Gelişmiş Sürekli Tehditler
Advanced Persistent Threats

Murat AKIN
Gazi Üniversitesi
Teknik Bilimler Meslek Yüksekokulu
Elektronik ve Otomasyon Bölümü
Ankara, TÜRKİYE
muratakin@gazi.edu.tr

Şeref SAĞIROĞLU
Gazi Üniversitesi
Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü
Ankara, TÜRKİYE
ss@gazi.edu.tr

Öz

Virüsler, solucanlar ve casus yazılımlar üzerinden yapılan saldırıların yanı sıra son birkaç yıl içerisinde geliştirilen ve adına gelişmiş sürekli tehditler denilen tamamen hedefe odaklı, iyi şekilde düzenlenmiş ve organize olmuş ve en önemlisi arkasında büyük kuruluşlar, devletler veya destekler olduğu bilinen yeni bir saldırı türü ortaya çıkmıştır. Bu çalışmada gelişmiş sürekli tehditler incelenmiş olup gelişmiş sürekli tehditlerin genel yapısı ve karakteristik özellikleri araştırılmış, geçmiş dönemde yapılan saldırılar ele alınarak, saldırı sonunda hedeflenen sonuçlara ne kadar ulaşabildiği değerlendirilmiştir. Son olarak bu tip tehditlere karşı alınabilecek önlemler sunulmuştur.

***Anahtar Sözcükler*— Gelişmiş Sürekli Tehdit, GST, Siber Saldırı, Siber Güvenlik**

Abstract

In addition to attacks using such as viruses, worms, spyware, etc., a new attack type developed over the past few years is called as "APT-Advanced Persistent Threats". APTs have emerged completely target oriented, well-arranged and well-organized, professionally backed up threats supported by large organizations, institutions and governments. This study reviews APTs, their general structures and characteristics, their successes to targets. Finally, measures can be taken against this type of threat are presented.

***Keywords*— Advanced Persistent Threat, APT, Cyber Attack, Cyber Security**

Gönderim ve kabul tarihi : 16.11.2016 - 01.07.2017

1. Giriş

Günümüzde kurum ve kuruluşlara karşı hedeflenen siber saldırıların giderek arttığı ve daha karmaşık, daha ciddi ve daha kapsamlı oldukları görülmektedir. 2000'li yılların ortalarında siyah şapka topluluğu kargaşa peşinde koşan genç bilgisayar korsanlarından ziyade organize olan tam donanımlı korsanlara doğru evrimleşmekte ve kurumsal-hükümet ağlarında biriken son derece büyük miktardaki veriler bu topluluğun hedefi haline gelmektedir. Daha yakın bir zamanda mobil, bulut ve sanallaştırma teknolojilerini içine alan IT altyapısında ve kullanım modellerindeki değişiklikler, klasik güvenlik tedbirlerini devre dışı bırakarak saldırganlar için rahat ve kolay erişilebilir ortamlar hazırlamaktadır. Belirtilen kapsam içinde en önemli tehdit, gizli hükümet aktörleri tarafından uzun vadeli ve hedefi iyi belirlenmiş uluslararası casusluk ve sabotaj olaylarına maruz kalmaktır. Bu gibi uzun vadeli ve hedefi iyi belirlenmiş devlet veya büyük organizasyonların arkasında oldukları saldırılara Gelişmiş Sürekli Tehditler (Advanced Persistent Threats) denmektedir. Bu terim son zamanlarda moda haline gelmiş ve bazı medya kuruluşları ve teknoloji sağlayıcılar tarafından yanlış anlamlarda kullanılmaktadır. Gelişmiş Sürekli Tehditler bugünün dünyasında gerçek anlamda siber güvenlik adına tehdit oluştururken bu tehditleri daha kapsamlı anlamak büyük bir önem teşkil etmektedir. Sadece gerçek tehditleri fark ederek hedefli saldırıları yöntemlerinin ve tekniklerinin daha geniş alanda nasıl ilişkili olduğunu görmesi, kuruluşların önümüzdeki yıllar içinde sahip oldukları bilgiler için koruyucu olacaktır.

2. Gelişmiş Süre

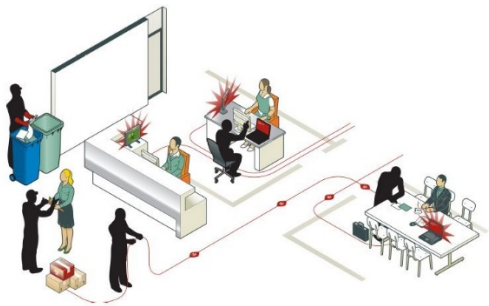
3. kli Tehditler

Gelişmiş Sürekli Tehditler(GST), genellikle yabancı bir devlet olan ve bir kuruluşu hedef alarak karşı taraftaki varlığı başarılı bir şekilde ele geçirmeden durmayan, uzun süreli erişime sahip olarak veri elde etmeye çalışan tehdidi tanımlamak için kullanılır. Gelişmiş sürekli tehditler için temel kavramlar gizli, hedeflenmiş, uyarlanabilir ve veri odaklı olmasıdır.

2.1 Gelişmiş Sürekli Tehditlere Giriş

GST, iyi bir şekilde kaynak sağlanmış, yüksek yeteneğe sahip ve amansız bir saldırgan grubu tarafından gerçekleştirilen saldırılardır. GST yeni olmasa da yapılan saldırılar ve bu işi yapısı gereği birçok kurum ve kuruluş klasik saldırganlara karşı mevcut savunma sistemlerini değiştirmeleri gerekliliğini fark etmişlerdir. Günümüzde GST 1990'lı yılların saldırganlarını değil iyi organize ve finanse olmuş profesyonellerin uğraş verdiği bir alandır. Birçok kişi siber saldırıların ve saldırganların savaş oyunları ve hacker filmlerindeki olaylar ve karakterlerle ilgili olduklarını düşünmekte bu gibi saldırıların verebilecekleri zararların farkında değillerdir. Günümüzde hassas kritik bilgiler bilgisayarlarda saklanmakta, kurumlar işleyişlerini ağ üzerinden yürütmekte ve e-ticaret ile yapılan alışverişler milyonlarca lirayı bulmaktadır ve bu sebeplerde saldırganları daha da profesyonel hale getirmektedir. Esasında herhangi bir kimsenin istediği bir bilgi dünya üzerinde bir bilgisayarda mevcuttur. Eğer kişi uygun tarama ve keşif yapabilirse bu bilgiye istediği şekilde ulaşabilmektedir [1]. GST saldırıda saldırganın hedef kurumda tarama ve keşif süreci, çalışanlar ile iletişim kurmasıyla olabileceği gibi kurum içerisindeki bir evrakın elde edilmesi ile de olabilir. Örnek bir tarama keşif süreci Şekil 1'de gösterilmiştir [2].

