Elm və İnnovativ Texnologiyalar Jurnalı
https://doi.org/10.30546/2616-4418.31.2024.1054
Nömrə 31, 2024. 54-69
http://www.ejsr.org

XXI. YÜZYILDA GÜVENLİK MESELESİ VE SİLAHLAR: STUXNET

Alper ASLAN
Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Avrupa Birliği Bölümü, Avrupa Çalışmaları Doktora Programı, İzmir, Türkiye

0000-0002-2191-5299

Giriş

Günümüzde insanlar, şirketler ve hatta devletlerin internete olan bağımlılığının artmasıyla birlikte, siber uzay potansiyel risk sahasına dönüşmüştür (Hatipoğlu 158). Görünen o ki geleceğin dünya savaşları siber uzayda başlayacaktır. Bu nedenle devletler; bilgi sistemlerinin, önemli verilerinin ve kritik altyapılarının gizlilik, bütünlük ve erişilebilirliğinin sağlanması adına büyük yatırımlara yönelmektedir. 2008 yılında gerçekleşen ancak varlığı 2010 yılında anlaşılan Stuxnet saldırısı birçok açıdan bir miattır.

İlk olarak Stuxnet; ulusal düzeyde kritik öneme sahip altyapılar arasında yer alan "Supervisory Control and Data Acquisiton (SCADA)" yani Merkezi Denetim ve Veri Toplama Sistemlerini hedeflemektedir ("Stuxnet worm hits Iran nuclear plant staff computers"). SCADA, altyapıdaki hassas süreçleri ve fiziksel fonksiyonları izlemek ve kontrol etmek için birçok endüstri tarafından kullanılmaktadır. Tipik şekilleriyle kontrol sistemleri alandan sensor ölçümlerini ve operasyonel verileri toplar, bu bilgiyi işler,

görüntüler ve ardından verilen kontrol komutlarını yine ekipmana iletir. Elektrik endüstrisinde devre kesicileri açıp kapatarak ya da önleyici kapatmalar için varılması gereken enerji eşiğini ayarlayarak elektrik akımı düzenlenebilir. Petrol, gaz ve nükleer tesislerde ise bu kontrol sistemleri aracılığıyla rafinaj işlemleri uzaktan kontrol edilebilir, boru hatlarının basıncı ve akışları uzaktan izlenilebilir ve iletim akışlarına müdahalede bulunulabilir. Bir başka örnek olarak barajlardaki su seviyeleri, su basıncı, su akışları ve hatta PH, klor gibi su kalitesini etkileyen ölçümlerin tespiti ve yönetilmesi işte bu denetim ve veri toplama sistemleri aracılığıyla yapılır. Bu bakımdan SCADA'nın işlevleri küçük bir binada kendisini gösterebileceği gibi devasa nükleer enerji santrallerinde de belirebilir (İç İşleri Bakanlığı 624; Radvanovsky ve Brodsky 3-5).

SCADA, küresel internet ağına bağlı olmadığından internet üzerinden bu sistemlere sızmak mümkün değildir. Bu nedenle SCADA sistemleri hakkındaki güvenlik kaygıları 2010 yılına dek yalnızca, tesislere yönelik silahlı saldırılarla veya tesislerin kötüye kullanımıyla ilgiliyken Stuxnet bu kabulü tamamen değiştirir (Meryem).

İkinci olarak Stuxnet, "worm" yani solucan tipi bir virüstür ancak önceki solucanlardan da oldukça farklıdır.

İnternetin yaygınlaşması ile çoğalan yazılımlar kendilerini e-postalara ekleyerek internet üzerinden yayıldıklarında "worm" yani solucan olarak nitelendirilirler (Mitra 50). 1971 yılında Bob Thomas tarafından yazılan, "Creeper", kendi kendine çoğalan ilk program olması nedeniyle solucanların öncüsü kabul edilirken bilgisayarı yavaşlatmaktan ibaret olan etkisiyle oldukça zararsızdır da (Bıçakçı 105). 2000'lere gelindiğinde ise LoveLetter gibileri tek başına milyonlarca bilgisayarı etkileyerek verilerin geri dönüşümünü de imkânsız hale getirebilmektedir (Mitra 50). Siber Fiziksel Sistem (Cyber-Physical System) sınıfından kötü amaçlı solucan tipi bir yazılım olan ve 2010 yılında tespit edilen Stuxnet ise tehditin boyutunu tamamen değiştirerek siber sahada yeni bir çağ başlatmıştır (Subrahmanian ve diğerleri 36). O, İran'da yer alan ve internet bağlantısı olmayan Natanz Uranyum Zenginleştirme Tesislerindeki santrifüjleri patlatarak solucan tipi virüslerin somut ve fiziksel tahribatlar yaratabileceğini göstermiştir.

Üçüncü olarak Stuxnet, Advanced Persistent Threat (APT) yani Gelişmiş Kalıcı Tehdit saldırılarının endüstriyel bir ağa yönelen ilk örneğidir. APT saldırıları, diğer saldırılardan farklı olarak sisteme yavaş ama gizlilikle sızan ve sistemde uzun süre barınabilen saldırılardır. Daha ziyade politik hedeflere ya da kurumsal firmalara yönelik gerçekleştirilen APT saldırıları oldukça karmaşık yazılımlara dayanırlar. Bu saldırılar ancak karmaşık bir kodlamayla meydana getirilebileceği için arkasında güçlü finansmanlar bulunur.

Stuxnet'i anlamak için; internet bağlantısı olmayan Natanz'a nasıl sızdığı, amacının ne olduğu, nasıl çalıştığı ve nasıl tespit edildiğini irdelemek gerekir.

Tesise Sızması

Genel kabule göre, bir sistem dünya ile bağlantısı ne denli seyrekse o derece güvenlidir. Bir başka ifade ile bağlantı arttıkça zafiyet artar. Dolayısıyla 21.yüzyılda siber güvenlik uzmanlarının temel hedeflerinden birisi sistemler arası etkileşimi asgariye indirgemek ve hatta tamamıyla ortadan kaldırmaktır (De Silva, 222).

Stuxnet'in gözler önüne serdiği gerçek, internet bağlantısı bulunmasa dahi hiçbir sistemin tamamen bağımsız olmadığıdır. Bu bağ kimi zaman seyyar diskler ile kimi zaman yazıcılar ile sağlanır. Dolayısıyla bünyesinde IP (Internet Protocol) barındıran hiçbir bilişim diğerlerinden tamamen izole edilemez. Evrensel Seri Veriyolu yani USB (Universal Serial Bus) yolu ile sisteme karıştığı anlaşılan Stuxnet bunun en güzel örneğidir (Macaulay ve Singer, 113).

