruluşların ağlarına sızılarak WellMess ve WellMail zararlılarının çalıştırılması şeklinde gerçekleştirildiği değerlendirilmiştir. Söz konusu zararlıların içinde bulundurdukları zararlı kodlar ile uzaktan komut çalıştırma yeteneğine, veri alma ve gönderebilme 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 üretir. Ürettiği anahtarlar, sisteme yine şifrelenmiş çalıştırılabilir dosyaları çalıştırmak için kullanılır. WellMail zararlısı ise çalıştırılabilir dosyalar ile edinilen veriyi şifreli bir biçimde komuta kontrol sunucusuna aktarır[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, 953b5fc9977e2d50f3f72c6ce85e89428937117830c0ed67d468e2d93aa7e-c9a, e329607379a01483fc914a47c0062d5a3a8d8d65f777fbad2c5a841a90a0af09, fd3969d32398bbe3709e9da5f8326935dde664bbc36753bd41a0b111712c0950, 47cdb87c-27c4e30ea3e2de620bed380d5aed591bc50c49b55fd43e106f294854
Dosya özet bilgileri (MD5)	861879f402fe3080ab058c0c88536be4, 3a9cdd8a5cbc3ab10ad64c4bb641b41f, 4d38ac3319b-167f6c8acb16b70297111, f18ced8772e9d1a640b8b4a731dfb6e0, 2f9f4f2a9d438cdc944f79bd-f44a18f8, 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

WellMail[4]:

İçerdiği dosya sayısı	2
Dosya İsimleri (aynı zamanda SHA256 bilgisi)	0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494 83014ab5b3f63b-0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18
Dosya özet bilgileri (MD5)	01d322dcac438d2bb6bce2bae8d613cb 8777a9796565effa01b03cf1cea9d24d
Bağlantı kurduğu IP adresleri	119.81.184.11

2- https://www.pharmaceutical-technology.com/features/covid19-ncsc-russian-cyber-attack/
3- https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198b
4- https://us-cert.cisa.gov/ncas/analysis-reports/ar20-198c

Cozy Bear grubunun yaptığı saldırılar 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, kurum bilgilerinin ele geçirilebilir olabileceği tespit edilmiştir[5].

Cozy bear tehdit aktör grubunun hedefinde olan bir diğer ülke İngiltere'de ise, İngiliz istihbarat teşkilatı eski başkanı Robert Hannigan, saldırıların birincil hedefinin İngiltere'deki Oxford Üniversitesi ve aşı üzerinde ortaklaşa 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, bir klinik araştırmayı finanse etmek ve 300 milyon dozu güvence altına almak için AstraZeneca'ya 1,2 milyar dolara kadar ödeme yapacağını belirtmiştir.

5- https://www.helpnetsecurity.com/2020/07/17/biomedical-cyber-attacks/

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 yapılan aşı çalışmalarında elde edilen bilgiler, formüller, çıktılar vb. daha nice verilerin saklandığı ortamların güvende tutulması gerekir. Yapılan araştırma aslında koronovirüs nezdinde çalışan firmalar için geçerli olsa da dünyada birçok kurumun bu ve bunlara benzer zafiyetleri bulunmaktadır. Kusurların önüne geçilmesi için şirketlerin tamamı personelini bilgi güvenliği alanında eğitime tabi tutmalı ve özellikle oltalama (phishing, spear phishing) konularında farkındalığı arttıracak eğitimler ve programlar oluşturmalıdır. Tabi buna şirketin BT departmanında çalışan kişiler de dahildir. Güvenlik duvarında yapılandırılmış yanlış bir politika ile kritik sunucu ve servisler, istenmeden de olsa internetten erişilebilir ve saldırganların hedefi haline gelebilir. Sınır güvenliğinin etkin bir şekilde sağlanması için erişim yetkileri, güvenlik cihazlarının konfigürasyonlarının kurum politikalarına göre yapılandırıldığı belli aralıklar ile test edilmelidir. Güvenlik duvarında uygulacak ağ segmentasyonu ile de kurumun ağ güvenliği arttırılmalıdır. 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 de azaltacaktır. İş sürekliliğinin sağlanması için önemli sunucular ve güvenlik cihazları yüksek erişebilirlik ile 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 da yüklenmesi, bu yazılımların güncel tutulması da bilinen zararlılara karşı önemli bir savunma sağlayacaktır.

Kurumun güvenlik altyapısının ve gerçekleşen olayların sürekli izlenmesi, Siber Tehdit İstihbaratı 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 çok büyük ölçekte korunabilecektir.