GST'nin karmaşık saldırı yolları ve yapısından dolayı kurban etkilendiğinin ve saldırı altında olduğunu anlaması aylarca hatta bazı durumlarda yıllarca alabilmektedir. İşin daha kötü tarafı ise güncel güvenlik araçlarının mevcut GST saldırılar için herhangi bir önlem alamamasıdır. Bazı durumlarda, ağ yapısında izlenebilirlik sağlandığında kayıt dosyaları(log) ile şüpheli durumlar tespit edilebilmekte ve bunlara karşı önlem alınabilmektedir [3].



Şekil 1. GST bir saldırıda saldırganın tarama-keşif süreci [2].

Siber tehdit kapsamında ifade edilen GST teriminin her bir ifadesi ayrı bir anlam taşımaktadır. Bu açıdan bakıldığında bu terimin kavramları şu şekilde açıklanabilir.

- Gelişmiş: Bir saldırgan sisteme yakalanmadan bilgi kazanma konusunda yetenekli, iyi korunan bir ağa sürekli erişebilen ve önemli bilgileri ele geçirebilen kişidir. Saldırgan genellikle yeterli kaynaklara sahiptir ve sisteme çabuk uyum sağlayabilmektedir. GST'yi oluşturan terimler içerisindeki gelişmiş ifadesi saldırganın özelliklerini tanımlamaktadır.
- Sürekli: Bir tehdidin sürekli olması o tehdidin bilgisayar ağına erişiminin sürekli olması anlamına gelmektedir. Yani saldırgan bilgisayara bir kere erişim sağladığında istediği bilgiye ulaşana kadar sistemde kalabilmektedir ve saldırganın sistemden uzaklaştırmak son derece zordur.
- Tehdit: Kişi veya kurumların sahip oldukları bilgilerin başka kişilerin erişim isteğine karşı maruz kaldığı durumu ifade etmektedir. Bir saldırgan ulaşmak istediği bilgi için sadece istekli değil aynı zamanda yeteneklidir [4].

2.2 Gelişmiş Sürekli Tehditlerin Genel Yapısı

Bir GST saldırısını önceki yıllarda yapılan saldırılara kıyasla daha gizli ve sinsi saldırılar yapan özellikleri çok-yönlü, kapsamlı olması ve sosyal mühendislik, otomatik araçları da içeren birçok atak tekniği kullanmasıdır. GST saldırıların genel saldırı stratejileri şu şekilde sıralanabilir.

- Saldırgan sistemde sosyal mühendislik ve kötü amaçlı yazılım kullanarak tutunacak bir alan arar.
- Sonrasında saldırgan kurban ettiği sistemde bir komut istemci açarak sistemin ağa bağlı olup olmadığını test eder.
- Kurban cihaz ağa bağlandığında saldırgan sistem üzerinde port taramasına başlar.
- Böylelikle saldırgan uygun bütün portları listeler, başka sistemlerde çalışan servisleri ve diğer ağ bölümlerini de keşfetmiş olur.
- Artık saldırganın elinde tüm ağın haritası mevcuttur ve onun için en değerli kurbanı bulduğu anda o sistemdeki bilgileri alabilir veya yok edebilir.

Sosyal mühendislik bilgi sistemlerini ele geçirmek için kullanıcıları avlama sanatı olarak ifade edilebilir [5]. Sistemlere teknik saldırılar yerine sosyal mühendislerin hedefinde bilgisini elde edeceği insanları manipüle ederek gizli bilgilerini açığa çıkarmak veya kötü niyetli yazılımlarını hissettirmeden tesir ettirmek vardır. Sosyal mühendislik yapıldığında teknik önlemler yetersiz kalmaktadır. Buna ek olarak çoğu insan da böyle saldırıları tespit edebileceğini düşünmektedir. Araştırmalar [6] ise tam tersini yani insanların bu tür saldırıları tespit etme de son derece yetersiz olduğunu ortaya çıkarmıştır.

Sosyal mühendislik çok yönlü olmakla birlikte mevcut saldırıların farklı aşamalarında kullanılmaktadır. Sosyal mühendislik genel olarak üç başlık altında incelenebilir. Bunlar fiziksel yaklaşımlar, sosyal yaklaşımlar, tersine sosyal mühendislik olarak ifade edilmiştir. Fiziksel yaklaşımda kurban hakkında araştırma yapılırken fiziksel nesnelerden yararlanılmaktadır. Sıklıkla kullanılan dumpster diving yönteminde bir şirkete ait bir çöp kutusunda kimlik bilgileri, parola gibi bilgilerin yazılmış olduğu kâğıtlar bulunabilir. Sosyal yaklaşımda, sosyo-psikolojik metotlar kullanılmaktadır. Kurban veya çevresi ile sosyal anlamda ilişkiler kurmak bu kapsamda değerlendirilebilir. Tersine sosyal mühendislikte ise saldırgan kurban ile direk iletişim kurmak yerine zamanla kendisinin yetkili ve güvenilir biri olduğunu ikna etmektedir. Böylelikle kurban istemeden güvenilir olduğuna inandığı kişiye gizli bilgilerini verecektir [7].

GST saldırıların birçoğu sosyal mühendislik yapılarak gönderilen maillerle yapılmaktadır. Bütün saldırılar e-mail yolu ile değil bazı durumlarda sıfır gün saldırısı ile kombine edilerek düzenlenmektedir. Saldırıya uğrayan kurbanlar genellikle saldırı detaylarını paylaşmaz iken sadece RSA saldırısında bir takım bilgiler verilmiştir. RSA saldırısında meydana gelen durum tipik saldırı durumudur[2].

Bir saldırgana ait kötü yazılım veya uygulama erişimi sürekli tutmak için ele geçirilmiş bir bilgisayarda çalıştırıldığı zaman bu sistemde süreklilik mekanizması vardır. Ayrıca saldırgan, uzaktan kontrolü sağlaması için hedef sistem ile sürekli irtibatta olması gerekmektedir. Günümüzde sağlanan bu uzaktan kontrol içeriden ve dışarıdan kaynaklar ile olabilmektedir[8].

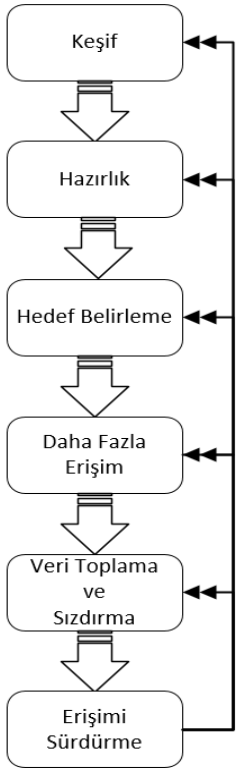
Buraya kadar anlatılanlar ile GST bir saldırının genel yapısı ortaya konulmuştur. Aşağıdaki maddeler ise GST saldırı yapısını maddeler halinde listelemiştir [9].

