Linux Virüsleri ile Tanışın

Barış Can

Nisan, 2016

İçindekiler

1 Giriş

Linux'un tabiri caizse "virüssüz" bir işletim sistemi olduğu yıllardır dillere pelesenk olmuş bir yargıdır. Birçok Linux kullanıcısı bu yazıyı okurken bir sürpriz yaşayabilir; çünkü Linux işletim sistemlerinde de virüsler mevcuttur. Gerçi, birçok muadili işletim sistemine nazaran Linux dağıtımlarında daha az virüs türevine rastlarsınız. Bunu, bazıları Linux işletim sistemi dağıtımlarının popülaritesine bağlar, bazıları ise güvenli olmasına. Biz konumuza dönelim. Bu yazımızda sizleri Linux tarihinde bugüne kadar tespit edilen bazı popüler Linux virüsleriyle tanıştıracağız.
Sizler için bugüne kadar tanınmış bir Linux Virüs Listesi derledik. Şimdi onların yarattığı risk seviyesini ve etkilerini inceleyelim.

2 ALAEDA (Virus.Linux.Alaeda)

Çıkış Tarihi: 2003
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Linux

Alaeda virüsü; çalışan bir sistemde, geçerli dizindeki ELF biçimli dosyalara hasar veren, yerleşik olmayan bir virüs çeşididir (ELF; yaygın kullanılan Linux dosya türevlerinden biridir. 32 bit, yanısıra 64 bit işletim sistemini de desteklemektedir.). Enjekte edilen dosyanın metin bölümüne eklenecek zararlı kod, asgari büyüklükte oluşur ve dosyaya hasar vermeye başlar. Alaeda virüsünden kurtulmak için virüs enjekte olmuş ELF dosya türevinin orijinal hâlini yüklemeniz yeterli olacaktır.

3 BADBUNNY (Perl.Badbunny)

Çıkış Tarihi: 2007
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platforum: Linux, Windows

Badbunny, açık kaynak kodlu Open Office aracını özellikle hedefleyen ilk solucan türevi olarak bilinmektedir. Bulaştığı sistemde, bir ormanda bulunan kadın ile tavşan kılığında bir adamın pornografik resmi görüntülenmektedir. Symantec Güvenlik Danışmanlarının açıklamasına göre yeni solucan, kaynağı bilinmeyen Open Office dokümanları ile yayılmaya başladı. Solucan aynı zamanda Windows, Linux, Mac OS X sistemlerine de etki edebiliyor. Bu yüzden bilinmeyen kaynaklardan Open Office belgesi alırken dikkatli olunmalıdır.

4 OSFX.8759

Çıkış Tarihi: 2002
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Unix

Linux.OSF.8759 virüsü Linux sistemleri üzerinde “backdoor” (arka kapı) görevi görebilen ve ELF yapılarını bozan bir virüstür. Çalıştırıldıktan itibaren mevcut tüm dosyalara bulaşır. Linux sistemlerinin kullanıcı ayrıcalıkları sayesinde pratikte yıkıcı olan virüs kolayca sistemimizden sınır dışı edilebilir. Her durumda en fazla 201 dosyaya bulaşabilen virüs, yıkıcı olmayan bir ELF virüsü olarak tarihe geçmiştir.

5 VIT VIRUS (Virus.Linux.Vit.4096)

Çıkış Tarihi: 1999
Risk Seviyesi: Linux kullanıcıları için düşük
Hasar Seviyesi: Düşük
Platform: Linux, Unix, Windows ve MSDOS

Vit virüsü, yerleşik belleği olmayan parazitik çapraz platform virüslerden biridir. Dahili ELF biçimine sahip olan virüs, Linux işletim sistemi altında çoğalır ve Linux'un çalıştırılabilir dosyalarına hasar verir. Aynı zamanda bu virüs "Linux.Bliss" adı verilen virüsten sonra Linux işletim sistemi için bilinen ikinci virüs olma özelliğini de taşımaktadır. Virüs, Linux'un sıkı güvenlik denetimleri sebebi ile sadece "yazılabilir" dosyalara ve dizinlere bulaşması ile bilinir. Geçerli kullanıcı adı ve parola ile erişim sağlarsa virüs tüm dizin ve dosyalara da etki edebilir. Ortalama bir Linux kullanıcısı için virüs -Root hakları olmaksızın- minimum risk seviyesine sahiptir.

