

Güvenlik Raporlarına Genel Bakış

Zararlı kodların gün geçtikçe daha komplike hale gelmeleri ve bununla birlikte, yayılma hızlarındaki artış, karşı karşıya kaldığımız tehdidin boyutunu gösterir mahiyette. Ayrıca bu zararlı kodların hatırı sayılır bir yüzdesinin asıl amacının gizli bilgileri ele geçirmek ve bulaştıkları bilgisayarları saldırganların kontrolüne sunmak olduğunu göz önünde bulundurursak ne kadar ciddi bir tehlikeyle karşı karşıya kaldığımızı görebiliriz.

Karşı karşıya olduğumuz tehditler hakkında biraz daha elle tutulur bilgiler vermek adına iki farklı rapordan kısa başlıklar sunmak istiyorum. Bunlardan birisi Symantec tarafından onikincisi yayınlanan “**Symantec Internet Security Threat Report Volume XII (Trends for January–June 07)**” raporu ve ikinci olarak da Microsoft tarafından yayınlanan “**Microsoft Security Intelligence Report (January through June 2007)**” raporu. Her iki rapor’da da birbirinden değerli bilgiler mevcut. Symantec’in raporuna ve rapor ile ilgili podcast’lere <http://www.symantec.com/business/theme.jsp?themeid=threatreport> adresinden ulaşabilirsiniz. Microsoft’un raporunu ise http://download.microsoft.com/download/a/a/1/aa1ac20e-514e-4ec1-a12e-022c35aa54cf/MS_Security_Report_Jan-Jun07.pdf adresinden indirebilirsiniz.

Symantec’in raporunda gözümüze ilk çarpan noktalardan birisi bot network’ler ve Türkiye’nin EMEA bölgesindeki bot bulaşmış bilgisayar barındıran ülkeler sıralamasındaki yeri. Aşağıdaki Şekil-01’de gösterilen grafikten de görülebileceği gibi Türkiye EMEA bölgesinde 9. Sırada.

Regional Rank	Previous Regional Rank	Country	Percentage of Regional Bots	Previous Percentage of Regional Bots	Percentage of Worldwide Bots	Average Lifespan (days)	Command-and-Control
1	2	Germany	23%	16%	9%	1	25%
2	3	Spain	15%	14%	6%	2	2%
3	1	France	11%	16%	5%	2	5%
4	6	Italy	9%	6%	4%	3	6%
5	4	United Kingdom	9%	11%	4%	3	11%
6	7	Israel	6%	5%	3%	3	2%
7	5	Poland	6%	8%	3%	3	2%
8	9	Portugal	2%	2%	1%	4	0%
9	8	Turkey	2%	3%	1%	2	5%
10	10	India	2%	2%	1%	4	3%

Table 3. Bot-infected computers by country, EMEA region

Source: Symantec Corporation

Şekil-01: Bot bulaşmış bilgisayar sayıları bakımından EMEA bölgesinde yer alan ilk 10 ülke

Bunun yanında, EMEA bölgesinde yer alan şehirler arasında en çok bot bulaşmış ilk 10 şehir sıralamasında başkentimizin de yer aldığını görüyoruz. Şekil-02’den de görülebileceği gibi, Ankara bu sıralamada 7. Sırada yer almakta. Her ne kadar hem Türkiye’nin hem de Ankara bir önceki 6 ay’a oranla

sıralamada gerilemiş olduğunu görmek sevindirici olsa da her iki kategoride de ilk 10 arasında yer almak ülkemiz açısından tehlikenin hangi boyutlarda olduğunu gösteriyor.

Regional Rank	Previous Regional Rank	City	Country
1	1	Madrid	Spain
2	9	Petah Tiqwa	Israel
3	7	Rome	Italy
4	5	Milan	Italy
5	2	London	United Kingdom
6	3	Paris	France
7	4	Ankara	Turkey
8	8	Lisbon	Portugal
9	6	Warsaw	Poland
10	12	Haifa	Israel

Table 4. Bot-infected computers by city, EMEA region

Source: Symantec Corporation

Şekil-02: Şehir bazında bot bulaşmış bilgisayar sayısı bakımından ilk 10 şehir

Bunun yanında, spam zombi olarak kullanılan bilgisayarlara ait istatistiksel bilgileri incelediğimizde yine ülkemizdeki durumu gözler önüne seren bir tabloyla karşılaşıyoruz. Şekil-03’de gösterilen tabloda görüldüğü gibi Türkiye spam için kullanılan zombi bilgisayarlar içeren ülkeler sıralamasında EMEA bölgesinde 5. sırada.