- Keşif: Saldırgan saldıracağı kurbanın bilgilerini en iyi saldırı yöntemi için toplamaktadır. Bu bilgiler toplanırken hedefin çalışma ortamının konum bilgisi, kullanılan bilgisayarların konum bilgisi, kurum tarafından kullanılan teknolojiler, kendi aralarında nasıl iletişim kurdukları(ofis arasında, müşteriler, tedarikçiler ve ortaklar arasında), müşteri bilgileri, ilgi alanları ve adres bilgileri gibi bilgiler de toplanmaktadır.
- Hazırlık: Saldırgan saldırmak istediği kurban için aktif olarak saldırı hazırlamakta, geliştirmekte ve uygun araçlarla test etmektedir. Bu aşama sistem açıklarını saptama, kötü amaçlı kod yazımı veya elde edilmesi, uygun sosyal mühendislik maillerinin hazırlanması ve hangi uygun hesaptan gönderileceğinin belirlenmesi gibi hazırlıklar yapılmaktadır. Ayrıca saldırgan bu aşamada saldırı için ihtiyaç duyacağı gerekli donanımı da temin etmekte, saldırı esnasında kullanacağı saldırı altyapısını oluşturmakta ve bunları uygun bir şekilde test etmektedir.
- Hedef Belirleme: Saldırgan atağını gerçekleştirdikten sonra bıraktığı izleri takip eder ve hata varsa bunları kontrol eder. Gönderici bir açığı kullanarak sunucu bilgisayarı ele geçirmeye çalışabilir, stratejik bir cihaza USB bağlayabilir, sosyal mühendislikle bir e-mail gönderebilir ve bu ilk eylemlerden sonra sistemden bir işaret bekleyebilmektedir. Geri dönen işaret ile kurban belirlenecek saldırı gerçekleşecektir.

- Daha Fazla Erişim: Bir saldırgan sisteme erişim sağladığında ilk yaptıkları iş, bulundukları bilgisayar ağın neresinde olduklarını tanımlamaktır. Sonraki hamlesi ise ağda komşu düğümler arasında yana doğru ilerleme sağlamak ve her geçtiği düğümde bir açık kapı bırakmaktır. Bu aşamada genellikle ikinci ve üçüncü adımlar olan hazırlık ve hedef belirleme aşamaları tekrar edilir. Kötü amaçlı yazılımlar ve araçlar yüklenir, ağ tanımlaması tekrar yapılır ve açık bırakılan düğümler işaretlenir. Bu aşamada domain kontrole ve şifresine erişmek için bazı çalışmalarda yapılır.
- Veri Toplama ve Sızdırma: Bir saldırgan istediği verileri belirledikten sonra bu bilgileri toplamaya başlamaktadır ve elde edilen bilgileri veya kendine ait izleri, programları, araçları başka bir yere (exfiltrasyon) kaydırmaktadır. Eğer saldırgan "kır ve elde et (smash and grab)" yöntemini kullanırsa istediği veriyi başka bir yere tespit etmeden taşımakta, eğer "düşük ve yavaş (low and slow)" yöntemini tercih ederse küçük parçalar halinde daha uzun sürede taşımaktadır.
- Erişimi Sürdürme: Saldırgan sisteme bir kez erişim sağladığında ve istediği bilgiyi elde ettiğinde sisteme erişimin devam etmesini ister. Bu aşamada sistemde tespit edilmeyi önlemek için kötü amaçlı yazılımların ve araçların çalışmasını minimize edilmekte, açık bırakılan arka kapıların istenildiği şekilde çalışıldığından emin olmak için periyodik olarak bu kapılarla iletişim kurulmakta gerekli ve uygun değişiklikler yapılmaktadır. Eğer otomatik bilgi toplama araçları kullanılmışsa bu arama araçları için arama terimleri güncellenmekte exfiltrasyon yolu ve sıklığı kontrol edilmektedir. Eğer bu aşamada bağlantı kaybedilirse saldırgan birinci aşamaya dönmek zorunda kalabilmektedir [3,9]. GST saldırıların genel işleyişi şekil 2'de görülmektedir.

2.3 Siber Tehditler için GST Rolü

Birçok güvenlik ihlali durumlarında GST anahtar rol oynamaktadır. GST genellikle çalışan süreçleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program veya programlar grubu olarak ifade edilen rootkitlerin etkin olduğu ve yetkilendirmenin arttırılarak ele geçirilen ağdaki diğer bilgisayarlardaki bilgilerin ele geçirildiği bir yöntemdir.

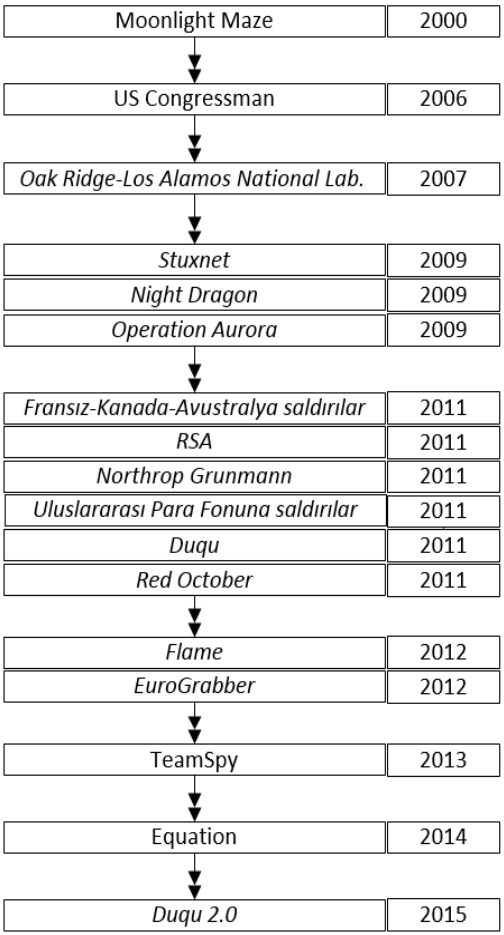


Şekil 2. GST genel işleyişi [9]

GST saldırılar nadiren pasif olarak fark edilebilmektedir ve bunun için mevcut sistemde aktif ve sürekli devam eden güvenlik ve trafik analizi yapılması gerekmektedir. İnternet ve günümüz şartlarındaki sınırsız ağlardan önce bir saldırgan bir kurumun bilgilerini erişmek istediği zaman bilgilerin saklandığı yere fiziksel erişim yapması gerekmekteydi. Günümüzde maalesef hassas veriler fiziksel donanıma bağımlı değildirler ve saldırganlar internete bağlı bir cihazla isimsiz olarak uzaktan erişim yapabilmektedirler. Kötü amaçlı yazılımlar internet ile birlikte gelişmektedirler ve saldırganlara için bir saldırı seçeneği olmaktadırlar [10,11,12].

