Zararlı Yazılımların Farklı İşletim Sistemlerine Etkileri

Elif Ekiz[1], Şerif Bahtiyar[2]

[1] İstanbul Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ayazağa, İstanbul

[2] Progress Ar-Ge Merkezi, Provus Bilişim Hizmetleri A.Ş., Şişli, İstanbul

ekize@itu.edu.tr, serif.bahtiyar@provus.com.tr

Özet: Günlük hayatımızda bilgi sistemlerinin kullanımının artması, casusluk amacı ile bilgi toplama yazılımları da hızla artmaktadır. Bilgi sahibinin izni olmadan ilgili bilgiyi toplayan yazılımlar zararlı yazılımlar kategorisine girmektedir. Zararlı yazılımlar, amaçlarını gerçekleştirmek için bilgi sistemlerinin değişik bölümlerini kullanabilmektedir ve veri toplamak için de farklı haberleşme kanallarını kullanabilirler. Ayrıca, çok farklı yöntemler kullanarak diğer bilgi sistemlerine yayılabilirler. Bir bilgi sisteminde, veriyi güvenli tutabilmek için en hassas ve kritik bölümlerden biri işletim sistemidir. Bu bildiride, zararlı yazılımların farklı türdeki işletim sistemleri üzerinde etkileri incelenmiştir. Yapılan inceleme, bir zararlı yazılımın farklı türdeki işletim sistemlerini daha çok etkileme eğiliminde olduğunu göstermektedir.

Anahtar Sözcükler: İşletim sistemi, zararlı yazılımlar

Effects of Malicious Software on Different Operating Systems

Abstract: The pervasive usage of information systems in our daily lives has set the stage for malware leverage multiple attacks to collect data for espionage. In doing so, the malware may take on various parts of an information system to collect data and may capture data by using different communication interfaces. The malware may also use many propagation methods to spread. One of the most critical and vulnerable parts of an information system to secure data is operating systems. In this paper, we have investigated effects of malware on different operating systems. We have found that malware tend to affect many kinds of operating systems.

Keywords: operating system, malware

1.Giriş

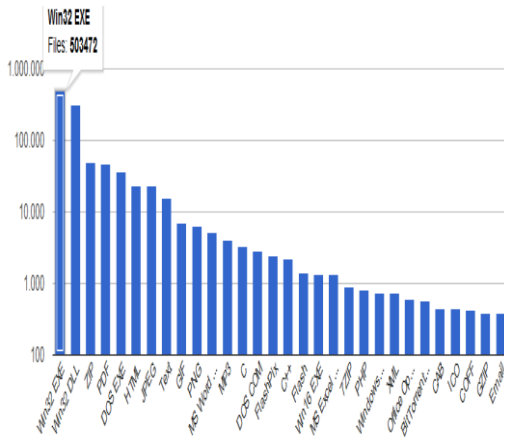
Bilişim sistemlerinin çok hızlı gelişmesiyle birlikte hayatımızda edindikleri yerler de hızla artmaktadır. Artık pek çok veri bilişim sistemleri üzerinde tutulmaktadır. Bu gün geçtikçe büyüyen bu veri seti bazı kötü amaçlı yazılımlar ile yetkisiz kişiler tarafından kullanılmak istenmektedir. Buna ek olarak sistemler başka sistemlere saldırılarında kullanılmak amacıyla da ele geçirilmek istenmektedir. Bu bildiri kapsamında, bu zararlı yazılımların farklı işletim sistemlerinde yayılma şekilleri incelenmiştir. Ayrıca, bu zararlı yazılımlardan korunma teknikleri araştırılmıştır.

Çalışmamızın ikinci bölümünde zararlı yazılımların yayılımlarını inceledik. Sonraki bölümde işletim sistemleri üzerinde durduk. Dördüncü bölümde araştırmamızın sonuçlarını verdik. Son bölümü önerilere ayırdık.

2. Zararlı Yazılımların Yayılımı

Zararlı yazılımlar, bilişim sistemlerine bulaşarak bu sistemlerin, kendi yaratılma amaçları doğrultusunda, çalışmasını amaçlarlar. Bu yazılımlar sisteme

bulaştıktan sonra sistem içerisinde kullanıcıya kendi varlığını fark ettirmeden yayılmaya başlarlar. Birçok bulaşma metodu vardır. Bunlar Şekil 1'de gösterildiği gibi aşağıda yer almaktadır. Bulaşma yollarını genel olarak web, dosya paylaşımı ve sosyal mühendislik ile olmaktadır.



Şekil 1. Zararlı yazılımların bulaşma yolları [1].