Stuxnet'in kodları, USB aracılığıyla yayılacak biçimde tasarlanmıştır. Bunun için zararlı yazılım ilk olarak USB bir belleğe bulaşmalıdır. Ardından bu belleğin bağlandığı bilgisayara sızar ve bilgisayarın bağlandığı internet ağlarına ya da diğer USB taşınabilir belleklere yayılır. Yayıldığı sistemlere, bilgisayarın algılamasını engelleyen dosyalarla birlikte kendisini kopyalamaya başlar (Evancich ve Li).

Stuxnet'in mimarları, güvenlik duvarlarını doğrudan değil dolaylı yollarla aşarlar. Sızma, tesise sınırsız erişimi olan mühendislerin bilgisayarlarına bulaştırılarak başlatılır, ardından mühendislerin tesise bağlanan bilgisayarları aracılığıyla Natanz'a sızılır. Bu yöntem, mühendislerin bilgisayarlarına sızmanın kolaylığını ve internet bağlantısı olmasa dahi hiçbir sistemin tamamen güvenlikli olmadığını gösterir. Mühendislerin kendi alanlarındaki kalifiyesi tartışılmamaktadır. Ancak çok az mühendis siber güvenlik konusunda temel yetkinliklere sahiptir. Tesislerin tüm güvenlik sistemleri, doğrudan dışarıdan yönelebilecek tehditleri engelleyecek tedbirler içermektedir. Fakat tıpkı bilinçli ya da bilinçsiz bir Truva Atı gibi tehlikeye içeriden sebep olabilecek kimseler göz ardı edilirler (Langner, To Kill Centrifuge 20).

Santrifüj ve sürücü mekanizmasına zarar verebilmek amacıyla Stuxnet, içerisinde barındırdığı dosyaları gizleyen "MRxNet" adlı rootkiti taşımaktadır. Rootkit, bilgisayar üzerinde çalışan programları gizleyerek sistemin kontrolünü ele geçirmesini sağlar (UITSEC). Stuxnet'in mühendisler tarafından fark edilmesini engelleyen başka bir unsur budur. Ayrıca USB ile bilgisayarlara sızan Stuxnet'i yalnızca kullanıcılar değil bilgisayarların güvenlik duvarı da fark edememiş, zararlı yazılım diski otomatik çalıştıran "autorun" özelliği ve .LNK dosyaları aracılığıyla iki ayrı yoldan hiçbir müdahale gerekmeksizin etkinleşerek yayılmaya başlamıştır.

Bu iki seçenekten .LNK güdümü, autorun seçeneğinden daha zekicedir. Zira autorun özelliği birçok bilgisayar yöneticisi tarafından basitçe kapatılırlar. Ancak .LNK dosyaları için aynısını söylemek mümkün değildir. Bilgisayarın .LNK işlevini kapatmak beraberinde birçok sorun da getirmektedir. Bu nedenle .LNK yolunun başarılı olması çok yüksek ihtimaldir. Stuxnet'in yapısını anlamaya çalışan araştırmacılar oldukça basit olan bu yolun önceden tercih edilmediğini şaşırtarak belirtirler (Zetter, Countdown to Zero Day Weapon).

LNK güdümü aynı zamanda oldukça karmaşık ve ilginç bir çalışma yapısına sahiptir. Windows'ta bulunan .LNK dosyaları, bir bilgisayara takılan USB sürücünün veya başka bir seyyar diskin içerisinde yer alan dosyaları görünür kılma işlevini üstlenirler. Dolayısıyla bilgisayara takılan USB'lerin içerisindeki müzik veya resim gibi unsurların görüntülenmesi için Windows Gezgini tarafından kendiliğinden .LNK dosyaları taranır. Stuxnet'te USB'nin içerisine gizlenmiş ve bilgisayar tarafından zararlı olduğu fark edilemeyen kodlar diğer zararlı yazılımlardan farklı olarak bir .LNK dosyasına gömülü halde bulunmaktadır. Windows gezgini tarafından bu dosya tarandığı anda yazılım USB'den bilgisayara sıçramak için başka herhangi bir müdahale gerekmeksizin harekete geçer (Zetter, Countdown to Zero Day Weapon).

Kullanıcıların Windows'a yine Windows'u kullanarak iki farklı yoldan saldıran Stuxnet adlı kötü yazılımı neden fark etmediği daha rahat anlaşılabilir. Ancak kendisi ile bağlantı sağlayan her sürücüyü denetleyen bilgisayarın Stuxnet'i fark etmemesi daha ilginçtir. Araştırmacılar bunun nasıl gerçekleştiğini araştırdıklarında kendilerini şaşırtacak yeni bulgulara ulaşırlar. Windows, güvenilirliğinden emin olduğu donanım üreticilerinin yazılımlarına bilgisayara yüklendikleri esnada herhangi bir denetimden geçmelerini engelleyecek özel izinler verir. Bu izinler dijital bir imza şeması ile sağlanır. Dolayısıyla bir yazılım Windows tarafından güvenilir olarak algılanan bu şemaları barındırıyorsa herhangi bir denetimden geçirilmeden sisteme yüklenebilir (E-C Council).

Zararlı yazılımın yaratıcıları bunun farkında olarak Stuxnet'i, merkezi Tayvan'da yer alan ve Windows tarafından denetimden geçirilmeyecek sertifikalara sahip JMicron Technology Corporation ve Realtek Semi Conductor Corporation adında iki şirketin imzası ile işlerler (Raiu). Windows bu imzaları güvenilir olarak algıladığı için yazılıma yönelik herhangi bir güvenlik taraması yapmaz (Singer ve Friedman). Oldukça ünlü bu iki şirketin sertifikalarının çalınması Stuxnet'in yaratıcılarının maddi kaygılar taşımadıklarını göstermektedir.

Tüm bu yönleriyle Stuxnet'in bir zero-day saldırısı olduğu belirtilmelidir. Zero-day saldırıları, saldırılan sistemin operatörleri tarafından henüz algılanmamış ve dolayısıyla kapatılması adına herhangi bir çaba da gösterilmeyen açıkların keşfi ile gerçekleştirilen saldırılardır. Başarılı olmama ihtimalleri oldukça düşüktür. "Zero-day" terimi güvenlik açığının kâşifi hariç kimse tarafından bilinmediğini ifade etmek için kullanılır. Bir sistemde keşfedilen zero-day açıkları, keşfeden tarafından ilk aşamada gizli tutulurlar.