2.4 Geçmiş Dönemde Gerçekleşen GST Saldırılar

Medya raporlarına ve kamusal duyurular dikkate alındığında Şekil 3'de önemli ve kayda değer GST saldırıların bir tarihi görülmektedir. Birçok durumda tek bir operasyon benzer ihlallere, ihlal denemelerine ve etkilenen çok sayıda hedefe isim vermiştir [9,13].



Şekil 3. Önemli GST Saldırıların Kronolojisi

Mart 2000 Moonlight Maze*:* Moonlight Maze adı verilen siber saldırı Pentagon, Nasa ve Birleşik Devletler Enerji Bakanlığı, araştırma laboratuvarları ve özel üniversitelere ait bilgisayarları hedef almıştır. Güvenlik uzmanlarının bu saldırı ile ilgili tespiti Mart 1998'de olmuştur. Ulusal altyapı koruma merkezinden sorumlu yetkili saldırının Rusya merkezli olduğunu ifade etmiştir. Saldırı sonrasında Pentagon şifreleme ve saldırı tespit sistemlerini güncellemek için 200 milyon dolar bütçe ayırmıştır [14].

Ağustos 2006 - US Congressman*:* İki kongre üyesine ait bilgisayar ele geçirilmiş olarak raporlanmıştır. Çalınan bilgilerin kritik bilgiler olup Çin-Pekin rejimine karşı muhaliflerle ilgili olduğu bildirilmiştir [9].

Ekim-Kasım 2007 - Oak Ridge - Los Alamos National Laboratory: Oak Ridge National Laboratory yapılan saldırılar başarılı bir şekilde sosyal mühendislik mailleri ile gerçekleştirilmiş ve mail yoluyla yapılan yazışmalar yasal bir şekilde yürütülmüştür. Tesisi ziyaret eden ziyaretçilere ait bilgilerin bulunduğu bilgisayarlar ele geçirilmiştir. Saldırganların veri tabanındaki tüm bilgileri çaldıkları tahmin edilmektedir Los Alamos National Laboratory bütün müşterilerine tanımlanamayan 'Sarı' ağda etkilenmiş küçük sayıdaki bilgisayarlara gönderilen kötü amaçlı bir mail için uyarması ile ortaya çıkmıştır. Önemli miktarda sınıflandırılmamış veri çalınmıştır. Saldırının geniş çapta ve koordineli olarak Birleşik Devletler enstitü ve laboratuvarlarını hedef aldığı düşünülmektedir [9].

Haziran 2009 – Stuxnet: Literatüre hedefli ilk saldırı olarak geçen Stuxnet solucanı, İran'ın Natanz kentinde bulunan uranyum zenginleştirme tesisini hedef almıştır. İran bu nükleer santralin sadece ülkede elektrik üretimine katkıda bulunacağını savunmuş fakat uluslararası tartışmalar da beraberinde gelmiştir. Stuxnet solucanı USB bellek ile Natanz tesislerindeki bilgisayarlara bulaştırılmış ve bu solucan kendini kopyalayarak çoğalmıştır. Temel amacı genellikle PLC(Programmable Logic Controllers) kullanan ve gerçek zamanlı veri toplama, kontrol ve izleme yapan SCADA sistemleri etkileyerek hatalı çalışmalarına yol açmaktır. Parola-kimlik hırsızlığı, spam-mail ve DDoS ataklar yapan diğer zararlı yazımların aksine Stuxnet bu saldırıların hiçbirini yapmamıştır ve sadece Microsoft tabanlı bilgisayarlarda yayılarak Siemens Step-7 endüstri tabanlı sistemlere zarar vermeyi hedeflemiştir. Bir bilgisayarı etkileyen Stuxnet solucanı, yerel ağda paketleri dinleyerek kendi üzerinden geçiren ve "man-in-the-middle" saldırısı olarak da bilinen saldırıyı yapmıştır. Bu yöntem ile elde edilen ağ paketlerindeki PLC kodlarını değiştirerek sisteme zarar verilmiştir.[15].

Kasım 2009- Night Dragon: 2009 Kasım ayı başlarında gizli, koordineli ve hedeflenmiş siber saldırıların küresel petrol ve gaz şirketlerine karşı yapıldığı gözlemlenmiştir. Night Dragon adı verilen bu ataklar sosyal mühendislik mailleri kullanılarak Windows işletim sistemi açıklarından faydalanılarak bilgisayarlarda erişim hakkı elde etmek için yapılmıştır. Kazanılan erişim hakkı ile bilgisayarlardaki petrol ve gaz üretim sistemlerinin bilgileri ve şirketlere ait finansal dokümanlar ele geçirilmiştir [9].

Ocak 2010 – Operation Aurora: Google firması 2010 yılının ocak ayında kendi şirket altyapısına yapılan ve

fikri mülkiyet haklarını çalmak üzere düzenlenmiş karmaşık bir saldırı olduğunu tespit etmiştir. Firma kendi sayfasından Çin orijinli bir siber saldırıya uğradığını duyurmuştur. Açıklamadan kısa bir süre sonra Adobe firması da kurumsal sistemlerinin saldırı altında olduğunu açıklamıştır. Spear-phishing temeline dayanan bu saldırı türü kullanıcılara Microsoft Messenger üzerinden bir link yollamakta ve kullanıcı bu linke tıkladığında Trojan.Hydraq isimli zararlı yazılım bilgisayara bulaşmaktaydı. Operation Aurora adı verilen saldırıda Google ve Adobe başta olmak üzere Symantec, Yahoo ve Northrop gibi firmaların aralarında bulunduğu 32 firma hedef alınmıştır. [16].

