Microsoft Güvenlik İstihbarat Raporu
8. Sayı (Temmuz - Aralık 2009 Dönemi)

Önemli Bulgular Özet Raporu

Giriş

Microsoft® Güvenlik İstihbarat Raporu 8. sayısı, hem Microsoft hem de üçüncü taraf yazılımlarında görülen kötü amaçlı ve istenmeyen yazılımlar, güvenlik ihlalleri, yazılım güvenlik açıkları ve güvenlik açıklarından yararlanma hakkında ayrıntılı görüşler sunmaktadır. Microsoft bu görüşleri, başta 2009'un ikinci yarısına odaklanarak (2H09) son birkaç yıldaki ayrıntılı analizlere dayanarak geliştirmiştir[1].

Bu belgede raporun önemli bulguları özetlenmektedir. Dünya genelindeki 26'dan fazla ülke/bölgede bulunan eğilimlerin ayrıntılı bir analizini içeren *Güvenlik İstihbarat Raporu (GİR)*, raporda belgelenen tehditleri yönetmek için kullanılabilecek stratejiler, hafifletme önlemleri ve karşı tedbirler önermektedir.

Tüm *Güvenlik İstihbarat Raporu*, raporun önceki sayıları ve ilgili videolar www.microsoft.com/sir adresinden indirilebilir.

Bilgisayar tehditlerinin genel görünümü sürekli değişim gösteriyor. Tehditler şöhret kazanmak isteyen bilgisayar korsanlarının yerine maddi kazanç için veri hırsızlığı yapan organize suç örgütlerinden gelmeye devam ettikçe, kamuoyundaki endişeler de yükselmeye devam ediyor. Microsoft, müşterilerine daha güvenli, özel ve güvenilir bir bilişim deneyimi sağlama stratejisi doğrultusunda 2002 yılında Güvenilir Bilgi İşlem'i (TwC) kurdu.

TwC Güvenlik; güvenlik sorunlarına çözüm getirmek, değişen tehditlerin daha iyi anlaşılması için gerek duyulan hizmetleri, bilgileri ve yanıtları sağlamak, müşterilerin çevrimiçi tehditlerden korunmasına yardımcı olmak ve bilgileri geniş güvenlik ekosistemiyle paylaşmak amacıyla birlikte çalışan üç teknoloji merkezinden oluşmaktadır. Bu üç güvenlik merkezi şunlardır:

- Microsoft Kötü Amaçlı Yazılımdan Koruma Merkezi
- Microsoft Güvenlik Yanıt Merkezi
- Microsoft Güvenlik Mühendislik Merkezi

Bu üç güvenlik merkezinin bloglarına ve “Data Privacy Imperative” blogu gibi diğer bloglara www.microsoft.com/twc/blogs adresinden erişebilirsiniz.

Bu *Önemli Bilgiler Özet Raporu* ve tam *Güvenlik İstihbarat Raporu*'ndaki veri ve analizler, bu üç güvenlik merkezinin ve çeşitli Microsoft ürün gruplarındaki iş ortaklarının bakış açısından sunulmaktadır.

[1] Raporda farklı raporlama dönemlerine işaret etmek için kullanılan nHYY adlandırma biçiminde nH kısaltması yılın birinci (1) veya ikinci (2) yarısı anlamına gelirken, YY kısaltması yıl anlamına gelir. Örneğin, 2H09 kısaltması 2009'un ikinci yarısını kapsayan dönemi (1 Temmuz - 31 Aralık) belirtirken, 2H08 kısaltması 2008'in ikinci yarısını kapsayan dönemi (1 Temmuz - 31 Aralık) belirtmektedir.

Microsoft Kötü Amaçlı Yazılımdan Koruma Merkezi'nin Önemli Bulguları

Küresel Kötü Amaçlı ve İstenmeyen Yazılım Eğilimleri

Microsoft güvenlik ürünleri, kullanıcıların onayı alınarak dünya genelindeki 500 milyon bilgisayardan ve Internet'teki en yoğun çevrimiçi servislerden veri toplamaktadır. Bu veriler üzerinde gerçekleştirilen analizler, dünya çapındaki kötü amaçlı yazılım ve istenmeyen yazılım etkinlikleri hakkında kapsamlı ve benzersiz bilgiler sağlıyor.

