Kendini-Kopyalayan Aktif Kötücül Yazılımların Ağlarda Yayılım Dinamikleri

Gürkan Gür
1 Provus - A MasterCard Company, Ayazaga, 34396, Istanbul, TR
2 SATLAB, Bilgisayar Müh. Bölümü, Boğaziçi Üniversitesi, Bebek, 34342, Istanbul, TR
gurkan_gur@mastercard.com

Özet: Bu çalışmada, kendini-kopyalayan aktif kötücül yazılımların ağlarda yayılım dinamiklerinin önemli yanları incelenecektir. Öncelikle bu güvenlik problemi tanımlanacak ve modelleme ile ilgili geliştirilmiş yaklaşımlar anlatılacaktır. Sonrasında kötücül yazılımların yayılımını modellemek için farklı yaklaşımlar ve bu modellerin hassasiyeti ve yetenekleri üzerindeki etkenler tartışılacaktır. Son olarak, bu alanda ortaya çıkan araştırma konuları ve açık problemler ile çalışmamız sonlandırılacaktır.

Anahtar Sözcükler: Kötücül yazılımlar, yayılım modelleri, bilgi güvenliği, ağ güvenliği.

Spread Dynamics of Self-Replicating Active Malware in Networks

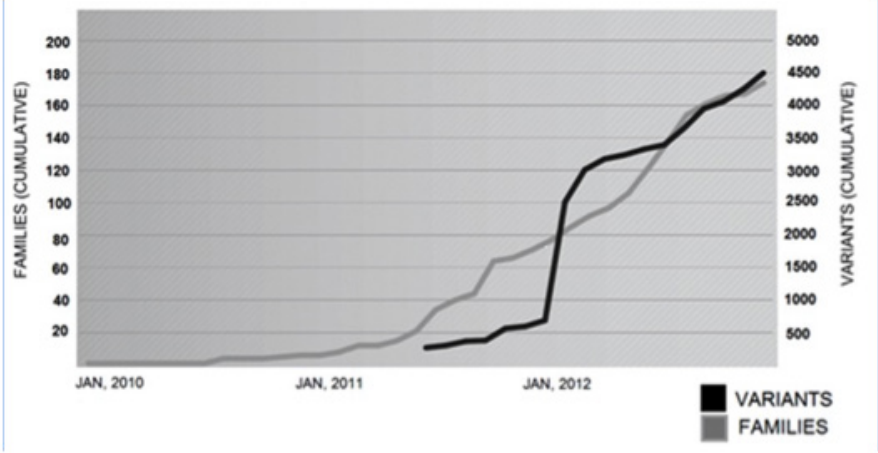
Abstract: In this work, we discuss important aspects of the spread dynamics of self-replicating active malware in networks. First, we will describe the problem and introduce approaches considering how to model it. Then we will present available control strategies and analyze relevant factors on the accuracy and capabilities of these models. Finally, we will conclude with research directions and open problems for this topic.

Keywords: Malware, propagation models, information security, network security.

1. Giriş

İnternetin ortaya çıkması ile birlikte mümkün hale gelen sayısız uygulamalarla artık bilgisayar ağları çok yaygın ve yaşamsal hale gelmiştir. Böylece bu ağları kullanan hizmetler ve sistemlere bağımlı olarak işleyen ulusal ve küresel ekonomilerin sürdürülebilirliği açısından güvenlik ve güvenilirlik kritik kavramlar olarak ortaya çıkmıştır. İnternetin yaygın kullanımı siber tehditlerde ve vakalarda hızlı bir artış meydana getirmiştir. Ortaya çıkan sorunlardan biri de kendini-kopyalan aktif kötücül yazılımların ağ sistemleri yoluyla yayılmasıdır. Kendini-kopyalan aktif kötücül yazılım zarar görebilecek makinaları tespit etmek için bir ağı özerk bir şekilde tarayan, kendini-kopyalayan bir kod parçasıdır ve kendi gücü ile yayılabilmek için açıklardan faydalanır. Kötücül aktiviteler için sömürülebilecek açıkları hedefler. Kendini kopyalama ve ağ iletişimini kullanarak otomatik bir şekilde yayıldıklarından bir alt ağı veya İnterneti çok hızlı bir şekilde basabilirler. Bu yazılımlar özellikle bulaştıkları ağlara izinsiz girişleri mümkün kılmak için kullanılırlar. Bu girişler aynı zamanda daha çok bulaşmayı ve böylece pozitif geribildirim döngüsü içinde daha çok izinsiz girişi sağlarlar.

Aktif kötücül yazılım saldırıları küresel iletişim ağına çok büyük zararlar verebilirler. Şekil 2'de Android mobil işletim sistemi için kötücül yazılımın son yıllarda çok yüksek



Şekil 1. Kümülatif olarak mobil Android kötücül yazılım aileleri (families) ve çeşitleri (variants), 2010 - 2012 (Kaynak: Symantec IST Report 2013)

hızla arttığı görülmektedir. Örneğin, 2001'de gerçekleşen ani bir Code Red salgınında yüz binlerce bilgisayar çok hızlı bir şekilde enfekte olarak milyarlarca ABD doları değerinde zarara neden olmuştur [2]. Bu nedenlerle bu tarz tehditlerin modellenmesi çok önemlidir. Bu gereksinimin arkasındaki temel neden, geçerli bir model elde ederek bu yayılıma karşı kontrol stratejilerini geliştirebilmektir [3]. Aynı zamanda aktif kötücül yazılımların yayılımının öngörülmesi ve anlaşılması konusunda yeteneklerin geliştirilmesi açısından da önemlidirler.