Mart-Haziran 2011 – Fransız, Kanada ve Avustralya Hükümetlerine saldırılar: Fransız hükümeti, Kanada hükümeti ve Avusturalya parlamentosu sosyal mühendislik yapılarak gönderilen mailler ile yapılan saldırılara maruz kalmışlardır. Fransa Ekonomi Bakanlığı ve Merkez Finans Servislerine ait 150'den fazla bilgisayar ele geçirilmiştir. Saldırganlar bu devlet kurumlarına ait bilgisayarları üç ay boyunca uzaktan kontrol edebilmiş ve veri kaynaklarına erişebilmişlerdir. Saldırganlar özellikle Fransa'nın başkanlık yaptığı G20 zirvesi ve uluslararası ekonomik olaylarla ilgili belgeleri aradıkları tespit edilmiştir. Kanada hükümetine saldırının hedefinde yönetim kadrosu vardır ve saldırı sonucunda hükümete ait gizli bilgiler çalınmıştır. Avusturalya parlamentosuna yapılan saldırı da ise parlamentoya ait bilgisayarlara bir ay süreden fazla erişim sağlanmış ve bu zaman zarfında Avustralya Başbakanı, Dışişleri Bakanı ve Savunma Bakanının da içinde olduğu birkaç kişinin binlerce mailine ulaşılmıştır [9].

Mart 2011 – RSA: RSA şirketine sosyal mühendislik yolu ile yollanan mailler ile saldırı gerçekleştirilmiştir. Saldırgan iki günlük periyodlar ile kurbanlarına iki farklı tipte mailler yollamıştır. Şirket içerisindeki alt kademedeki çalışanlara "2011 yılı işe alımlar" konulu ve Excel dosya ekli mail atılmış kullanıcılar maile ekini açtıktan sonra bilgisayar etkilenmiştir. Adobe Flash açığından yararlanılarak yapılan sıfır gün saldırısı ile birtakım veriler şirket dışına sızdırılmıştır [17].

6 Mayıs 2011 – Northrop Grunmann: ABD merkezli, uzay ve savunma teknolojileri alanında faaliyet gösteren, 1994 yılında Grunmann ve Northrop girişimiyle kurulan küresel savunma şirketi olan Northrop Grunmann herhangi bir uyarı yapmadan ağ erişimini kesmiş ve bütün şirket çapında şifreleri yenilemiş ve bu eylemlerin muhtemel bir RSA saldırısına maruz kaldığı söylentilerini çıkarmıştır [9].

Mayıs-Haziran 2011 – Uluslararası Para Fonuna (IMF) saldırılar: Yapılan saldırıda en az bir IMF'ye ait bilgisayar geniş ve karmaşık bir siber atağa maruz kaldığı ve bu saldırının önemli bir keşif süreci ve IMF için özel yazılmış bir program ile yapıldığı ifade edilmektedir. Ele geçirilen bilgisayar sistem içi dosyalara erişim amacıyla kullanılmıştır. Saldırganların eriştikleri bilgiler hassas ekonomik veriler ve politik kararları içermekteydi [9].

Eylül 2011 – Duqu: 2011 yılında keşfedilen Duqu Şubat 2010'dan beri aktif olduğu tahmin edilmektedir. Stuxnet ile oldukça benzerlik gösteren Duqu aynı saldırganlar tarafından geliştirildiği fakat farklı amaçlara odaklandığı düşünülmektedir. Hedefinde ise İran, Sudan, Fransa ve Macaristan bulunmaktadır. Duqu saldırısında temel hedef sabotaj yerine casusluk yapmaktır. Microsoft Word dosyasında bulunan True Type font açığından yararlanarak sıfır gün saldırısı düzenlenmiştir. Duqu yazılımı kendini çoğaltmamakla birlikte saldırgan hedef aldığı bilgisayarı bir sonraki hedef için bir adım olarak kullanmıştır. Ayrıca saldırılarda key-logger yöntemi ile elde edilen verilere XOR şifreleme yapılmıştır [18].

Ekim 2012 – Red October: Kırmızı Ekim diye adlandırılan kötü bir yazılım hükümet ve araştırma kurumlarından gizli bilgileri çalmak için tasarlandığını Kaspersky firması tarafından kamuoyuna açıklamıştır. Diğer kötü yazılımlardan farklı olarak küçük bir mimari yapıda bir ana bileşenin C&C(Command&Control) sunuculara bağlanması ile saldırı gerçekleştirilmiştir. Saldırgan tarafından verilen komutla yaklaşık 1000'den fazla modül fonksiyonu gerçekleştirilmek üzere çalıştırılmıştır. Bu modüllerin bazı karakteristik özellikleri Iphone ve Nokia marka mobil cihazlardan bilgi aktarımı, ağ cihazlarına erişim sağlamak için SNMP brute force saldırı ve taşınabilir hafıza birimlerinden silinen dosyaların tekrar geri getirilmesi gibi fonksiyonları kapsamaktadır. Ayrıca bu modüller klavye karakteri ve ekran yakalama fonksiyonu ile Outlook e-posta mesajları engelleyebilmektedir. Saldırı yapılırken Microsoft Word ve Excel programlarının açıklarından yararlanılmıştır. Saldırıda C&C sunucuları erişim dışı kalsalar bile kullanılan malware ile Office programlarına yerleştirilen plug-in, saldırganın özel e-posta göndermesini ve tekrardan kontrolü ele geçirmesini sağlamaktadır [18].

2012 – Flame: İlk olarak Mayıs 2012'de keşfedilen Flame saldırısının 5-8 yıldan beri aktif olduğu tahmin edilmektedir. Başka tür saldırılar araştırılırken tesadüfen keşfedilmiştir. Bu malware ait en ilginç özellik tüm modülleri ile birlikte yaklaşık 20 Megabayt

civarında bir büyüklüğü olmasıdır. Flame ile Stuxnet ve Duqu arasında çok güçlü bir bağ kurulamasa da genel kod yapısı ve fonksiyonları benzerlik göstermektedir. Bu yüzden Stuxnet ve Duqu saldırılarını gerçekleştiren aynı saldırganlar değil fakat işbirliğinde olan saldırganların yaptığı tahmin edilmektedir. Flame, Duqu'ya benzer olarak bilgi sızdırmayı hedeflemiş fakat bunu Ortadoğu'daki ülkeler başta olmak üzere binlerce Windows tabanlı sisteme çok geniş alanda yapmıştır. Büyük ve karmaşık bir yapıya sahip olan Flame malware yazılımı USB flash belleklerle yerel ağlarda yayılması için tasarlanmıştır. Kendini çoğaltma yeteneği olmayan malware için saldırgan iki farklı sıfır gün(Yazıcı Kuyruğu ve Windows Shell) açığını kullanarak başka bilgisayarları etkilemesini sağlayabilmektedir. Flame saldırısında C&C sunucu için 80'den fazla domain kullanılmış olup şifreleme tekniği olarak XOR şifreleme ve RC4 algoritmaları kullanılmıştır [18].