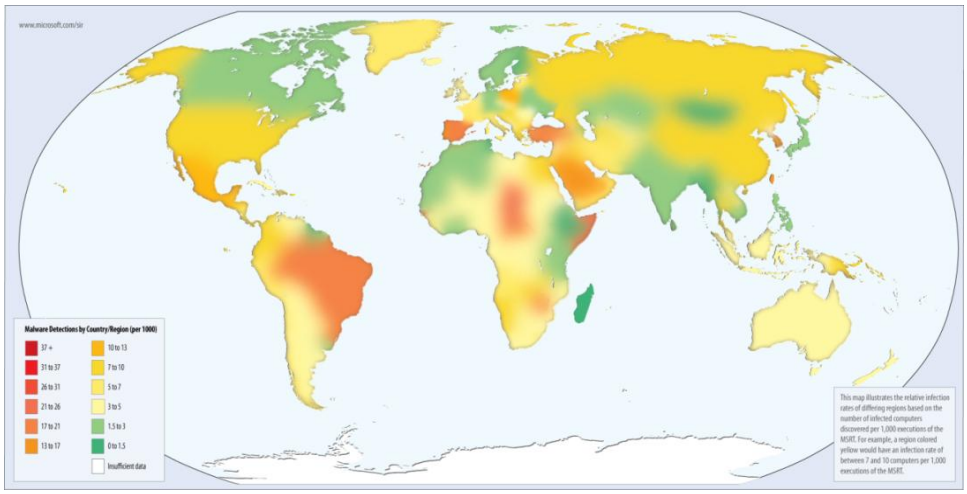
Coğrafi Eğilimler

Şekil 1: 2H09'da Microsoft masaüstü kötü amaçlı yazılımdan koruma ürünleri tarafından en fazla bilgisayarın temizlendiği ilk 15 konum (tam *GİR (Güvenlik İstihbarat Raporu)* ilk 25 konumu içermektedir)

	Ülke/Bölge	Temizlenen Bilgisayarlar (2H09)	Temizlenen Bilgisayarlar (1H09)	Değişiklik
1	Amerika Birleşik Devletleri	15.383.476	13.971.056	%10,1 ▲
2	Çin	3.333.368	2.799.456	%19,1 ▲
3	Brezilya	2.496.674	2.156.259	%15,8 ▲
4	Birleşik Krallık	2.016.132	2.043.431	%-1,3 ▼
5	İspanya	1.650.440	1.853.234	%-10,9 ▼
6	Fransa	1.538.749	1.703.225	%-9,7 ▼
7	Kore	1.367.266	1.619.135	%-15,6 ▼
8	Almanya	1.130.632	1.086.473	%4,1 ▲
9	Kanada	967.381	942.826	%2,6 ▲
10	İtalya	954.617	1.192.867	%-20,0 ▼
11	Meksika	915.786	957.697	%-4,4 ▼
12	Türkiye	857.463	1.161.133	%-26,2 ▼
13	Rusya	677.601	581.601	%16,5 ▲
14	Tayvan	628.202	781.214	%-19,6 ▼
15	Japonya	609.066	553.417	%10,1 ▲
	Dünya Çapında	41.024.375	39.328.515	%4,3 ▲