2.1. Web

Web sitelerin arka planında bulunan HTML, sabit diske yazma veya silme işlemleri yapılmasına izin vermez. Bunun yanı sıra, web sayfalarında çok kullanılan Java ve JavaScript ile yazılmış web uygulamaları da diske bir şey yazmaz ve silmez. Ancak, zararlı yazılımlar tarayıcı açıkları ile bulaşabilmektedir. Ziyaret edilen bir web sitesi drive-by-download ile size sormadan yanında başka eklentiler indirebilir. Bu şekilde zararlı yazılımlar bulaşmış olur. Ayrıca, gömülü HTML etiketleri veya JavaScript DOM nesneleri ile cookie dosyanızdan veri çalabilir veya size danışmadan başka işlemler yapacak şekilde tasarlanmış olabilir. Şekil 2'de örnek bir cross-site script gösterilmiştir.

```
"><SCRIPT>var+img=new+Image();img.
src="http://hacker/"%20+%20document.c
ookie;</
SCRIPT>

var img=new Image();

document.cookie;

img.src="http://hacker/" +
document.cookie;
```

Şekil 2. Cross-site script örneği [2].

2.3 Dosya Paylaşımı

Dosya paylaşımı, Internet'teki web siteleri üzerinden PDF veya Office dosyalarının paylaşımı, P2P veya USB ile program paylaşımı gerçekleştirilebilmektedir. P2P paylaşım ortamları virüs taraması bulundurmamaktadır ve bu tür paylaşımlar ile virüs yaymak oldukça kolaydır. O yüzden, zararlı yazılımlar genellikle Kazaa, Limewire, Ares ve Gnutella gibi programlar aracılığıyla yayılmaktadır. PDF tipinden dosyalar içerisinde çoklu ortam dosyaları, direk URL ve HTTP iletişimleri araçlarını bulundurması aracılığıyla virüs yayabilirler [3]. Ayrıca Office dosyaları ve PDF tipinden dosyalar script tabanlı oldukları için içerisine farklı kodlar eklenebilir. USB'ler ise autorun özellikleri sayesinde sisteme eklendikleri anda bir dosya çalıştırabilmeleriyle virüs yayabilme özelliğine sahiptirler.

2.3. Sosyal Mühendislik

Sosyal ağ siteleri kullanarak da zararlı yazılımları yaymak mümkündür. Kişiler, arkadaşları tarafından gönderildiğini sandıkları linkleri düşünmeden açabilirler. Arkadaşlarından geldiğini sandıkları dosyaları bilgisayarlarına indirebilirler. Sadece sosyal ağlarda değil e-posta ile de virüs bulaşmış dosya gönderilebilir. .exe, .pif, veya .scr uzantılı dosyalar potansiyel olarak virüslü dosyalardır [3].

3. İşletim Sistemleri

Zararlı yazılım yayılma metotları işletim sistemlerinin açıklarını kullanmaktadır.

Bazı metotlar farklı işletim sistemlerinde çalışmamaktadır. Bu bildiride, işletim sistemlerinden Windows, Linux ve Mac incelenecektir.

3.1. Windows

Windows işletim sistemi tüm dünyada en çok kullanılan işletim sistemidir. Zararlı yazılım üreten kişiler bu işletim sisteminin açıklarını kullanarak yayılabilen bir yazılım ürettiklerinde diğer pek çok bilgisayar sistemini etkileyebilecekleri için en çok saldırı bu işletim sistemine gerçekleştirilmektedir. Bu zararlı yazılımlar bilişim sistemine bulaştıklarında ilk olarak sisteminizin *"Windows Registry"* ayarlarını değiştirirler. Sisteminizde *"başlat -> çalıştır -> regedit"* dediğinizde açılacak olan pencerede aşağıdaki yolu izleyip buraya kendi programlarının adını yazarlar. Böylece sistem başlatılır başlatılmaz zararlı içerik bulunduran program çalışmaya başlar. İşte bu nedenle bu *"path"*i zararlı yazılım kod parçasına eklemektedirler [4].

HKEY_LOCAL_MACHINE\ Software\ Microsoft\Windows\ CurrentVersion\

- RunServices
- RunServicesOnce
- Run
- RunOnce

HKEY_CURRENT_USER\Software\ Microsoft\ Windows\ CurrentVersion\

- Run
- RunOnce
- RunServices

Windows işletim sistemi üzerindeki ilk makro virüs –*Concept*- 1995 yılında keşfedilmiştir. Bu virüs, Microsoft Word Office dokümanlarıyla bulaşmıştır.

Boza adlı virüs ilk olarak 1996 yılında keşfedilmiştir. Microsoft Windows'95 işletim sistemi dışında birkaç Windows sürümünde daha görülmüştür. Microsoft Excel dokümanıyla bulaşmıştır.