6 STAOG

Çıkış Tarihi: 1996
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Linux

Staog, Linux sistemler üzerinde çalışanlar için özel olarak geliştirilen ilk virüs türevidir. Virüs o yıllarda Linux çekirdeğindeki, hafızada kalıcı izin açığı istismar edilerek işletilmiştir. Bellekte yerleşik durumda iken çalıştırılabilir ikili dosyaları etkileyen virüsün işlevselliği, açık duyurulduktan hemen sonra yazılım güncellemesi ile giderilmiş ve açık kapatılmıştır. Virüs o yıllarda Avusturalya'nın bilinen hacker grubu VLAD tarafından yazılmıştır.

7 BLISS

Çıkış Tarihi: 1997, Şubat
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Linux

Bliss, Linux sistemlere bulaşması ile bilinen ilk bilgisayar virüsü olma özelliğini taşımaktadır. Virüsün, Linux sistemlere virüs girmez, diyenlere karşın gireceğini kanıtlamak için yazıldığı düşünülmektedir. Bliss virüsü yazıldığı zamanda bir popülarite elde etmemiştir; çünkü sisteme herhangi bir zarar vermemektedir. Sadece Linux'a virüs girebileceğinin bir kanıtı olarak gösterilmiştir. Virüsün sınıflandırılmasının tartışmalı olması ile birlikte, genellikle solucan veya trojan olarak kabul edilmiştir.

8 Virus.Linux.Winter.341

Çıkış Tarihi: 2000
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Linux

Bu virüs, yerleşik belleği olmayan parazitik olarak bilinen zararsız bir Linux virüsüdür. Yaklaşık 341 bayt olan virüsün boyutu dahi bir virüs olabilmek için çok çok düşüktür.

9 Zipworm

Çıkış Tarihi: 2001
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Linux

Zip arşivlerini etkileyen zararsız virüs türevi olan Zipworm etkinleştirildiğinde geçerli dizinde bulunan tüm zip dosyalarını kopyalamakta ve dosyaların ismini aşağıdaki beş olası isimden biriyle değiştirmektedir:

- Linux'un berbat olmasındaki on neden!
- Neden Windows Linux'tan daha mükemmeldir?!
- Linux, senin için? ASLA!
- Linux virüse karşı korumalı mı? HAYIR!
- zipworm!

Virüs ayrıca, "elf zip worm vecna" şeklinde bir telif hakkı metni de içermektedir.

10 SATYR (Virus.Linux.Satyr.a)

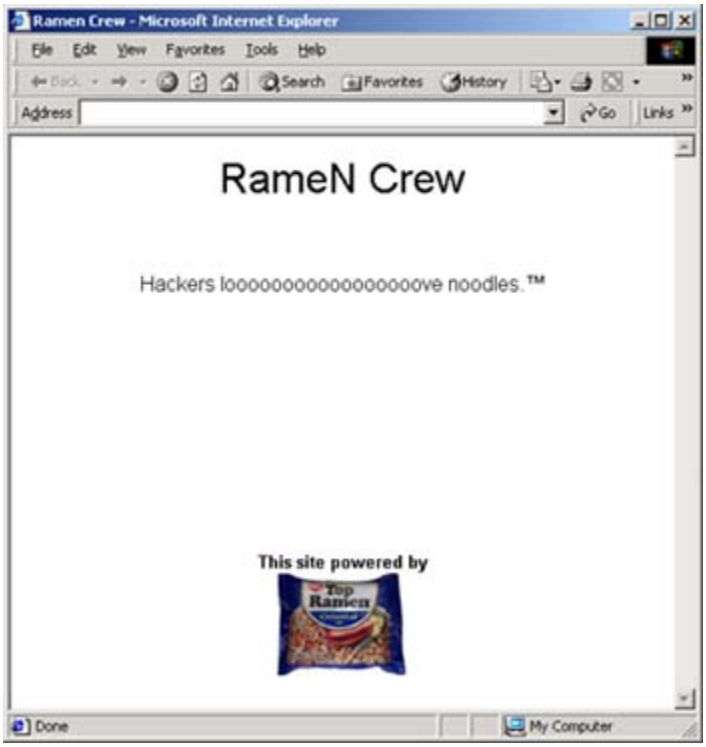
Çıkış Tarihi: 2001
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Linux