Bu açıklar sistemin sahibine veya sisteme saldırma amacı güden kötü niyetli kimselere satılarak açığın kâşifi tarafından nakde çevrildiklerinden açığı keşfeden, keşfini uzun süreler boyunca gizli tutmayı yeğler (Johnson, 12-13).

Bir Zero-Day saldırısının önemi iki noktada belirir. İlk olarak zero-day açıkları ancak saldırı neticesinde kesin başarı elde etmek isteyen kimseler tarafından hedef alınırlar. Dikkat çeken ikinci nokta ise bu açıkların piyasada oldukça yüksek fiyatlarla satılması ve bu nedenle kuvvetli bir ekonomik birikimi olmayan kimseler tarafından tercih edilebilir olmamalarıdır.

Stuxnet saldırısı ise önceden görülmemiş biçimde 4 tane zero-day açığının kullanılması ile gerçekleştirilir. Stuxnet bu açıdan da dünyada bir ilk olma özelliği taşımaktadır. Artık araştırmacılar saldırının arkasında basit bir oluşumdan ziyade kuvvetli bir yapının bulunduğu hususunda hemfikirdirler (Naraine). Bu saldırıyı düzenleyenler herkimseler, neticesinde istediklerini elde edeceklerine dair bir kesinlik istemekte ve başarı için yüklü paraları gözden çıkartmaktadırlar. Söz konusu gerçekler, Stuxnet'in yaratıcılarının Natanz'a sızmakla ne elde etmek istediklerine dair derin bir merak uyandırmaktadır.

Amacı

Natanz tesisi, İran'ın en büyük gaz santrifüj uranyum zenginleştirme tesisidir. BM Güvenlik Konseyi kararlarına aykırı olarak 2007 Şubat'ında faaliyete geçen bu tesisin Siemens tarafından üretilen SCADA sistemlerinde yer alan Programmable Logic Controller (PLC) yani Programlanabilir Mantık Denetleyicileri, 6 aydan uzun bir sürede ancak geliştirilebileceği düşünülen Stuxnet'in odağındadır ("Stuxnet worm hits Iran nuclear plant staff computers"). PLC'ler fabrikalarda yer alan ve üretim hatlarında kullanılan robot ve taşıyıcı bant gibi sistemlerin kontrölü için kullanılan bilgisayarlardır (İzgöl). PLC'lerin bir bölümünde meydana gelen sorunlar diğer PLC'leri etkilemezler (Kaya). SCADA ise bir operatörün tüm sistemi canlı olarak tek merkezden izleyebilmesine ve sisteme müdahale edebilmesine olanak sağladığından elektrik santralleri gibi daha geniş coğrafi bir alana yayılan ve tüm tesisi etkileyen geniş tabanlı yapılardır (Mondi). SCADA sistemleri internete bağlı olmadıklarından, USB aracılığıyla sisteme sızan Stuxnet'in birbirine bağlı iç LAN ağı veya MS10-061 güvenlik açığı nedeniyle yazıcılar aracılığıyla tüm tesise yayıldığı düşünülmektedir (Pahi ve Skopik).

Bilgisayar, Remote Procedure Call (RPC) yani Uzaktan Yordam Çağrısı üzerinden kullanılan bir yazıcı arabirimine sahip başka bir bilgisayara yazdırma isteği gönderirse, MS10-061 güvenlik açığı nedeniyle isteği devralan bilgisayar tarafından uzaktan kod yürütülebilmektedir. Uzaktan kod yürütülmesi, zararlı yazılımların başka bilgisayarlara yayılması ile sonuçlanabilir. Stuxnet, bu açıkları kullanarak tesisin içindeki diğer bilgisayarlara hızla yayılmıştır. Stuxnet ile fark edilmesi neticesinde Microsoft, bu ve benzer açıkların kapatılması için güncelleştirmeler yayınlar ("Microsoft Security Bulletin CriticalStuxnet, santrifüjleri doğrudan etkileyen PLC'lere erişene dek varlığını belli

etmemek için herhangi bir müdahalede bulunmaz. PLC'lere eriştiğinde ise onları santrale zarar verecekleri biçimde yeniden programlamaktadır. İlk olarak kendi sürümünün diğer PLC'lere aktarılmasına ortam hazırlayan ve böylelikle kendi kendisinin çoğalması ile sonuçlanan zararlı komutları sisteme gönderir. Ardından santraldeki pompalar üzerindeki görünümleri değiştirir ve değiştirmekle yetinmez, değişiklik izlerini de ortadan kaldırır. Stuxnet tarafından manipüle edilmiş veriler nedeniyle santralin operatörleri sistemdeki bozukluklardan haberdar olamadıklarından sorunlara müdahale de edemezler. Öte yandan Stuxnet, Danimarka ve Malezya'da yer alan iki sunucu ile bağlantılı olarak kendisini sürekli güncelleştirmektedir (Britz, 19).

Stuxnet'in amacı İran'ın uranyum zenginleştirme tesisinden bilgi çalmak veya doğrudan finansal bir gelir elde etmek değildir. O, uranyum zenginleştirme hedeflerine çok yaklaşan tesisteki işleyişi bozmak ve hatta tesisi yok etmek üzerine politik amaçlarla programlanır (Campbell ve Kennedy). Dönemin yetkilileri 6000 santrifüje erişmeyi amaçladıklarını duyursalar da 23 Haziran 2009 tarihinde Stuxnet'in Natanz'a sızdığından habersizdirler ("İran'ın yeni nükleer yarattı"). Stuxnet, 5 ay içerisinde, SCADA sisteminde görülmediği için müdahale edilemeyen aşırı hız değişiklikleri nedeniyle yaklaşık 1000 santrifüjün kaybına neden olur. Yazılım, santrifüjleri 15 dakika boyunca aşırı hızlı biçimde döndürmeye başlatır ve dönüş hızını aniden azaltarak imha eder (Stuxnet).

Çalışma Aşamaları

Uranyum zenginleştirme tesislerine zarar vermeyi amaçlayan yazılımcıların, uranyum tesislerinin işleyişi hakkında geniş bilgilere sahip oldukları düşünülmektedir. Zira uranyumun saf ve kullanılabilir biçimde kalması için tesislerin sabit bir hızda çalışması gerekirken Stuxnet, doğrudan santrifüj hızını değiştirirerek göstergeleri de bozmakta ve hızın olumlu seyirde olduğu izlenimi yaratmaktadır.