CIH virüsü -Çernobil olarak da bilinir- ilk olarak 1998'de keşfedilmiştir. Bu virüsün amacı veri kaybına neden olmaktır. Çalıştırılabilen dosyalar ile bulaşmıştır.

StrangeBrew virüsü ilk olarak 1998'de keşfedilmiştir. Java tabanlı bir program olduğu için Windows işletim sisteminin pek çok sürümünü etkilemiştir. Bu virüs herhangi bir zarar vermemiştir. Amacı çok sayıda sisteme bulaşabilmek olmuştur.

Melissa menace makro virüsü ilk olarak 1999 yılında keşfedilmiştir. Microsoft Word dokümanlarını veya e-posta eklentilerini kullanarak yayılmıştır.

BubbleBoy adıyla bilinen bir diğer virüs çeşidi 1999 yılında keşfedilmiştir. Bu virüs kendini e-postalara ekleyerek ve Internet Explorer'ın açıklarından faydalanarak yayılmıştır.

LoveBug virüsü – ILOVEYOU olarak da bilinir – ilk olarak 2000 yılında keşfedilmiştir. Yayılmak için Outlook kullanmıştır. Birkaç saat içerisinde tüm kıtalara ve on binlerce bilgisayar sistemine bulaşmıştır [5].

3.2. Linux

Linux işletim sistemi açık kaynak kodlu bir işletim sistemi olduğundan dolayı, daha güvenilirdir. Bu işletim sistemi pek çok program geliştiricisi tarafından incelendiği için çok az açık bulundurmaktadır. Bu açıkları zararlı yazılım üreticileri kolaylıkla bulamamaktadır. Bu nedenle bu işletim sistemini hedefleyen saldırı miktarı oldukça azdır.

İlk Linux virüsü, *Staog* isimli virüs, 1996 yılında keşfedilmiştir. Assembly dili kullanılarak yazılmış olan bu virüs *elf* dosyalarını kullanarak yayılmıştır.

StrangeBrew virüsü ilk olarak 1998 yılında keşfedilmiştir. Java kullanılarak

geliştirildiği için Linux işletim sisteminin tüm sürümlerini etkilemiştir. Herhangi bir zarar vermemiştir. Sadece yayılmıştır [6].

3.3. Macintosh

Mac işletim sistemi diğer işletim sistemlerine oranla dünya çapında daha az makinede bulunmaktadır. Çünkü bu işletim sistemi sadece Apple ürünlerinde kullanılmaktadır. Bu nedenle zararlı yazılım üreticileri daha çok miktarda sistemi etkileyebilecek özellikte olan Windows işletim sistemine saldırıda bulunmayı tercih ederler. Ancak Mac işletim sisteminin kullanım kolaylığını sağlamak amacıyla Windows üzerinde çalışan pek çok program bu işletim sistemi üzerinde de çalıştırabilmesi özelliği nedeniyle zararlı yazılım saldırılarına maruz kalmaktadır.

Salomon adlı makro virüs ilk olarak 1995 yılında keşfedilmiştir. Windows işletim sistemi üzerindeki Concept virüsünün aynısıdır. Microsoft Word Office dokümanlarını kullanarak yayılırlar.

Boza adlı virüs ilk olarak 1996 yılında keşfedilmiştir. Microsoft Excel dokümanıyla bulaşmıştır. Ancak Mac işletim sistemi Microsoft dokümanlarını okuyabildiği için o da bu virüs türünden etkilenmiştir.

Scores virüsü ilk olarak 1988 yılında keşfedilmiştir. Truva atı da denilmektedir. Mac işletim sistemleri için özel olarak üretilmiştir.

StrangeBrew virüsü ilk olarak 1998 yılında keşfedilmiştir. Java kullanılarak geliştirildiği için Mac işletim sistemini etkilemiştir. Herhangi bir zarar vermemiştir. Sadece yayılmıştır.

LoveBug virüsü – ILOVEYOU olarak da bilinir – ilk olarak 2000 yılında Windows işletim sisteminde keşfedilmiştir. Ancak Mac işletim sisteminin mimarisi nedeniyle Mac bilgisayarlara da bulaşmıştır.

Opener virüsü ilk olarak 2004 yılında keşfedilmiştir. Bu virüs işletim sisteminin kontrolünü ele geçirip finansal işlem şifreleri çalması amacıyla üretilmiştir [5].