Aralık 2012 – EuroGrabber: Aralık 2012'de güvenlik sağlayıcıları Versafe ve Checkpoint şirketleri adı EuroGrabber olan karmaşık saldırıyı duyurdular. Truva atı ile yapılan saldırıda 30 Avrupa bankasında 30 binden fazla banka müşterisinin hesabından tahmini 36 milyon Euro çalındığı ifade edildi. ZITMO yani Zeus-in-the-mobile-trojan yazılımın farklı bir versiyonu Eurograbber saldırısında kullanılmıştır. Saldırı Zeus yazılımın e-posta avlama yöntemi ile kurbanın bilgisayarına bulaşması ve daha sonra kurban bankacılık işlemleri için banka sayfasını açtığında ek güvenlik için mobil telefona link yollaması ile başlamaktadır. Sonraki aşamalarda mobil yazılıma gelen linke tıklayan kurban farkında olmadan mobil cihazın modeline göre kötü yazılımı cep telefonuna yüklemekte ve saldırgan sahip olduğu banka hesap ve cep telefonu bilgileri ile kullanıcı hesabından para transfer yapabilmektedir. Saldırı İtalya'da başlayıp hızlı bir şekilde İspanya ve Hollanda başta olmak üzere birçok Avrupa ülkesinde gerçekleşmiştir [19,20].

Mart 2013 – TeamSpy: Siber tarama faaliyetlerini kapsayan TeamSpy saldırısı Bağımsız Devletler Topluluğu ve doğu Avrupa ülkelerindeki yüksek seviyedeki politikacıları ve insan hakları örgütlerini hedef almıştır. Saldırgan kurban bilgisayarları yasal dijital sertifikası olan ve yüz milyondan fazla kullanıcısı bulunan TeamViewer uzaktan erişim programı ile kontrol etmektedir. Bir tarama ve veri sızdırma operasyonu olan TeamSpy kurbanlarından klavye hareketleri ve ekran bilgilerini, gizli şifre ve içerikleri, Itunes programı ile Apple cihazların geçmişi gibi bilgileri sızdırmaktadır. Saldırının belirtilen ülkelerde hala aktif olduğu düşünülmektedir [21].

2014 – Equation: Equation grubu çok yönlü, tam donanımlı ve şimdiye kadar görülen en tehlikeli saldırgan bir grup olarak tanımlanmaktadır. Bu saldırgan grubu kullandıkları şifreleme algoritmaları, gizlenme stratejileri ve saldırı esnasında kullandıkları gelişmiş teknikler ile dikkat çekmektedir. Kullandıkları kötü amaçlı yazılımlar için çeşitli isimlendirmeler yapılmış olup GrayFish, Fanny ve EquationDrug öne çıkan yazılımlardır. Equation grubu saldırıları gerçekleştirirken kendini çoğaltabilen solucandan(Fanny), Cd-rom gibi fiziksel medya aygıtlarından veya web tabanlı açıklardan yararlanmaktadırlar. Kullandıkları şifreleme algoritmaları RC5,RC6 ve XOR şifreleme tekniklerdir. İran, Rusya, Pakistan başta olmak üzere 30'un üzerinde ülkede faaliyet göstermektedirler. Hedeflerinde hükümet ve diplomatik kurumlar, telekomünikasyon sistemler, nükleer enerji, doğalgaz üretim ve askeri tesisler vardır [22].

2015 – Duqu 2.0: 2011 yılında ortaya çıkan ve 2012 yılında aktif olmayan olan Duqu saldırısının gelişmiş bir versiyonu olarak tanımlanmaktadır. Üç adet sıfır gün açığından faydalanan Duqu 2.0 saldırısında gelişmiş kötü amaçlı yazılımlar kullanılmaktadır. Şimdiye kadar olan tüm saldırılardan farklı bir süreklilik mekanizması olan bu saldırının sadece bilgisayar hafızasında kod gizleme özelliği tespit edilebilmiştir. BM daimi üyesi beş ülke olan Rusya, ABD, Çin, Fransa ve İngiltere'nin yanı sıra Almanya'yı kapsayan P5+1 olarak adlandırılan ülkelerin birlikte yaptığı faaliyetleri hedef almıştır. Duqu 2.0 saldırısının gelecekteki tüm GST saldırılar için örnek teşkil edeceği düşünülmektedir [23].

4. GST saldırılara karşı Savunma

GST saldırılardan korunmak için birçok kurum ve kuruluş yüksek seviyede savunma stratejisi kullanmaktadır. Her zaman dikkat edilmesi gereken nokta korunmanın ideal olduğu fakat tespit sisteminin mutlaka gerektiğidir. Kurumların çoğu sadece önleyici tedbirler üzerinde durmaktadır fakat GST saldırılarının esas problemi kötü niyetli kişinin sisteme dâhil olması ve trafik akışını hissettirmeden izlemesidir. GST saldırılara karşı alınabilecek tedbirler şu şekilde sıralanabilir [1].

1. *Kullanıcıları kontrol etmek ve farkındalığı arttırmak*: Genel kural şudur; bilinçsiz kullanımı engelleyemezsiniz fakat bilinçsiz kullanıcıyı kontrol altına alabilirsiniz. Birçok saldırgan kullanıcıların bir mail eklentisini açması ile ya da

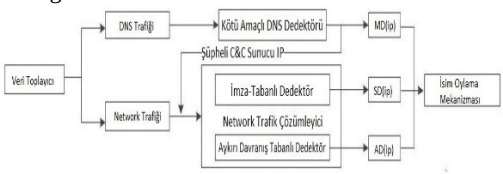
tıklamaması gereken bir bağlantıyı tıklaması ile ağa sızmaktadır. Tam bir farkındalık yaratmak ile ve kullanıcının hareketleri kısıtlama ile tehlikeler azalacaktır. Saldırganın keşif tarama süreci içerisinde yer alan kullanıcı avlama teknikleri, ağı kullanan kişi veya çalışanların bilinçlendirmesi ile önlenebilmektedir [1,24].

2. *İsim oylama yöntemini ağ davranışlarında yürütme*: Geleneksel güvenlik çözümleri ağ içerisinde iyi kötü olarak sınıflandırmakta erişime izin vermekte veya engellemektedir. Fakat gelişmiş ataklarda sınıflandırma yöntemi işe yaramamaktadır. Birçok saldırgan ağ içerisinde meşru davranarak ağ içerisinde şüphe çekmezler. Bu yüzden saldırganın ağa karışma hedefinden dolayı ağ içerisindeki hareketler için bir güven seviyesi belirlenerek kullanıcılara oy verme yöntemi uygulanabilir ve oylama mekanizmasının üreteceği güven değeri ile bir IP adresinin kötü amaçlı DNS ve trafik vektörlerinden etkilenip etkilenmediği belirlenebilir[1,25].

3. *Değişen saldırıları anlamak*: Bilinmeyen bir tehdide karşı savunmak yapmak oldukça zordur. Bu nedenle iyi bir savunma yapabilmek için saldırıyı iyice anlamak ve nasıl yürütüldüğünü bilmek gerekir. Eğer kurumlar yeni teknikleri ve saldırganların geliştirdikleri metotlarını anlamaya çalışmazlarsa savunma mekanizmalarını doğru ve etkin bir şekilde ayarlamazlar [1].