Özetle Stuxnet, birden çok aşamayla hazırlanmış kaliteli bir planın ürünüdür. Bu plan yalnızca sisteme sızmak değil aynı zamanda sistemde barınmak üzerine inşa edilmiştir. Diğer bir ifade ile Stuxnet saldırısı, yazılımın barınmasını engelleyecek ihtimalleri ortadan kaldırmayı da içerir. Stuxnet'in politik amaçlar gütmeyen basit bir grup tarafından üretildiğini düşünmek olası gözükmemektedir. Saldırganların saldırıdan önce defalarca kez denemeler yaptıkları da açıktır (Diogenes ve Ozkaya, 58). Bu etkili planın aşamaları şöyle özetlenebilir (Knapp, 38-41);

1) Stuxnet ilk olarak bilgisayar tarafından güvenilir olarak algılanan imzalı sertifikaları (Realtek ve JMicron) kullanarak zero-day açıkları aracılığıyla mühendislerin Windows sistemine bulaşır. Zero-day açıklarının bir sistem açısından büyük tehlike arz edeceği zira henüz tespit edilemediklerinden mutlak bir boşluk oluşturacağı hatırlanmalıdır.

2) Ardından bilgisayarın herhangi bir virüs taşıyıp taşımadığına odaklanmadan kendisi ile uyumlu bir Windows sürümü çalıştırıp çalıştırmadığını kontrol eder. Bununla birlikte sistemde kendisine engel teşkil edebilecek herhangi bir koruma programı bulunup bulunmadığını denetler.

3) Sonrasında ağ bağlantıları, çıkarılabilir medya barındırıcıları ve seyyar disklere yayılmaya başlar. Bu noktada Stuxnet'in varlığı ne sistem tarafından ne de mühendis tarafından tespit edilememektedir. Zira Stuxnet izini kaybettirmek üzerine programlanmıştır ve hedeflediği sisteme ulaşana dek herhangi bir etki göstermez.

4) Ağ bağlantıları ve seyyar diskler gibi bilgisayarları diğerleriyle doğrudan veya dolaylı olarak etkileşime sokacak unsurlara yayılmasının akabinde, asıl hedefi olan endüstriyel sistemi yani Siemens WinCC SCADA'yı arar. Sistemi bulana dek herhangi bir etkinlik göstermeyen Stuxnet, sistemi bulduğunda nokta hedefi olan PCL'lere erişmek için SCADA veri tabanına değişiklikleri işler. Bu değişiklikler PLC'nin işlemlerini durdurabilen, PLC ile diğer cihazlar arasındaki bağlantıları yavaşlatabilen ve sair çıkış bitlerini etkileyen nitelikler taşır. İşte bu noktada Stuxnet'in sistemin işleyişine müdahalesi ortaya çıkmaktadır.

5) Eğer sistemde frekans kontrol cihaz ayarlarının varlığını anlarsa, döngü başına frekans hızını 1410'dan 2Hz'e indirir ve zaman zaman aniden artırır. Değişikleri tespit edemeyen mühendisler müdahale etmezler. Santrifüj adım adım çöküşe gitmektedir. Neticeten değersiz üretim yapar ya da üretimi tamamen durdurur.

6) Son olarak Stuxnet, yapısıyla uyumsuz bir cihazın içerisine yerleştiğini fark ederse kendisini yok etmektedir. Öte yandan kendisini gizlemek adına uyku moduna da alabilir, kendisini fark edip temizleyen cihazlara yeniden bulaşabilir, kendisini güncellemek amacıyla diğer ağlardaki sistemlerle iletişime geçebilir.

Bütüncül bir bakış açısıyla Stuxnet'in temel olarak üç modülünün bulunduğu söylenilebilir: saldırının ana amacını yani santrifüje zarar vermeyi tetikleyen bir virüs, saldırıyı kendiliğinden etkin kılarak kopyalayan yani diğer sistemlere de yayan bir .LNK dosyası ve tüm zararlı hareketleri gizleyen yani Stuxnet'in algılanmasını engelleyen MRxNet isimli bir rootkit (Alsmadi, 156).

Stuxnet birçok gerçeğin farkına varmamızı sağlar. Stuxnet'ten önce kontrol sistemlerinin diğerlerinden tamamen izole edilebileceğine dair bir kanı yaygındır ancak Stuxnet ne yapılırsa yapılsın bunun tamamen mümkün olamayacağını bizlere gösterir.

Öte yandan Stuxnet PLC'leri hedef almadan önce, PLC'lerin herhangi bir yazılımsal saldırıya hedef olamayacağı düşünülür. Diğer sistemlerden farklı olarak üst düzey gizliliğe sahip SCADA gibi sistemlerin, sistem dışından erişilebilir olmadıkları düşüncesi yıkılır.

Aynı zamanda SCADA gibi yapılarda bulunan yüksek korumalı güvenlik duvarları veya saldırı tespit ve önleme sistemlerinin işlevsizleştirilebileceği de anlaşılır. Bu durum özellikle kritik altyapı tesisleri için büyük riskler arz etmektedir.

Tespit Edilmesi

Stuxnet'in varlığının nasıl tespit edildiğini bilmek, benzer tespitlerin gerçekleştirilebilmesini mümkün kılar. Yanımızdan eksik etmediğimiz tabletlerimizde, yokluğu gündelik yaşantımızı durduran telefonlarımızda, sayısız işlemler gerçekleştirebildiğimiz bilgisayarlarımızda ve hatta her akşam karşısından ayrılamadığımız televizyonlarımızda zararlı birer yazılım bulunuyor olabilir. Bu yazılımların varlığı birey için tehlike, devletler için felakettir. Felaketin boyutunu anlamak için nasıl Stuxnet'in taşıdığı önemi tekraren vurgulamak zaruri ise bu tehdidi önlemek için Stuxnet'in tespitini bilmek de hayatidir.

17 Haziran 2010 tarihinde Belarus'taki ofisinde çalışmakta olan ve VirusBlokAda adlı küçük bir bilgisayar güvenlik şirketinin antivirüs bölümüne başkanlık eden Sergey Ulasen, İran'daki bir müşterisinin bilgisayarının sürekli olarak kendisini yeni başlattığına dair bir e-posta alır. Bilgisayara zararlı yazılımların bulaştığı aşikardır. VirusBlokAda adlı şirket, McAfee ve Karspersky gibi şirketlerin yanında çok da bilinmeyen bir şirkettir. Fakat bu e-postanın sonucunda, yakında dünyada bilgisayar ile ilgilenen herkesin hakkında bilgi sahibi olduğu ünlü bir şirket olur (Zetter, "How Digital Detectives Deciphered Stuxnet History").