Literatürde, kötücül yazılımların yayılımını modellemek için farklı yaklaşımlar önerilmiştir. Bu yaklaşımlar 4 ana gruba ayrılabilir:

•Biyolojik-esinli (Biologically-inspired): Bu grupta en önde gelen model epidemiyolojik modeldir [4]. Bu yaklaşım bir popülasyonda bir salgın hastalığın yayılımından esinlenmiştir. Bu modelde doğrusal olmayan bir diferansiyel denklem kullanılarak kötücül yazılım popülasyonunun dinamikleri

$$\frac{dn}{dt} = \beta \cdot n \cdot (1 - n) - \alpha \cdot n$$

şeklinde modellenir. Bu denklemde n(t) enfekte olmuş düğümlerin oranını, β bağışıklığı olmayan makinelerin enfekte olma hızını gösteren doğum oranını ve α ölüm oranını göstermektedir [5].
•Matematiksel: Bu grupta sistem parametrelerini matematiksel analiz kullanarak aşağıdan yukarı doğru bir model oluşturmak için kullanan yaklaşımlar bulunmaktadır [6,7].

•Çizge tabanlı (graph-based): Bu metotlar ağın çizge tabanlı modellemesini kullanırlar ve modellerini bu çizgesel gösterim üzerinden geliştirirler. Sistem dinamikleri topoloji üzerine uygulanır ve sonuç olarak yayılım karakteristikleri ile ilgili çıkarımda bulunulur [8].

•Ampirik: Bu yaklaşımlar geçmiş veya şimdiki kötücül yazılımların mevcut olan yayılım dinamiklerine ait verileri kullanarak model oluştururlar. Örneğin, Rassal Sabit Yayılım modeli (Random Constant Spread (RCS) model) CodeRed solucanının ortaya çıkıp yayılmasının deneye dayalı verisi kullanılarak geliştirilmiştir [9].

2. Model parametreleri

Temel olarak kötücül yazılım yayılımının aşağıdaki parametreleri incelenerek model geliştirilmesi sağlanacaktır:

• **Ağ topolojisi:** Ağ topolojisi yayılım dinamiklerinin ağ düğümü tabanlı yön ve hızı açısından önemlidir.
• **Yayılım stratejisi:** Kötücül yazılımların gizlilik ve yayılım hızı gibi önemsedikleri kıstaslara göre değişik yayılım stratejileri olabilir.
• **Bulaşma sonrası durum:** Bulaşma sonrası sistemlerin işlevlerindeki değişimler ve enfeksiyon algılama olasılığı yayılım modellerinin içerdiği etkenlerdendir.
• **Açıkların sistemde dağılım karakteristikleri:** Bu özellikler yayılımın dinamiklerini belirleyen çok temel etkenlerdir. Güvenlik açısından gelişkin altyapısı olan ağlarda açıkların dağılımı güvenlik açısından tasarlanmamış ağlara göre çok farklıdır.

• **Yama stratejisi:** Yayılımın dinamiklerini uygulanan karşı-önlemler çok önemli derecede etkiler. Gelişmiş ve aktif bir yama stratejisi herhangi bir kötücül yazılımın yayılımını doğrudan ve olumlu şekilde (engelleyici tarzda) etkiler.

Bu parametre seti, bağlam tabanlı olarak değişik önceliğe sahip elemanlardan oluşmaktadır. Örneğin bağlantı derecesinin yüksek olduğu ağlarda ağ topolojisi yayılımın ilerleyişi açısından öncelik kazanmaktadır.

2. Sonuç ve tartışma

Bu çalışmada aktif kötücül yazılımların yayılım dinamiklerine dair temel meseleleri ele aldık ve literatürdeki metodolojileri gözden geçirdik. Farklı metodolojilerin çeşitli artıları ve eksileri olduğundan ağırlıklı olarak hangi modelin hangi bağlamda daha iyi işlediği üzerinde durduk. Ayrıca bu konudaki önemli gelişmelerden de bahsederek yapılabilecek araştırma çalışmalarını tartıştık.

Teşekkür

Bu çalışma ITEA3 ADAX Projesi kapsamında desteklenmektedir.

5. Kaynaklar

[1] W.H. Debany, "Modeling the spread of Internet worms via persistently unpatched hosts," IEEE Network, vol.22, no.2, pp.26 - 32, March-April (2008).

[2] S.H. Sellke, N.B. Shroff, and S. Bagchi, "Modeling and automated containment of worms", IEEE Transactions on Dependable and Secure Computing, vol. 5, no. 2, pp. 71 - 86 (2008).

[3] Liping Feng, Xiaofeng Liao, Qi Han, and Huaqing Li, “Dynamical analysis and control strategies on malware propagation model,” Applied Mathematical Modelling, vol. 37, no. 16–17, pp. 8225-8236 (2013).
[4] J. O. Kephart and S. R. White, “Measuring and modeling computer virus prevalence,” IEEE Symposium on Security and Privacy (1993).
[5] S.H. Sellke, N.B. Shroff, and S. Bagchi, "Modeling and automated containment of worms", IEEE Transactions on Dependable and Secure Computing, vol. 5, no. 2, pp. 71 - 86 (2008).
[6] Zesheng Chen, Lixin Gao, and K. Kwiaty, "Modeling the spread of active worms," Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM 2003), vol.3, pp.1890-1900 (2003).

[7] Yini Wang, Sheng Wen, and Yang Xiang, "Modeling worms propagation on probability," 2011 5th International Conference on Network and System Security (NSS), pp.49-56, 6-8 (2011).
[8] E. Jonckheere, "Worm propagation and defense over hyperbolic graphs," 43rd IEEE Conference on Decision and Control (CDC), vol.1, pp.87-92, 14-17 (2004).
[9] S. Staniford, V. Paxson, N. Weaver, “How to own the Internet in your spare time,” Proceedings of the 11th USENIX Security Symposium (Security ’02) (2002).