Regional Rank	Previous Rank	Country	Regional Percentage	Previous Regional Percentage	Worldwide Percentage	Previous Worldwide Percentage
1	1	Germany	17%	16%	9%	8%
2	4	Poland	11%	9%	6%	5%
3	5	Italy	10%	8%	5%	4%
4	2	France	9%	14%	5%	7%
5	6	Turkey	6%	6%	3%	3%
6	3	Spain	6%	13%	3%	7%
7	10	India	6%	4%	3%	2%
8	7	Israel	6%	5%	3%	3%
9	9	Russia	5%	4%	3%	2%
10	8	United Kingdom	4%	5%	2%	3%

Table 17. Top spam zombie countries

Source: Symantec Corporation

Şekil-03: Ülke bazında spam için kullanılan zombi bilgisayar sayısına göre sıralama

Spam zombi olarak kullanılan bilgisayarların şehir bazında sıralamasında ise ilginç bir bilgi daha yer alıyor. Ülkemizin en büyük iki şehri , İstanbul ve Ankara sıralamada 5 ve 6 sırada. Symantec’in raporunda yer alan ilginç notlardan birisi de 2007 yılının ilk yarısında en çok karşılaşılan 50 zararlı kodun %65’i

değerli ve gizli bilgileri çalmaya yönelik programlanmış kodlar. Sırf bu rakamlar bile karşı karşıya olduğumuz tehdidin hangi yöne doğru kaydığının görülmesi açısından yeterli diye düşünüyorum.

Symantec'in raporunda dikkat çeken başka bir başlık ise işletim sistemleri bazında zafiyet-yama ilişkisini gösteren yani açığın duyurulması ile bu açığı kapatmaya yönelik yamanın çıkartılması arasında geçen süreyi ele alan başlık. Şekil-04'de görüleceği gibi bu konuda en hızlı cevap veren üretici Microsoft. Burada gösterilen sürelerin 2007 yılı içerisinde duyurulan açıklar ve bu açıklara ilişkin yamaların çıkartılması için geçen sürelerin bir ortalaması olduğunu söylememiz gerekiyor. Yani özetle Microsoft açısından ele alırsak, işletim sistemindeki bir açığa ilişkin yamanın çıkartılması için geçen süre ortalama olarak 18 gün.

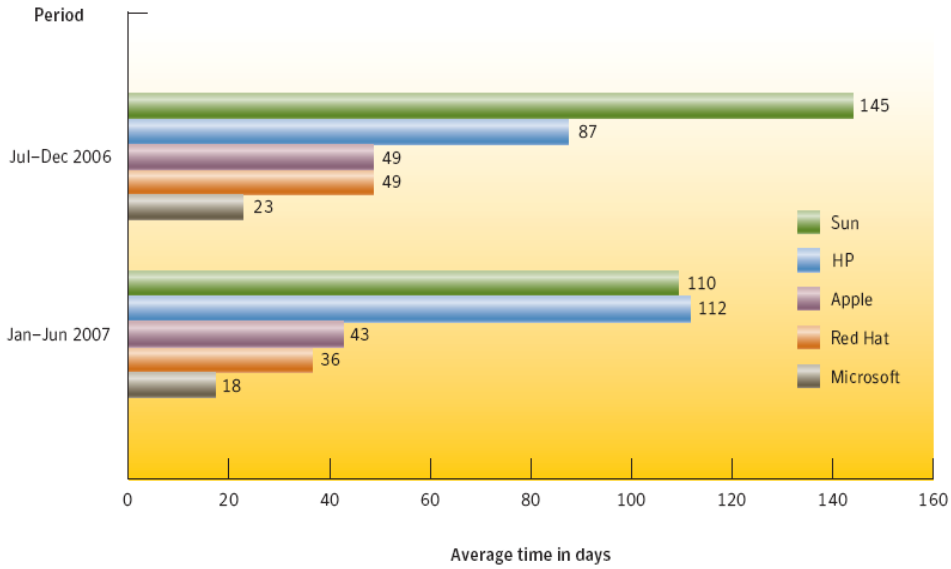


Figure 18. Patch development time for operating systems
Source: Symantec Corporation

Şekil-04: Zafiyet-Yama İlişkisi

Bu zafiyetlerin dağılımına göz attığımızda ise karşımıza beklediğimiz bir tablo çıkıyor. Tesbit edilen zafiyetlerinin hatırı sayılır bir kısmı istemci ve browser açıklarından meydana geliyor. Saldırganların açık bulma konusundaki çabalarının hangi yönde yoğunlaştığında göstergesi olan bu tabloyu Şekil-05'de bulabilirsiniz.