Ulasen ve ekibi ilk olarak müşterilerinin bilgisayarına bulaşan zararlı yazılımın yukarıda kendilerinden bahsedilen zero-day açıklarından faydalandıklarını anlarlar. Bu açığın fark edilmesi dahi büyük bir başarıdır zira zero-day açıkları kimsenin bilmediği açıklardır. Öyle ki, yeryüzünde her yıl keşfedilen yaklaşık 12 milyon zararlı yazılımdan yalnızca bir düzinesi bu açıklardan faydalanmaktadır. Bilahare, derhal Microsoft ile iletişime geçerler ve yazılımın inceliklerini anlatmaya başlarlar. Sonrasında ise VirusBlokAda tarafından forumlara yazılan yazılar ile virüs kamuya açıklanır. Microsoft, Realtek'in sertifikasını iptal etmek için bir güncelleme hazırlar fakat zararlı yazılımın kullandığı tek sertifikanın Realtek'e ait olmadığı anlaşılınca tüm siber güvenlik firmaları Microsoft'tan zararlı yazılımın örneğini istemeye başlarlar (Zetter, "How Digital Detectives Deciphered Stuxnet History").

Bir anda tüm dünyanın gözü Stuxnet'in üzerinde olur. Symantec adlı şirkette çalışan Liam O'Murchu ise takımında yer alan Eric Chien ve Nicolas Falliere ile birlikte daha önce eşine rastlanmamış bu yazılımın oldukça karmaşık bir yapıda olduğunu tespit ederler.
Siber güvenlik şirketlerinin işleyişi, ele geçirilen zararlı yazılımların otomatik programlarla taranarak imha edilmesi üzerine kuruludur. Fakat Stuxnet'in bir programdan çok daha ötesini gerektirdiği anlaşılır.

Olağan bir zararlı yazılım yaklaşık 10-15 KB (Kilobyte) arasında bir boyuta sahip iken Stuxnet 500 KB boyutundadır (Zetter, Countdown to Zero Day Weapon).

Stuxnet'in bulaştığı sistemleri raporlamak ve kendisini güncelleştirmek adına www.mypremierfutbol.com ve www.todaysfutbol.com isimli internet sitelerine bağlandığı fark edilir. Symantec, internet sitelerinin sağlayıcıları ile iletişimi geçer ve zararlı yazılımı kendi trafiğine yönlendirmelerini sağlar. Ertesi sabah Symantec trafiği Stuxnet'in gönderdiği bir dizi raporla doludur. Bu raporlar aracılığıyla Stuxnet'in gerçek saldırganlara bildirmek üzere programlandığı veriler Symantec personeli tarafından toplanır. 20 Temmuz Salı gününe gelindiğinde toplanan veriler iyice çoğalır. O'Murchu başkanlığındaki ekip verileri toplamakta ve aralarındaki ortaklıkları sınayarak tasnif etmektedir. Bir hafta içinde düzinelerce ülkeden yaklaşık 38.000 bilgisayarda kötü yazılımın varlığı tespit edilir. Sayı günde yaklaşık 9.000 artmaktadır. Kısa zaman içerisinde ise 100'den fazla ülkede görülür ve toplamda 100.000'i aşar. Stuxnet hızla yayılmaktadır. Antivirüs üreten firmalar yazılımın yayılmaması için olağan güçleriyle çalışsalar da onu engelleyememektedirler. Zira birçok kullanıcı antivirüs yazılımlarının eski sürümlerini kullanmaktadır (Zetter, "How Digital Detectives Deciphered Stuxnet History").

O'Murchu ve ekibi zararlı yazılımların yayılmış olduğu coğrafyayı gelen verilere dayanarak şemalandırınca ortaya ilginç bir görünüm çıkar. Virüsün bulaştığı ilk 38.000 makineden 22.000'den fazlası doğrudan İran merkezlidir. İran'ı ise yaklaşık 6.700 makine ile Endonezya ve 3.700'den fazla makine ile Hindistan takip eder. Amerika Birleşik Devletleri'nde ise 400'den az bulaşma tespit edilir. Öte yandan virüsün bulaştığı makinelerin önemli bir bölümünün Siemens yazılımları ile donatıldığı görülür. Akıllara gelen ilk soru evvelde Orta Asya ve Orta Doğu'dan kaynaklanan saldırılarda dahi listenin üst sıralarında yer almayan İran'daki enfekte sayısının neden bu kadar fazla olduğudur. Saldırının geçmişte hiçbir benzeri görülmemiştir. Bir diğer soru ise saldırının doğrudan İran, Hindistan ve Endonezya'da yayılmasının neden kaynaklandığıdır. Neden önceki saldırılarda Amerika Birleşik Devletleri ve Avrupa ülkeleri istatistiklerin üst sıralarındayken şimdi geridedirler? Bu soruya yanıt aramak amacıyla İran ve Hindistan arasındaki ortak noktalar tespit edilmelidir. Yanıt İran ve Hindistan arasında iki ülkeyi birbirine bağlamak amacıyla inşa edilen ve İran'ın Güney Pars gaz havzasından Pakistan'a ve oradan da Hindistan'a uzanan yaklaşık 1.700 millik bir doğal gaz boru hattında bulunur. Amerika Birleşik Devletleri'nin sıkı baskıları, fon sıkıntıları ve iklim değişiklikleri gibi sebeplerle askıya alınan projeden 2009 yılında çekilen Hindistan, Stuxnet'in varlığının tespit edilmesinden yaklaşık 2 ay önce projeye yeniden katılmıştır. (*Zetter, Countdown to Zero Day Weapon).*

Fakat sorulan sorulara verilebilecek yanıtlar bununla sınırlı değildir. İran'ın nükleer faaliyetleri de hızla artmaktadır. İran özellikle ülkenin güneyinde yer alan Bushehr'de kendisini İsrail ve Batı ile sonu olmayan bir gerilime sürükleyen nükleer reaktörler inşa etmektedir. En az bu reaktörler kadar tartışmalı olan bir diğer faaliyet ise Natanz adı verilen ve reaktörlere nükleer yakıt sağlamak için yapıldığı anlaşılan uranyum zenginleştirme tesisleridir.

Birleşmiş Millet tesislerin faaliyetlerini durdurması için İran'ı defalarca uyarsa da bir sonuç alamaz. Hatta tartışmalar öyle ilerler ki, tesise yönelik bir hava saldırısının planlandığı dahi duyulur. Söz konusu bilgiler ve araştırmaları bir bütün olarak değerlendirerek zararlı yazılımın İran'ın nükleer programını sabote etmeyi amaçlayan hassas bir silah olduğunu iddia eden ilk isim 52 yaşındaki Alman SCADA güvenlik uzmanı Ralph Langner olur. 16 Eylül 2010 tarihinde kendi bloğunda yayınladığı yazıda bu yazılımın diğerlerinden farklı olarak bir tesisi sabote etmek üzerine programlandığını ileri sürer (Langner, "Stuxnet Logbook Mesz").