4. *Son noktayı yönetmek*: Saldırganların ağa bir giriş noktasından girmesiyle istediği bilgiye son noktada erişmektedir. Eğer zarar azaltılmak isteniyorsa hedeflenen son noktayı kontrol altına almak veya geçici olarak kilitlemek uzun süreli bir koruma sağlayacaktır [1,18].

5. *Ağın tüm trafiğine odaklanmak*: Mevcut ağ sistemin tüm trafiğinin izlenmesi GST saldırıları tespit etmek için etkin bir yöntemdir. Bunun için birçok makine öğrenme algoritması ve birçok modelleme belirli ağ özelliklerini ayırt etmek için kullanılmaktadır. Bilinen ataklar için imzaya dayalı tespit sistemi, ağda normal davranışlar dışında dağılım gösteren hareketleri tespit etmek için kullanılan olağan dışı durum tespit sistemi ve bu iki sistemin birleştirilerek kullanıldığı hibrit sistemler GST tespiti için uygulanabilmektedir. Ayrıca geliştirilen ihlal tespit sistemleri ile mevcut ağ DNS ve Network trafiği olarak ikiye ayrılmaktadır ve ağ trafiğinin uç yapılarında çalışarak bilinmeyen saldırıları da belirli özniteliklere dayanarak yakalayabilmektedir [24,25]. Örnek bir modelleme Şekil 4'de görülmektedir.



Şekil 4. Örnek GST Tespit Sistemi [25]

5. Değerlendirme

Çok uzun bir geçmişe sahip olmasa da GST saldırılar, günümüzde faaliyetlerini elektronik ortamda sürdüren kurum ve kuruluşlar için büyük tehlike arz etmektedir. Bu tür saldırıların gelecek yıllarda gitgide artacağı kesindir. Bunlardan korunmak için aşağıdaki hususlara dikkat edilmesi gerekmektedir. Bunlar:

1. Bu tür saldırıların önemli ve stratejik hedeflere yapıldığı unutulmamalıdır. Bu özelliğe sahip kurumlar bu konuya kaynak ayırmalı ve önlemler almalıdır.

2. Kurumlar açısından problemleri görmezden gelmek ilerisi için kuruma bir zarar gelebileceği anlamını taşıdığından, GST saldırılarının geleneksel saldırılardan farklı olduğu unutulmamalıdır.

3. GST saldırganları nereye saldıracaklarını çok iyi bilmektedirler ve bu tür saldırılar öncelikle hedeflenen sistemi tanımak için zaman harcamakta sonrasında sisteme özel kötü yazılımlar üreterek yapacağı saldırının başarısını arttırmaktadırlar.

4. Saldırganlar son derece organizedir. Bunun farkında olunmalı ve yetenek geliştirici özel ve genel önlemler alınmalıdır.

5. Kullanılan kötü amaçlı yazılım maksimum etkiyi verebilmek için isteğe göre hazırlanmaktadır. GST saldırılar arkasında büyük devletler olan, son derece eğitimli, motive edilmiş kişiler tarafından gerçekleştirilmektedir. Bu da saldırıyı yapacak kişilerin hedefine başarı ile ulaşmaları için yeterli kaynağa sahip oldukları anlamına gelmektedir.

6. GST saldırılar hedeflenmiş saldırılardır ve hedeflenmiş saldırıların tespiti zor olabilmektedir. Sağlam bir trafik-izleme ve ağ analiz sistemi çevre savunması için son derece yararlıdır fakat tam anlamıyla yeterli değildir. Ağ içerisinde davranış analizi de yapmak faydalı olacaktır.

7. GST saldırılar ile mücadele etmenin başlıca yolu kullanıcıları bilinçlendirmek ve farkındalık oluşturmaktır. Kullanıcı bilmediği epostaları açmamalı, rastgele linklere tıklamamalı, güncel tehditleri takip edip uygulamalıdır.

8. GST'ler içerisinde sıfır gün saldırıları içerdiğinden, çoğu zaman fark edilemez durumdadır. Bu tehditten tamamen olmasa da kısmen korunmak ancak ve ancak bilgi birikimi, yetenek, bu hususlarda çalışan uzmanlar ve bu konuda açıkları bulup yayımlayan sitelerin takip edilmesiyle önlenebilmektedir. Bu hususun farkında olunmalıdır. Saldırılardan tamamen korunulamasa da bu sayede sistemin etkilenme oranını oldukça düşecektir.

9. Kurum ve kuruluşların kendi sistemini ve ağını iyi bir şekilde tanımlaması ve yönetmesi gerekmektedir. Daha açık bir ifadeyle bir kurum ağ trafiğini ve servislerini iyi bir şekilde takip etmeli ve böylelikle sistemde bulunabilecek anormal durumları anında tespit edebilmeli, şüpheli durumları iyice araştırmalı, uzmanlardan destek almalıdır.

10. Alınacak önlemler ve tespit edilen zafiyetlerin ivedilikle giderilmesine yönelik aksiyon planları hazırlanmalı ve hayata geçirilmelidir.

11. Çözülemeyen problemler ile şüpheli durumlar ülkelerin müdahale merkezlerine (USAM) anında bildirilmeli ve destek istenilmelidir.

12. Üniversitelerde GST yeteneklerini anlama ve karşı koyma yeteneklerini geliştirici tezler yaptırılmalı, ulusal birikimler arttırılmalıdır.

13. GST'lere karşı koyabilmek için ulusal bir grup oluşturulmalı veya mevcut gruplar arasında bilgi paylaşımı yapılmalıdır.

14. GST Yetenek geliştirici seminerler, konferanslar, etkinlikler veya çalışmalar yapılmalı ve yetenekler daha da geliştirilmelidir.

15. Ülkelerin resmi olarak GST geliştiren veya GST oluşturarak düşman sistemleri ele geçirmeye yönelik çalışmalar yaptığı bilinse de bunu resmi olarak yaptıklarını gösterir bir kanıta rastlanmadığı dikkate alınarak bu alanda da gerekli çalışmalar yapılmalıdır.

16. Karşı adli bilişim metotlarının çok iyi bilinerek yapılacak yetenek geliştirme işlemlerinde kullanılması veya yapılan saldırıların daha iyi anlaşılabilmesi konusunda yetenek geliştirilmelidir.

17. Soğuk savaş döneminden siber savaş dönemine giren dünya ülkeleri için GST saldırılar büyük bir öneme sahip olmakla birlikte önümüzdeki yıllarda bu saldırıların daha da su yüzüne çıkacağı aşikârdır. Bu hususların dikkate alındığı uluslararası işbirlikleri yapılmalıdır.