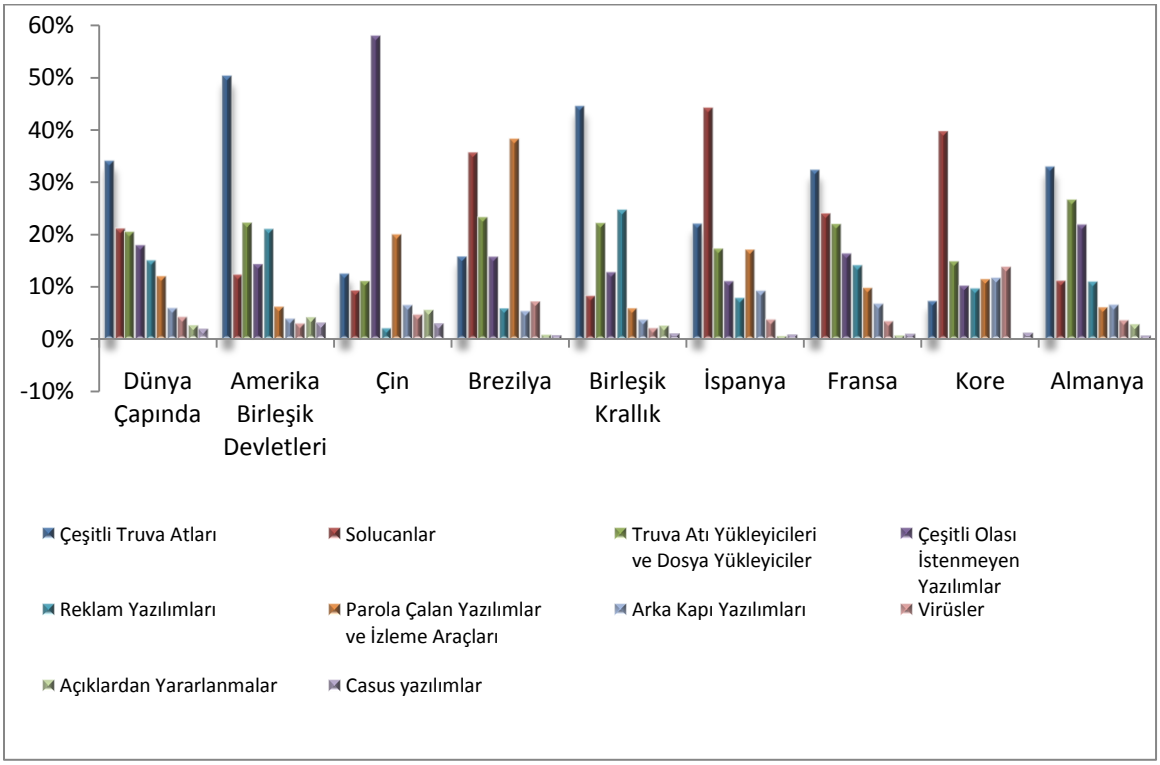
- Temizlenen bilgisayar sayısındaki en büyük iki artış, 1H09 dönemine kıyasla sırasıyla yüzde 19,1 ve yüzde 15,8 ile Çin ve Brezilya'da gerçekleşti. Bu artışın büyük bir bölümü, lisanslı Windows kullanıcılarına ücretsiz olarak sunulan kötü amaçlı yazılımdan koruma çözümü Microsoft Security Essentials'ın Eylül 2009 sürümünden kaynaklandı. Çin ve Brezilya Security Essentials'ı en erken kullanmaya başlayan ülkeler oldu.
- Birçok ülkede bulaşma oranlarında önemli düşüşler yaşandı:
  - Temizlenen bilgisayar sayısındaki en büyük düşüş, esas olarak çevrimiçi oyun oyuncularını hedef alan Win32/Taterf ve Win32/Frethog adlı iki parola çalan yazılımın etkisinin azalmasına bağlı olarak yüzde 26,2 ile Türkiye'de gerçekleşti.
  - Taterf ve Frethog'un azalan etkisi Tayvan'daki yüzde 19,6'lık düşüşte büyük rol oynadı.
  - İtalya'daki yüzde 20,0'lik düşüş, büyük oranda Truva atı ailesinden Win32/Wintrim'in tespit edilme sayısındaki hızlı azalmadan kaynaklanıyor.

Şekil 2: CCM[2] cinsinden 2H09 döneminde ülke/bölge bazında görülen bulaşma oranları, 2H09 döneminde dünya genelinde MSRT aracının ayda ortalama en az 1 milyon kez çalıştırıldığı bölgeler için geçerlidir.



Tam *GİR* 200+ ülke/bölgenin CCM rakamlarını içermektedir.

Şekil 3: 2H09 döneminde, Microsoft masaüstü kötü amaçlı yazılımdan koruma ürünleriyle temizlenen tüm bilgisayarlardaki vakalara göre dünya genelindeki ve en fazla virüs bulaşmış bilgisayarın bulunduğu sekiz bölgedeki tehdit kategorileri