23 Kasım 2010'da İran Atom Enerjisi Örgütü Başkanı Ali Akbar Salehi, İran nükleer tesislerinin saldırı altında olduğuna yönelik ilk kabulü açıklayacaktır. Açıklamasını batılıları suçlayarak ve tesislerin zarar görmediğini belirterek sürdürür (Iran denies Stuxnet disrupted its nuclear programme). 6 gün sonra yapılan bir basın toplasında İran Cumhurbaşkanı Mahmud Ahmedinejad tesisin sabote edildiğini ve zarar gördüğünü onaylar. Basın açıklamasının yapıldığı gün, uranyum tesislerinde çalışan İranlı iki nükleer mühendis Majid Shahriari ve Fereydoun Abbasi de suikaste uğrarlar. Onlar suikaste uğrayan ilk mühendis değildirler, son da olmayacaklardır (Zetter, Iran: Computer Malware Sabotaged Uranium Centrifuges).

Uzmanlar tesisleri hedef alan bir yazılımın hedefini şaşarak bireysel bilgisayarlara karışmasının sebebini halen dahi çözemezler. Tahminleri Stuxnet'in yine USB'ler aracılığıyla tesise bağlanan diğer mühendislerin bilgisayarlarına bulaştığı ve akabinde bu bilgisayarların etkileşim sağladığı internet ağları üzerinden yayıldığıdır. Çözülemeyen bir diğer sorun da bu yazılımın bilgisayarlara verebileceği zararın boyutudur. Cevaplanamayan soruların sınırı ve sayısı ne olursa olsun herkes Stuxnet'in varlığı üzerinde hemfikirdir. Stuxnet'in bireysel bilgisayarlardan ve tesislerden temizlenmesi adına ardı ardına güncelleştirmeler yayımlanır. Güncelleştirmeler neticesinde tamamen ortadan kalkıp kalkmadığı bilinmese de Stuxnet, varlığı, yaptıkları ve yaşattıkları ile tarihin sayfalarında kendisine hiç de kolay silinmeyecek bir yer edinir. Onun misyonunu (!) kendi türevleri olduğu iddia edilen Duqu ve Flame gibi zararlı yazılımlar sürdürmekte, siber tehditler yaşamın her anında varlığını günden güne hissettirmektedir.

Sonuç ve Öneriler

Stuxnet bir evrim değil, devrimdir. Zira o, varlığı ile birlikte soyutun somuta yönelik tehlikesizliği algısını tamamen yıkmaktadır. Artık türü ve işleyişi fark etmeksizin içerisinde yazılım kodları barındıran bütün sistemler ve dolayısıyla bireyler ile hükümetler bizzat tehlike altındadırlar.

Bu tehlike tonlarca ağırlığa sahip bombalardan veya devasa silahlardan değil her gün önümüzden eksik etmediğimiz klavyeden kaynaklanmaktadır. Klavyenin sınırsızlığı, saldırıların sınırsızlığını da beraberinde getirir.

Saldırıların boyutu bilgi sızdırmaktan ya da salt ekonomik kayıplara uğratmaktan çok daha fazlasıdır. Artık amaç imha etmektir.Stuxnet'ten önce kritik altyapıların, nükleer tesislerin ve diğer tüm SCADA sistemlerinin dünyadan tamamen izole edildiği anlayışı hakimken Stuxnet'ten sonra "Hiçbir sistem, güvenli değildir." kabülüyle sıkça karşılaşılır.

Amaçları farklı olsa da Stuxnet'in türevleri yayılmaya devam etmektedir. 2011 yılında varlığı tespit edilen Duqu kurtçuğu, Stuxnet'in aksine endüstriyel kontrol sistemlerinden bilgi çalmak için geliştirilir (Kushner). 2012 yılında da "Flame" kod adlı kötü niyetli yazılım tespit edilir. Stuxnet'in devamı olarak kabul edilen Flame, internet bağlantısı aracılığıyla bilgisayarların ara birimlerini çalıştırabilmekte, mikrofonu açarak sesleri kaydedebilmekte ve topladığı verilen hepsini yine internet aracılığıyla yaratıcılarına gönderebilmektedir. Flame'nin amacı da Stuxnet'ten farklı olarak doğrudan fiziksel hasar vermek değildir (Köylü).

Sonuç olarak, hiçbir sistemin güvenli olmadığına yönelik kabulün karşısında her taarruzun bir müdafaası olacağı gerçeği yer alır. Siber tehditlerin felakete dönüşmesini engellemek için öneriler şu şekilde özetlenebilir:

• Her şeyden önce hükümetler savaşın siber sahaya taştığının bilincinde olmalı ve kendilerine siber güvenlik uzmanlarından oluşan bir ordu kurmalıdırlar. İran yaşadıklarından çıkardığı dersler neticesinde günümüzde bir siber güvenlik ordusuna sahiptir. Stuxnet'in yaşanmasının ardından birçok İranlı genç, hükümet tarafından kurulan bu orduya katılmak için gönüllü başvurularda bulunur. Öyle görünmektedir ki, İran bu çabasıyla aslında Stuxnet saldırısının mağlubu değil galibidir. Birkaç yüz santrifüj kaybettiği aşikardır. Fakat binlerce asker kazanmıştır ("Dünyanın İran'da").

• Ülkelerdeki mevcut tüm tesisler ve kritik altyapı sistemleri yenilenmeli ve bakımları periyodik olarak sağlanmalıdır. Bu konuda Venezuela yakın tarihimizdeki acı örneği teşkil eder. Venezuela'daki santrallerin ve tesislerin bakımsızlığı ve güvensizliği ülkenin haftalarca elektrikten yoksun kalmasına sebep olur. Yerel makamlar bu mahrumiyetin Amerika Birleşik Devletleri'nden kaynaklanan bir siber saldırıdan meydana geldiğini ileri sürseler de santrallerin bakımlarının gerçekleştirilmemesi hususundaki ihmalleri ortadadır (Lendman).