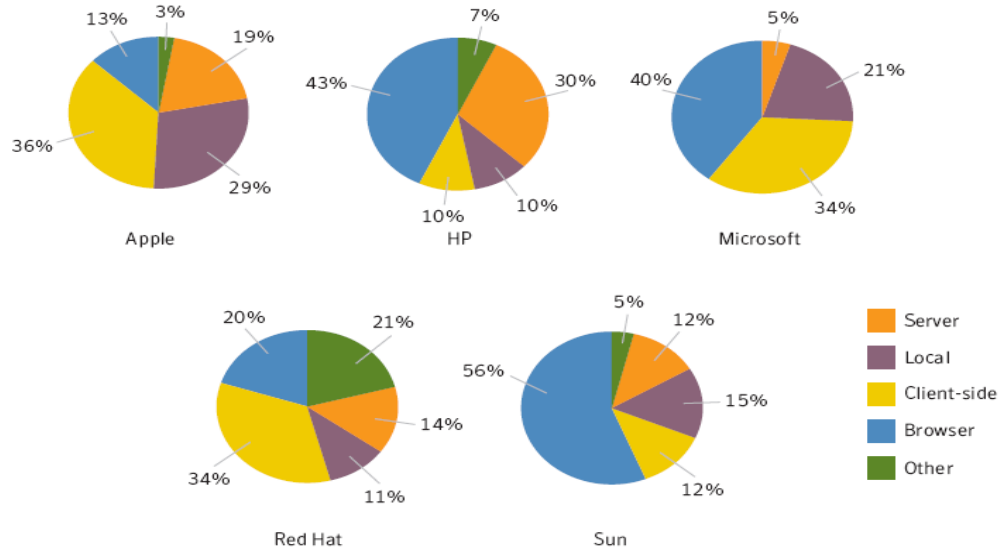


Figure 19. Patched operating system vulnerability by type
Source: Symantec Corporation

Şekil-05: Tesbit edilen açıkların açık tiplerine göre dağılımları

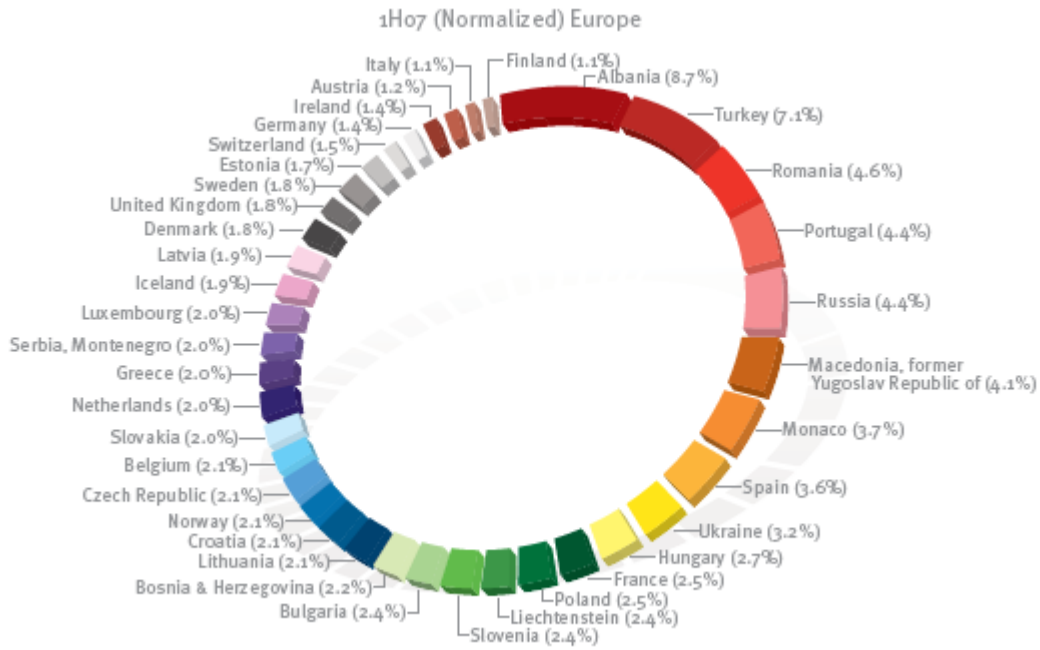
Biraz da Microsoft'un Security Intelligence Report'una göz atalım. Dikkat çeken ilk başlık 2007'nin ilk yarısında tesbit edilen zafiyet sayısı. Yılın ilk yarısında 3400'den fazla zafiyet tesbit edilmiş ve bu zafiyetlerin 2000'e yakınının kritiklik seviyesi yüksek. Zafiyetler ve kritiklik seviyeleri değerlendirmesinde National Vulnerability Database (NVD) (<http://nvd.nist.gov>) 'in kritiklik seviyeleri baz alınmış.