4. Sonuç

Bir zararlı yazılımın birden çok işletim sisteminde yayılabildiği yukarıdaki virüs adlarından anlaşılmaktadır. Her işletim sistemi Java kodlarını çalıştırabildiği için Java ile yazılmış bir kod tüm işletim sistemlerini etkileyebilmektedir. *StrangeBrew* virüsü buna örnektir. Microsoft Office dokümanları hem script tabanlı olmaları nedeniyle hem de çok sayıda bilgisayar tarafından çalıştırılabilmeleri nedeniyle en çok Windows işletim sistemi saldırıya uğramaktadır. İkinci sırada Macintosh gelmektedir. En az saldırıya uğrayan ise Linux işletim sistemidir.

Bazı iddialara göre, Linux açık kaynak kodlu bir işletim sistemi olduğu için onun açıklarının saldırganlar tarafından daha kolay bulunabileceği düşünülmektedir. Ancak statiksel sonuçlar gösteriyor ki açık kaynak kodlu olması işletim sisteminin açıklarını birçok geliştiricinin katkısı ile en aza indirilebilir.

Ayrıca, Linux işletim sisteminin açıklarını hedef alan virüs yazılmış olsa bile virüs etkin hale getirildiğinde bulaşmaya başlayacaktır ve sadece kullanıcının erişim hakkı olan alanlara bulaşabilecektir. Linux kullanıcısı, program yüklemiyorsa veya yazılım ayarları ile ilgilenmiyorsa yönetici hesabıyla oturum açmayacağı için virüsün işletim sistemini ele geçirme ihtimali yoktur. Ancak Windows böyle bir işlemin gerçekleşmesine müsaade etmez. Bu nedenle Linux işletim sistemi hedef alınarak üretilmiş virüsler daha düşük yoğunluklu tehdit oluştururlar [7].

5.Öneriler

İşletim sistemleri birbirleri ile uyumlu olmamalıdır. Birinin çalıştırabildiği bir uygulamayı, bir başka işletim sistemi kendi uygulamasıyla açabilmelidir. Örneğin, Windows Microsoft Office ile Linux Libre Office uyumlu olmalıdır.

İşletim sistemleri arasında en güvenilir olanı açık kaynak kodlu olanıdır. Ancak yine de bu kötü amaçlı yazılımlardan korunmak için yeterli gerekli tedbirler alınmalıdır. Bu tarz yazılımların yayılmasında en büyük etken kişilerin bilgisizliğidir.

Korunmak için:

- Bir anti-virüs programımız olmalıdır.
- Güvenilir olmayan kaynaklarla dosya alışverişi yapmamalıyız.
- Internet'ten bir şey indirdiğimizde onu açmadan önce virüs taramasından geçirmeliyiz.
- Saldırı gelebilecek durumlar hakkında haberdar olmalıyız. Ona göre önlem almalıyız.
- Anti-virüs programımızın veya işletim sistemimizin güncelleştirmelerini ertelememeliyiz.
- Internet'te dolaşırken bizi yönlendireceği sayfaları, butona tıkladığımızda ne olacağını dikkatli okumalıyız [8].

Teşekkür

Bu çalışma EUREKA ITEA2 projesi ADAX (proje no. 10030) ve TEYDEB projesi AKFİS (proje no. 1130018) tarafından desteklenmiştir.

6. Kaynaklar

[1]. (Eylül, 2012). http://www.totalvirus.com/statistics /

[2]. Grossman, J., "Cross-Site Scripting Worms & Viruses", (Haziran, 2009) https://www.whitehatsec.com/assets/WP5CSS0607.pdf

[3]. Zhuang, W., Ye, Y., Chen, Y., Li, T., "Ensemble Clustering for Internet Security Applications", **IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,** 42:1784 – 1796, (2012).

[4]. Ulucenk, C., Varadharajan, V., Balakrishnan, V., Tupakula, U., "Techniques for Analysing PDF Malware", **18th Asia Pacific Software Engineering Conference (APSEC)**, 41 – 48, (2011).

[5]. Salomon, D., "Foundations of Computer Security", **Springer-Verlag**, 35:27-28, (2006).

[6]. Sarnsuwan, N., Charnsripinyo, C., Wattanapongsakorn, N., "A New Approach for Internet Worm Detection and Classification", **6th International Conference on Networked Computing (INC)**, 1 – 4, (2010).

[7]. Zhang, D., Wang, Y., "SIRS: Internet Worm Propagation Model and Application", **International Conference on Electrical and Control Engineering (ICECE)**, 3029 – 3032, (2010).

[8]. Faghani, M.R., Nguyen, U. T. "A Study of XSS Worm Propagation and Detection Mechanisms in Online Social Networks", **IEEE Transactions on Information Forensics and Security,** 8:1815 – 1826, (2013).