18. GST saldırılarının bilindiğinden daha fazla olduğu bu araştırmada elde edilen bulgulardan birisidir. Günümüzde yapılan ve gelecekte daha da şiddetlenecek olan saldırılara karşı ülkelerin ortak çözümler üretmesi gerekmektedir. Buna yönelik olarak AB ülkeleri arasında işbirliği veya bilgi paylaşımı yapılabilecek ortamlar oluşturulmalı veya kurulmalıdır.

19. Ülkemizde GST konusunda yapılan çalışmaların çok az olduğu, ülkemizde tespit edilen bir GST bulunmadığı/bulunamadığı, yapılan çalışmaların ise gerçek bir GST olduğunu gösterir net bulguları içermediği belirlenmiştir. Bu hususlara daha çok önem verilmeli, bu konuda yetenek geliştirmenin yanında milli ürünlerin geliştirilmesi de özendirilmelidir.

Kaynakça

[1] Cole E., "The Changing Threat" in *Advanced Persistent Threats Understanding the Danger How to Protect Your Organization*, Waltham, MA:Syngress-Elsevier, 2013,pp.20-26.

[2] Internet: "Advanced Persistent Threats: A Symantec Perspective", URL: www.webcitation.org/query?url=http%3A%2F%2Fwww.symantec.com%2Fcontent%2Fen%2Fus%2Fenterprise%2Fwhite_papers%2Fb-advanced_persistent_threats_WP_21215957.en-

us.pdf&date=2016-01-04 Son Erişim tarihi: 04 Ocak 2016.
[3] Brewer R., "Advanced Persistent Threats: Minimizing the Damage", Network Security, vol.2014 (4), pp.5-9, 2014.
[4] Bayrak M.E., "Gelişmiş Kalıcı Tehdit Saldırılarının Ağ Akış Analiziyle Tespit Edilmesi", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara,2015.
[5] Tankard C., "Advanced Persistent threats and how to monitor and deter them", Network Security, vol. 2011 pp.16-19, 2011.
[6] Mouton, F., Leenen, L., Venter, H.S., "Social engineering attack examples, templates and scenarios", Computers & Security, vol. 59, pp. 186-209,2016.
[7] Krombholz, K., Hobel, H., Huber, M., Weippl, E., "Advanced Social Engineering Attacks", Journal of Information Security and Applications, vol.22, pp.113-122, 2015.
[8] Auty M., "Anatomy of Advanced Persistent Threat", Network Security, vol. 2015(4), pp.13-16, 2015.
[9] İnternet: "Advanced Persistent Threats: A Decade in Review", URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.commandfive.com%2Fpapers%2FC5_APT_ADecadeInReview.pdf&date=2015-12-27 Son Erişim Tarihi:27 Aralık 2015.
[10] Denning E.D., "Framework and principles for active cyber", Computers & Security, vol. 40, pp.108-113, 2014.
[11] Sood A.K. and Enbody R.J., "Targeted Cyberattacks: A Superset of Advanced Persistent Threats", Security & Privacy, IEEE, vol.11, pp.54-61, 2013.
[12] Thompson, G., "APTs: a poorly understood challenge", Network Security, vol.2011, pp.9-11, 2011.
[13] Raiu C., "Cyber-threat evolution: the past year", Computer Fraud & Security, vol. 2012, pp.5-8, 2012.
[14] İnternet: Llongueras A., "Moonlight Maze The beginning of a new era", URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.academia.edu%2F6182336%2FMOONLIGHT_MAZE._The_beginning_of_a_new_era&date=2015-12-27 Son erişim tarihi:27 Aralık 2015
[15] Shakarian P., Shakarian J. and Ruef A., "Attacking Iranian Nuclear Facilities: Stuxnet" in *Introduction to cyber-warfare*, Waltham, MA: Syngress-Elsevier, 2013, pp.224-235.
[16] Shakarian P., Shakarian J. and Ruef A., "Why Cyber Espionage is a Key Component of Chinese Strategy" in *Introduction to cyber-warfare*, Waltham, MA: Syngress-Elsevier, 2013, pp.114-153.
[17] İnternet: "Anatomy of an Attack", URL: http://www.webcitation.org/query?url=http%3A%2F%2Fblogs.rsa.com%2Fanatomy-of-an-attack%2F&date=2015-12-30 , Son erişim tarihi:27 Aralık 2015.
[18] Virvilis N., Gritzalis D., Apostolopoulos T., "Trusted Computing vs. Advanced Persistent Threats : Can a Defender win this game",in *2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 2013 IEEE 10th International Conference on Autonomic & Trusted Computing*, Vietri sul Mare, Italy,2013,396-403.
[19] İnternet: "A Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware", URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.mtechpro.com%2F2013%2Fmconnect%2Ffebruary%2Fdyncontent%2FEurograbber_White_Paper.pdf&date=2015-12-30 Son erişim tarihi:30 Aralık 2015.
[20] İnternet: "The Most Famous Advanced Persistent Threats in History", URL:http://www.webcitation.org/query?url=http%3A%2F%2Fwww.itbusinessedge.com%2Fslideshows%2Fthe-most-famous-advanced-persistent-threats-in-history-23.html&date=2015-12-30 Son erişim tarihi:30 Aralık 2015.
[21] İnternet: "The TeamSpy Crew Attacks – Abusing TeamViewer for Cyberespionage", URL:http://www.webcitation.org/query?url=https%3A%2F%2Fsecurelist.com%2Fblog%2Fincidents%2F35520%2Fthe-teamspy-crew-attacks-abusing-teamviewer-for-cyberespionage-8%2F&date=2015-12-30 Son erişim tarihi:30 Aralık 2015.
[22] İnternet: "Equation Group: Questions and Answers", URL: http://www.webcitation.org/query?url=https%3A%2F%2Fsecurelist.com%2Ffiles%2F2015%2F02%2FEquation_group_questions_and_answers.pdf&date=2015-12-30 Son erişim tarihi: 30 Aralık 2015.
[23] İnternet: "The Duqu 2.0", URL: http://www.webcitation.org/query?url=https%3A%2F%2Fsecurelist.com%2Ffiles%2F2015%2F06%2FThe_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf&date=2015-12-30 Son erişim tarihi: 30 Aralık 2015.
[24] De Vries J.A., "Towards a roadmap for development of intelligent data analysis based cyber attack detection systems", MSc Thesis, Delft University of Technology, Technology Policy & Management, Delft Hollanda, 2012.
[25] Guodong Z., Ke X., Lei X and Bo W., "Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis", IEEE Access, vol. 3,pp. 1132 – 1142, 2015.