Bununla birlikte Microsoft, tesbit edilen açıkları işletim sisteminin açıkları ve işletim sistemi dışındaki diğer açıklar şeklinde ayırmış ve burdada iki kategori arasındaki oran farkını gözler önüne sermiş. 2007'nin ilk yarısında tesbit edilen açıkların içinde işletim sistemi seviyesindeki açıkların tesbit edilen bütün açıklara oranı %10'un bile altında. Hazır işletim sistemi seviyesindeki açıklardan bahsetmişken Microsoft'un raporunda yer alan ve Microsoft'un kendi ürünlerine ilişkin tesbit edilen zafiyetler ve bu zafiyetlerin exploit edilip edilemediğine dair bilgilerin yer aldığı tablodan Windows işletim sistemleri ile ilgili kısma biraz değinelim. Şekil-06'dan görülebileceği gibi 2007'nin ilk altı ayında Windows XP işletim sistemi için tesbit edilen açık sayısı 13 iken bu açıkları kullanan exploit sayısı 4. Yüzde olarak verilen rakamlara baktığımızda ise Windows XP haricindeki diğer işletim sistemlerinin tamamında belirli bir düşüş söz konusu.

By Microsoft Security Bulletin		2006			2007			Delta Microsoft Security Bulletin
Product	Version	Microsoft Security Bulletin Count	Exploits	Percent	Microsoft Security Bulletin Count	Exploits	Percent	
Windows								
	98	5	0	0.0%	0	0	0.0%	
	ME	5	0	0.0%	0	0	0.0%	
	NT	3	1	33.3%	0	0	-33.3%	
	2000	26	9	34.6%	11	2	-16.4%	
	XP	27	8	29.6%	13	4	1.1%	
	2003	27	7	25.9%	13	2	-10.5%	
	Vista	1	1	100.0%	4	2	-50.0%	

Şekil-06:Microsoft işletim sistemleri bazında tesbit edilen açıklar ve exploitler ilişkisini gösteren tablo

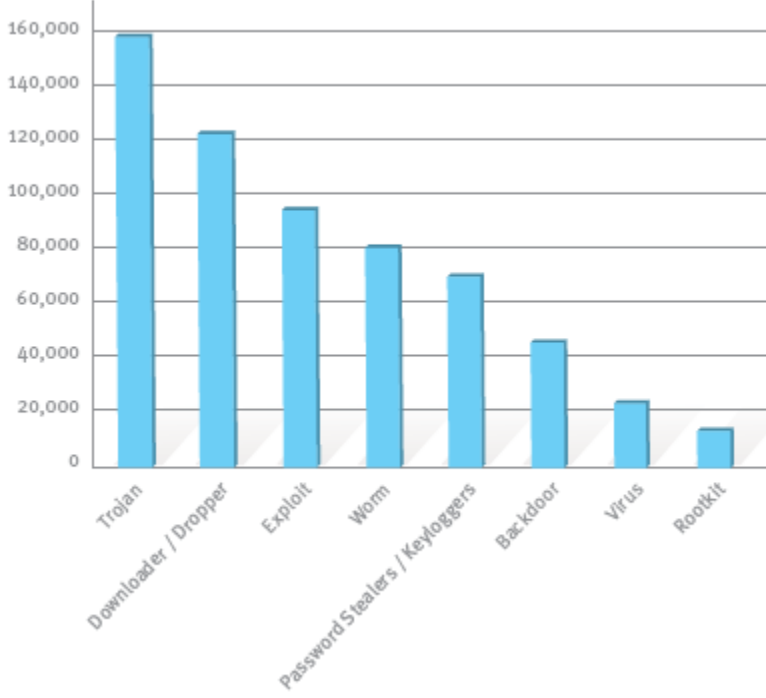
Microsoft'un raporundan değinmek istediğim bir diğer başlık ise MSRT (Malicious Software Removal Tool) istatistiklerinin yer aldığı başlık olacak. Şekil-7'de ülkemizin de içinde yer aldığı Avrupadaki ülkeler hakkında bilgilerin bulunduğu grafiği bulabilirsiniz. Buradaki rakamlar 2007 yılının ilk 6 aylık kısmında MSRT tarafından temizlenen zararlı kodların yüzdesel olarak genel toplam'a oranını gösteriyor. Türkiye'nin burada %7.1'lık bir değerle tüm Avrupa içinde ikinci sırada olması oldukça düşündürücü.



Şekil-07:MSRT tarafından temizlenen zararlı kod sayısının yüzdesel olarak ülke bazlı dağılımı

Tespit edilen bu zararlı kodların türlerine göre yüzdesel olarak dağılımlarını gösteren Şekil-08'deki grafik ise bize zararlı kod yazarlarının motivasyonun hangi yöne doğru kaydığını gösterir mahiyette.

FIGURE 31. Number of variants from over 7,000 malware families in 1H07



Şekil-08:Microsoft tarafından tespit edilen zararlı kodların türlere göre sıralaması

Halil ÖZTÜRKÇİ

Microsoft MVP (Windows Security)

CISSP,CISA, CEH,CHFI,CCSI,CCSE,CCNP