Börteçin Ege

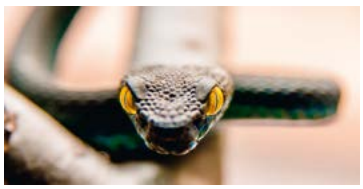
# Epic Turla
## Devletlerin Yeni Kâbusu

Bilişim dünyasındaki gelişmeler artık sadece bireysel kullanıcılar açısından değil aynı zamanda devletler açısından da baş döndürücü bir hızla devam ediyor. Dünyaca bilinen Rus siber güvenlik şirketi Kaspersky Lab tarafından yaklaşık 10 ay önce ilk defa tespit edilip takibe alınan Epic Turla adlı bir bilgisayar virüsü, bugünlerde tüm devletlerin tam anlamıyla kâbusu olmuş durumda. Bu yılın Ağustos ayında ABD'nin Las Vegas kentinde 17. defa düzenlenen Black Hat adlı siber güvenlik konferansında Kaspersky Lab tarafından açıklandığına göre, bilgisayar tarihinde ilk defa kritik görevler için devletler tarafından kullanılan bilgisayarların büyük bir bölümü artık devletlerin kontrolünden çıkmış gibi görünüyor. Hatta artık istihbarat teşkilatlarının kendileri de siber casusluk kurbanı olmaya başlamış, hem de ruhları bile duymadan. Anlaşıldığı kadarıyla Stuxnet ve Flame ile başlayan siber savaşlar, arka planda ancak sert ve etkin bir şekilde hâlâ devam ediyor. Yine Kaspersky Lab tarafından bildirildiğine göre söz konusu casus yazılım şu anda toplam 45 ülkede yüzlerce, hatta belki de binlerce bilgisayarı kontrolü altına almış bulunuyor. Hedefleri konusunda hayli seçici olduğu gözlemlenen ve etkin olduğu ülkelerde gözünün özellikle devlet daireleri, büyükelçilikler, askeri kurumlar ve ilaç üreticilerinin üzerinde olduğu anlaşılan Epic Turla adlı bu virüs, devletler için tam bir baş belası haline gelmiş durumda.

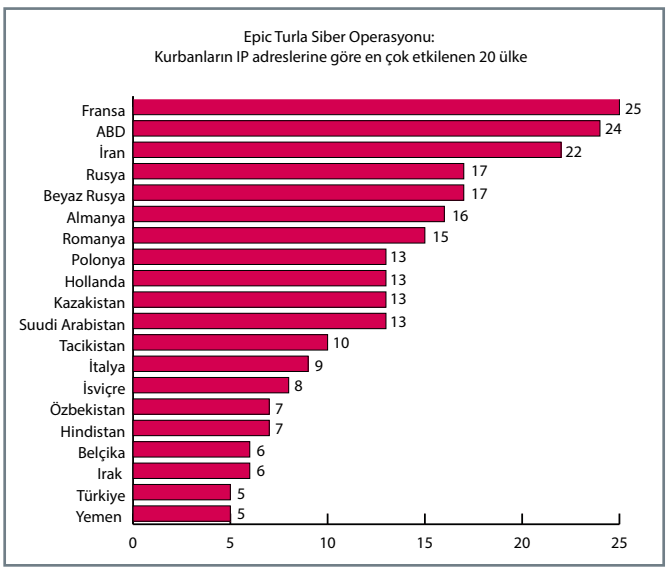
Virüsün yapısından elde edilen bilgilere göre, Epic Turla en başta Windows XP ve Adobe Reader'da bulunan ve bugüne kadar keşfedilmemiş iki güvenlik açığı olmak üzere birbirinden çok farklı güvenlik açıklarını ve "*watering holes*" (sulama kanalı) gibi siber saldırı tekniklerini kullanarak hareket ediyor. İlk defa 2012'de ABD'li siber güvenlik şirketi RSA tarafından tespit edilen ve "*watering holes*" adı verilen bu siber saldırı tekniğine göre, saldırganlar ilk aşamada kurbanlarının önceden ziyaret edeceğini bildikleri veya tahmin ettikleri web sitelerine zararlı yazılımlarını yerleştirerek bu sitelerin hedefteki kullanıcılar tarafından ziyaret edilmesi durumunda kullanıcının bilgisayarına sızıyor. Epic Turla "*watering holes*" saldırılarını Java, Microsoft Internet Explorer ve Adobe Flash Player'da bulduğu bazı güvenlik açıklarını kullanarak hatta bazen söz konusu kullanıcıları sahte Flash Player yükleme sitelerine yönlendirerek gerçekleştiriyor.

İşte her şey tam bu noktada, Epic Turla'nın hedefteki kullanıcıların bilgisayarına sızmasıyla başlıyor. Epic bir yandan bulaşmış olduğu bilgisayar üzerinden büyük bir hızla o sistemdeki diğer bilgisayarlara yayılırken, diğer yandan da söz konusu bilgisayarlarda birer "arka kapı" açmaya başlıyor. Bunun ardından kendi kontrol ve komuta merkeziyle iletişime geçerek söz konusu merkezdeki sunucuya sızdığı bilgisayarların sistem bilgilerini göndermeye başlıyor. Merkezden, gönderdiği sistem bilgilerinin karşılığında nelerin yapılması gerektiğine dair ilk komutların yanı sıra bir dizi program (kullanıcının klavye hareketlerini kaydetmek için keylogger programı, RAR dosya sıkıştırma ve arşivleme programı ve Microsoft DNS sorgulayıcı) alan virüs, bu programları bulunduğu bilgisayara yükleyerek operasyonun ilk ve en önemli aşamasını tamamlıyor (son yıllarda bilgisayar virüslerinin büyük bir bölümü internet üzerinden komut alabilmek için DNS üzerinden sorgulama yöntemini tercih etmeye başladı). Böylece çember tamamlanıyor ve her casusluk yazılımından olduğu gibi Epic'ten de, kendinden istenen veri ve bilgileri bağlı olduğu merkeze göndermesi ve görevini mümkün olduğunca göze çarpmadan yerine getirmesi bekleniyor.

Yine Kaspersky'nin tahminine göre Epic Turla'nın bir sisteme yerleşmesinden sonra olası bir aşama daha var. Bu aşamada, kurbanın gerçekten ilgi çekici bulunması durumunda bilgisayarına Carbon olarak da adlandırılan yeni bir konfigürasyon dosyası yüklenerek Turla Carbon sistemine yani daha üst bir aşamaya geçiliyor. Kurbanın bilgisayarında bu üst aşamaya geçilmesi durumunda ise Cobra/Carbon adı verilen çok daha gelişmiş bir arka kapı sistemi açılıyor.



Kendini çok iyi kamufle edebildiği belli olan Epic Turla'nın 2012'den veya daha eskiden beri etkin olduğu tahmin ediliyor. Kaspersky tarafından bildirildiğine göre, virüs 5 Ağustos'ta müşterilerinden birinin sistemine sızmaya çalışırken tespit edildi. Şu sıralar özelikle Ortadoğu ve Avrupa'da toplam 45 ülkede etkili olan virüsten en çok etkilenen ülkelerin başında Fransa, ABD, İran, Rusya, Almanya, Hollanda ve Türkiye geliyor. Tıpkı Stuxnet ve Flame gibi kimler tarafından geliştirildiği tam olarak bilinmeyen virüsün arkasında bir devlet olduğu tahmin ediliyor.




**Kaynak**
Kaspersky Lab, "Epic Turla – catching the reptile's tail",
http://business.kaspersky.com/epic-turla-catching-the-reptiles-tail/, 07.08.2014