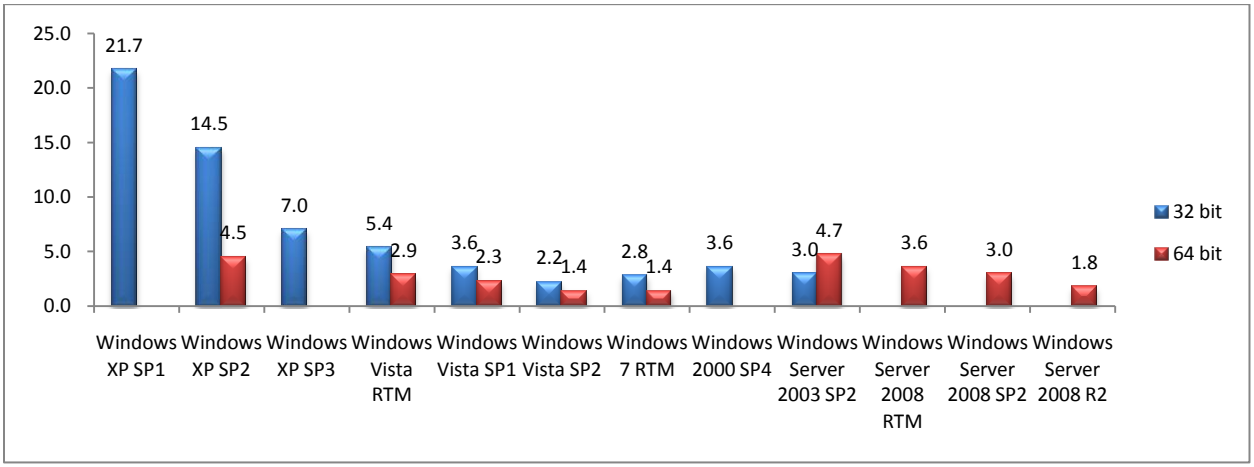


[2] Farklı bölgelerdeki bilgisayar sayılarını birbiriyle karşılaştırmak üzere kullanılabilecek tutarlı bir bulaşma ölçümü sağlamak için, bu rapordaki bulaşma oranları bin çalıştırma başına temizlenen bilgisayar sayısı adı verilen veya MSRT'nin çalıştırıldığı her 1000 defada temizlendiği rapor edilen bilgisayar sayısını temsil eden CCM ölçüsü kullanılarak ifade edilmektedir. (CCM'deki M harfi, Latince'de bin anlamına gelen mille sözcüğünün kısaltmasıdır.)

- Amerika Birleşik Devletleri ve Birleşik Krallık'taki tehdit ortamları büyük ölçüde benzerlik göstermektedir. Her iki bölge hemen aynı tehdit kategorisi oranına sahiptir ve ilk 10 virüs ailesinden 7'si aynıdır. Çeşitli Truva Atları, en büyük tek tehdit kategorisidir. Win32/FakeXPA, Win32/Renos ve Win32/Alureon gibi aileler her iki konumda da üst sıralarda yer almaktadır.
- Çin'de yaygın olan çoğu tehdit, diğer hiçbir bölgede en büyük tehditler listesinde yer almayan yerel ailelerdir. Bunlar arasında Çince tarayıcı araç çubuğu olan Win32/BaiduSobar virüsünün bazı sürümleri ve Çin'de yaygın olan çevrimiçi oyunları hedef alan Win32/Lolyda ve Win32/Ceekat gibi parola çalan yazılımlar bulunmaktadır.
- Brezilya'da, Brezilya bankalarının çevrimiçi kullanıcılarını hedef alan birçok Portekizce parola çalan yazılım yüzünden Parola Çalan Yazılımlar ve İzleme Araçları en yaygın tehdit kategorisini oluşturmaktadır. Win32/Bancos, parola çalan yazılımların en yaygın örneğidir.
- Kore'de, başta çevrimiçi oyun oyuncularını hedef alan Win32/Taterf olmak üzere birçok solucan bulunmaktadır. Taterf'in Kore'de yaygın olması, solucanların Kore'de çok popüler olan Internet kafelerde ve LAN oyun merkezlerinde kolayca yayılabilme yeteneklerinden kaynaklanmaktadır.