Satyr, yerleşik belleği olmayan parazitik olarak bilinen zararsız Linux virüsüdür. İşlevi sistemdeki ELF dosyalarını hedefleyerek bozmaktır.

11 RAMEN VIRUS (Ramen Worm)

Çıkış Tarihi: 2001
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Linux (Redhat)

Ramen, Red Hat Linux 6.2 ve 7.0 varsayılan kurulumları çalıştıran sistemleri etkiler. Bilgisayar ağı aracılığı ile yayılır ve karmaşık bir solucan/virüs olduğu bilinir. Üç açığı istismar ederek yayılan virüs (bkz; wu-ftpd, rpc.statd and lpd services), sisteme "brute force" tekniği ile sızmaya çalışır. Sızdıktan sonra web sunucusu dahilinde tüm sistemin "index.html" dosyalarını aşağıdaki metin ile değiştirir.



Şekil 1:

12 KOOBFACE

Çıkış Tarihi: 2010
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Linux, Windows, Mac

Koobface virüsü 2010 yılında türemiş yeni nesil virüslerden biridir. Sosyal ağ siteleri ve belli platformlar aracılığı ile yayılan virüsün hedefi, bilgisayarınıza sızdıktan sonra sosyal ağ bilgilerinizi ele geçirip tüm arkadaşlarınıza –ya da takipçilerinize- virüslü mesajlar göndermektir.

13 KAITEN

Çıkış Tarihi: 2006
Risk Seviyesi: Düşük
Hasar Seviyesi: Düşük
Platform: Linux

Kaiten, Linux sistemlerde “backdoor” (arka kapı) açılmasını sağlayan bir Truva atı virüs türevidir.

14 RIKE

Çıkış tarihi: 2003
Risk seviyesi: Düşük
Hasar seviyesi: Düşük
Platform: Linux

Rike, Assembler programlama dilinde yazılmış, 1627 baytlık neredeyse zararsız parazit virüsüdür. Dosyalar ile çalışırken düşük seviyeli Linux işlevleri kullanır. Herhangi bir dosyaya nüfuz ederken, SHT_PROGBITS ile bölümleri tarar. Son bölümün boyutunu artırdıktan sonra kendini boş alana yazar.

Linux gibi açık kaynak kodlu işletim sistemlerinde ELF dosyası formatı, virüs riskini artırabilir.
Sonuç olarak, Linux için virüsler, var olmayan varlıklar değildir. Her işletim sisteminde olduğu gibi Linux işletim sistemi dağıtımlarında da virüsler ile karşılaşabilirsiniz. Fakat, bu virüslerin oluşturduğu risklerin çoğu düşüktür ve ihmal edilebilir. Kısa sürede açık zaten gerekli güncellemelerle giderilir. Tabii, virüsler sadece Linux içindeki zaafiyetler ile değil, sizin kişisel güvenliğinizi ihmal ettiğiniz vakit, sisteminize kişisel güvenliğiniz üzerinden sızarak da girebilir.

Kısacası, Linux'un virüs geçirmez olmasının nedeni, virüslerin oluşturdukları riskin çok düşük seviyede olmasıdır. Pek tabii Linux'un popülaritesi arttıkça, bilgisayar korsanları da bu sistemde açık aramaya ağırlık vermektedir. Bu yüzden her ihtimale karşı bir anti-virüs ya da güvenlik duvarının yüklü olması şarttır.