• Hukuksal düzenlemeler ancak tehlikenin boyutları belirince tedvin edilmektedirler. Onlar bu yönleri ile kovuşturma ve önleme işlevi görürler. Siber sahanın sınırsızlığı, bu saha hakkındaki hukuksal düzenlemelerin tespitini zorlaştırmaktadır. Ancak mezkûr zorluklar, hukukun siber sahadan tamamıyla el çektirilmesi biçiminde yorumlanmamalıdır. Hükümetler gerek bireylerin gerekse devletin güvenliğini sağlamak amacıyla mevzuat düzenlemelerine öncelik vermelidir. Özellikle uluslararası hukukta devletler arası antlaşmalar ile siber savaşın ve siber saldırıların sınırları çizilmeli, alınacak tedbirler somutlaştırılmalıdır.

Bu konuda 23 Kasım 2001 tarihinde Avrupa Konseyi'nde imzalanan Budapeşte Siber Suç Sözleşmesi ve Eylül 2019'da aralarında Türkiye Cumhuriyeti'nin yer almadığı Birleşmiş Milletler üyesi 27 devletin imzaladığı ortak bildiri dikkat çekicidir.

Bildiriye göre askeri hedeflere saldırmak meşru iken sivil altyapılara saldırmak gayri meşru bir harekettir (Joint Statement on Advancing Responsible State Behaviour in Cyberspace). Birleşmiş Milletler, NATO, Avrupa Konseyi gibi kuruluşlar siber saha hakkındaki çalışmalarını sürdürmektedirler.

• Stuxnet'in gözler önüne serdiği bir diğer gerçek ise yurttaşların siber güvenlik eğitiminin önemidir. Zira güncel kabule göre Stuxnet, siber güvenlik hakkında hiçbir eğitim ve deneyime sahip olmayan mühendislerin kullandıkları bilgisayarlar aracılığıyla tesise yayılmıştır. Natanz örneğinden hareketle yurttaşlar siber saha ve siber güvenlik hakkında çocuk yaşlardan itibaren eğitilmeli ve bu eğitimin yanında kendilerine kodlama dilleri de öğretilmelidir. Yeni ve büyük saldırıların önlenmesi ancak sağlam bilince sahip yurttaşların yer aldığı toplumlarda kaimdir. Siber saldırılar yapıları gereği bir veya birkaç uzmanın karşılayabileceklerinden çok daha büyüktürler. 21.yüzyılda, günlük hayatımızın her alanına yayılan bilişim sistemleri olmadan alınan bir nefes tahayyül edilememektedir. Hülasa bu sistemlerin hepsi, siber savaşta açılmış bir cephe, potansiyel birer silahtırlar. Yalnızca yeterli bilince sahip kullanıcılar ile tehlikeler savuşturulabilir. Dünyayı bir örümcek ağı gibi sararak hızla yayılan internet, ihmalkarlığının bedelini birisine değil binlercesine ödetmektedir.

Açıklama bildirimi

Bu çalışmada herhangi bir potansiyel çıkar çatışması bulunmamaktadır.

Iletişim

E-mail: alper.aslan24@ogr.deu.edu.tr

Kaynakça

Alsmadi, Izzat. The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics. Springer, 2019.

Anderson, Mondi. "What Are The Differences Between DCS and SCADA.". Real Pars. Y.Y., 10 07 2019, https://realpars.com/dcs-vs-scada/. 09 12 2019.

Bıçakçı, Salih. "NATO'nun Gelişen Tehdit Algısı: 21.Yüzyılda Siber Güvenlik." Uluslararası İlişkiler 10.40 (2014): 101-130.

Britz, Marjie T. Computer Forensics and Cyber Crime. Pearson, 2013.

Campbell, Q. ve David M. Kennedy. "The Psychology of Computer Criminals." Ed.Bosworth, Seymour, M.E. Kabay ve Eric Whyne. Computer Security Handbook. Wiley, 2014. 12.1-12.26.

De Silva, Eugenie. National Security and Counterintelligence in the Era of Cyber Espionage. IGI Global Disseminator or Knowledge, 2016.

Diogenes, Yuri ve Erdal Ozkaya. Cybersecurity - Attack and Defense Strategies. Packt Publishing, 2018.

"Dünyanın en büyük hacker ordusu İran'da." Tech İnsıde. Y.Y., 08 07 2016, https://www.techinside.com/dunyanin-en-buyuk-hacker-ordusu-iranda/. 10 12 2024.

E-C Council. Computer Forensics Investigating Network Intrusions & Cyber Crime. New York: E-C Council Press, 2010.

Evancich, Nick ve Jason Li. "Attacks on Industrial Control Systems." Colbert, Edward J. M. ve Alexander Kott. Cyber-security of SCADA and Other Industrial Control Systems. Switzerland: Springer, 2016.

Hatipoğlu, Cemalettin. "Teknolojik Savaşlar: Siber Terörizm Tehditleri." 3nd International Congress on Political, Economic and Social Studies (ICPESS). Ankara, 2017.

"Iran denies Stuxnet disrupted its nuclear programme." BBC News, BBC, 24 November 2010, https://www.bbc.com/news/technology-11821011. 08 12 2019.

İç İşleri Bakanlığı. Güvenlik Terimleri Sözlüğü. Ankara: Uluslararası Piri Reis Kültür Ajansı, 2017.

"İran'ın yeni nükleer tesisi tartışma yarattı." BBC News, BBC, 26 Eylül 2009, https://www.bbc.com/turkce/haberler/2009/09/090926_iran_nuclear. 08 12 2019.

İzgöl, Kerem. "PLC Nedir? PLC Programlama Teknikleri ve Özellikleri." Robotistan, Y.Y., 18 04 2018, https://maker.robotistan.com/plc-nedir-plc-programlama-teknikleri-ve-ozellikleri/. 09 12 2019.

Johnson, Thomas A. "Historical Reference Points in the Computer Industry and Emerging Challanges in Cybersecurity." Ed.Johnson, Thomas A. Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. New York: CRC Press, 2015. 1-33.

"Joint Statement on Advancing Responsible State Behavior in Cyberspace." U.S. Department of State. 23 09 2019,. https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/. 10 12 2024.

Kaplan, Meryem. "SCADA Nedir? Kritik Altyapıya Yönelik Tehditler ve Güvenlik." Siber Tehdit. Y.Y., 10 08 2016, https://sibertehdit.com/731/. 07 12 2019.

Kaya, Mert. "PLC Ve DCS Arasındaki Farklar Nelerdir?" Roboturka. Y.Y., 08 09 2017, http://roboturka.com/plc/plc-ve-dcs-arasindaki-farklar-nelerdir/. 09 12 2019.

"Advanced Persistent Threat (APT)." Lostar. Y.Y., 29 11 2014, https://lostar.com.tr/2014/11/advanced-persistent-threat-apt.html. 07 12 2019.

Knapp, Eric D. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Massachusetts: Syngress, 2011.

Köylü, Hülya. "En tehlikeli virüs: Flame." Deutsche Welle Türkçe. DW, 31 05 2012, https://www.dw.com/tr/en-tehlikeli-vir%C3%BCs-flame/a-15988868. 09 12 2019.

Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum. IEEE, 26 02 2013, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. 09 12 2019.

Langner, Ralph. "Stuxnet Logbook, Sep 16 2010, 1200 Hours Mesz." Langner. Reshaping Operations Technology, 16 09 2010. https://www.langner.com/2010/09/stuxnet-logbook-sep-16-2010-1200-hours-mesz/#more-217. 09 12 2024.

---. To Kill a Centrifuge. Munich: The Langner Group, 2013.

Lendman, Stephen. “Trump Regime Electricity War in Venezuela More Serious than First Believed.” Global Research. Global Research Publishers, 11 03 2019, https://www.globalresearch.ca/trump-regime-electricity-war-venezuela/5670970. 09 12 2024.

Macaulay, Tyson ve Bryan Singer. Cybersecurity for Industrial Control Systems SCADA, DCS, PLC, HMI, and SIS. New York: CRC Press, 2011.

“Microsoft Security Bulletin MS10-061 - Critical.” Microsoft, Microsoft Corporation, 14 09 2010, https://docs.microsoft.com/security-updates/securitybulletins/2010/ms10-061. 09 12 2019.

Mitra, Ananda. The Digital World Digital Security Cyber Terror and Cyber Security. New York: Chelsea House Publishers, 2010.

Naraine, Ryan. “Stuxnet attackers used 4 Windows zero-day exploits.” ZD Net, Y.Y., 14 09 2010, https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/. 08 12 2019.

Pahi, Timea ve Florian Skopik. “A Systematic Study and Comparison of Attack Scenarios and Involved Threat Actors.” Skopik, Florian. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level. Florida: CRC Press, 2018. 19-68.

Radvanovsky, Robert ve Jacob Brodsky. “Introduction.” Radvanovsky, Robert ve Jacob Brodsky. Handbook of SCADA/Control System Security. Florida: CRC Press, 2016. 3-15.

Raiu, Costin. “Stuxnet signed certificates frequently asked questions.” Secure List. AO Kaspersky Lab, 21 07 2010, https://securelist.com/stuxnet-signed-certificates-frequently-asked-questions/29725/. 08 12 2019.

Singer, P.W. ve Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know? New York: Oxford University Press, 2014.

“Stuxnet.” New Jersey Cybersecurity and Communications Integration Cell, NJCCIC, 10 August 2017, https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/stuxnet. 09 12 2019.

“Stuxnet worm hits Iran nuclear plant staff computers.” BBC News, BBC, 26 September 2010, https://www.bbc.com/news/world-middle-east-11414483. 07 12 2019.

Subrahmanian, V.S., ve diğerleri. The Global Cyber-Vulnerability Report. New York: Springer, 2015.

UITSEC. Siber Güvenlik Cep Sözlüğü. İstanbul: UITSEC Teknoloji A.Ş., 2016.

Zetter, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown Publishers, 2014.

—. “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.” Wired. 11 07 2011, https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/. 10 12 2024.

—. “Iran: Computer Malware Sabotaged Uranium Centrifuges.” Wired. 29 11 2010, https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/. 10 12 2024.

Makaleni böyle alıntılayın:.Aslan A. XXI. Yüzyılda güvenlik meselesi ve silahlar: Stuxnet .Bilim ve İnovatif Teknolojiler Dergisi.Numara 31,2024.s.54-69. https://doi.org/10.30546/2616-4418.31.2024.1054

XÜLASƏ

XXI. Əsrdə təhlükəsizlik məsələsi və silahlar: Stuxnet

Alper ASLAN
Dokuz Eylül Universiteti, Sosial Elmlər İnstitutu, Avropa Birliyi Bölməsi, Avropa Araşdırmaları üzrə Doktorantura Proqramı, İzmir, Türkiyə

Elm və texnologiyanın təkamülü, beş hiss orqanının qəbul etdiyi konkret dünyadan kənarda mücərrəd və virtual dünya yaratmışdır. Virtual dünya dövlətlər üçün müasir təhlükəsizlik problemlərinə çevrilən özünəməxsus alətləri ilə yanaşı əhəmiyyətli təhlükələri də ehtiva edir. Əvvəlcə İrana, sonra isə bütün dünyaya təsir edən Stuxnet, mücərrəd silahların yeni dövrünün ilk addımlarıdır. 2010-cu illərin əvvəllərində 2008-ci ildə başlayan Stuxnet hücumundan yalnız xəbərdar olan İran kiber müharibənin ilk hədəfidir. Lakin Stuxnet-in əhəmiyyəti təkcə bir dövlətə hücumu ilə məhdudlaşmır.

Bu araşdırma Stuxnet-ə yönəlib. Stuxnet-in strukturu araşdırılaraq, hədəfinin nə olduğu, hədəfinə çatıb-çatmadığı, necə işlədiyi və necə aşkarlandığı kimi suallara cavablar axtarılır və oxşar təhdidlər üçün müxtəlif təkliflər verilir.

Açar sözlər: *Kritik İnfrastrukturlar, Kiber Hücum, SCADA, Stuxnet, Zero-day*

РЕЗЮМЕ

Проблемы безопасности и оружие в XXI веке: Stuxnet

Альпер АСЛАН
Университет Докуз Эйлюль, Институт социальных наук, Департамент Европейского Союза, Программа докторантуры по Европейским исследованиям, Измир, Турция

Развитие науки и техники создало абстрактный и виртуальный мир, выходящий за рамки конкретного мира, воспринимаемого пятью чувствами.Виртуальный мир таит в себе значительные угрозы и уникальные инструменты, которые стали современными вызовами безопасности государств.Stuxnet, который сначала поразил Иран, а затем и весь мир, — это первые шаги в новую эру абстрактного оружия. Иран, который узнал об атаке Stuxnet, начавшейся в 2008 году, только в начале 2010-х годов, стал первой целью кибервойны. Однако значение Stuxnet не ограничивается его атакой на одно государство.

Данное исследование посвящено Stuxnet. Изучается структура Stuxnet, чтобы найти ответы на такие вопросы, как его цель, достиг ли он своей цели, как он работал и как был обнаружен, а также высказываются различные предположения относительно подобных угроз.

Ключевые слова: *Критические инфраструктуры, Кибератака, SCADA, Stuxnet, Нулевой день*