İşletim Sistemi Eğilimleri

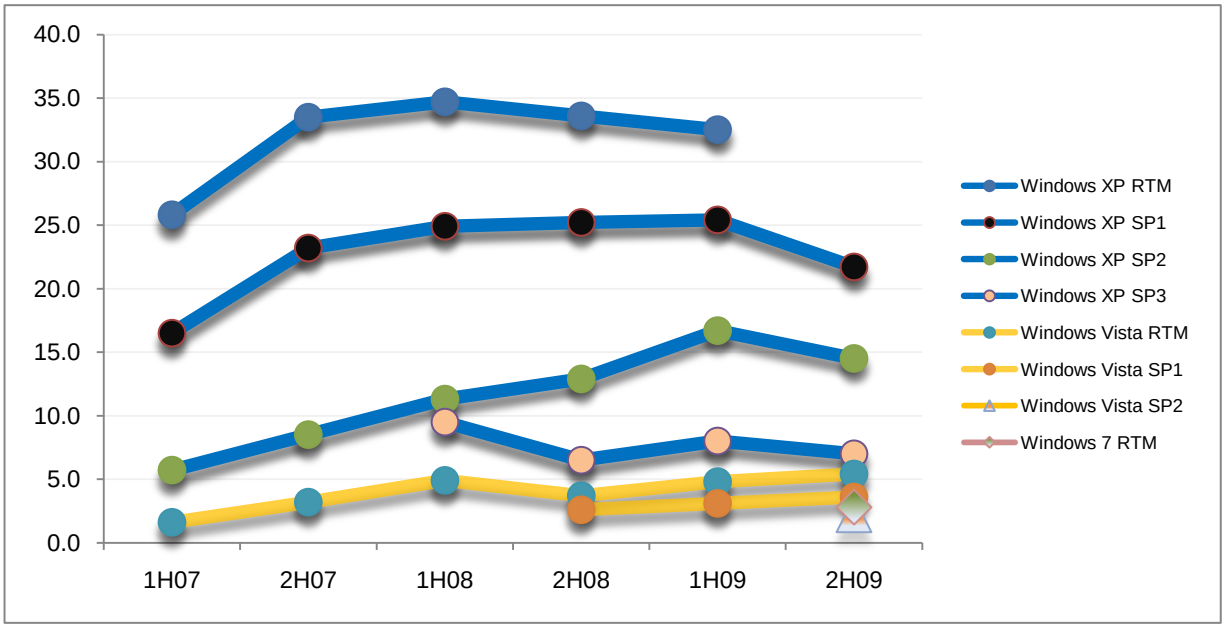
Şekil 4: 2H09 döneminde işletim sistemine göre her 1.000 MSRT çalışmasında temizlenen bilgisayar sayısı



- Önceki dönemlerde olduğu gibi, hem istemci hem de sunucu platformlarında, yakın zamanda yayınlanan işletim sistemleri ve hizmet paketlerinde bulaşma oranları önceki sürümlere göre istikrarlı bir şekilde daha düşüktür.
- 2H09 döneminde piyasaya sürülen Windows 7 ve Windows Vista® Service Pack 2, tablodaki platformlar arasında en düşük bulaşma oranına sahiptir.
    - Windows 7 ve Windows Vista SP2'nin 64 bit sürümleri, 2H09 döneminde diğer tüm işletim sistemi yapılandırmalarından daha düşük bulaşma oranlarına (her ikisi için 1,4) sahipti ve her ikisinin 32-bit sürümleri de en güncel hizmet paketi olan SP3 yüklü Windows XP'nin bulaşma oranının yarısından daha düşük bir bulaşma oranına sahipti.
- Hizmet paketleriyle güncellenmiş işletim sistemlerinde, her bir hizmet paketi kendinden bir öncekine göre daha düşük bir bulaşma oranına sahiptir.
    - Windows XP SP3'ün bulaşma oranı, SP2 yüklü sürümlere göre yarıdan daha düşük ve SP1 yüklü sürümlere göre üçte birden daha düşüktür.
    - Benzer şekilde, Windows Vista SP2 de, Windows Vista RTM'den daha düşük bir bulaşma oranına sahip SP1'e göre düşük bir bulaşma oranına sahiptir.
    - Sunucu işletim sistemlerinde, Windows Server® 2008 SP2'nin bulaşma oranı 3,0'dır, bu oran selefi Windows Server 2008 RTM'ye göre yüzde 20 daha düşüktür.

Aşağıdaki şekil, bu eğilimlerin zaman içindeki istikrarını göstermektedir; Windows XP ve Windows Vista 32 bit işletim sistemlerinin farklı sürümlerinin 1H07 ve 2H09 arasındaki her bir altı aylık dönemdeki bulaşma oranlarını gösterilmiştir.

Şekil 5: Windows XP ve Windows Vista 32 bit sürümlerinin CCM eğilimleri, 1H07–2H09



Dünya Genelindeki Kategori Eğilimleri

Şekil 6: 2H09 döneminde Microsoft masaüstü kötü amaçlı yazılımdan koruma araçları tarafından tespit edilen ilk 10 kötü amaçlı ve istenmeyen yazılım aileleri (tam *GİR* ilk 25 aileyi içermektedir)

	Aile	En Önemli Kategori	Temizlenen Bilgisayar Sayısı (2H09)
1	Win32/Taterf	Solucanlar	3.921.963
2	Win32/Renos†	Truva Atı Yükleyicileri ve Dosya Yükleyiciler	3.640.697
3	Win32/FakeXPA*	Çeşitli Truva Atları	2.939.542
4	Win32/Alureon†	Çeşitli Truva Atları	2.694.128
5	Win32/Conficker†	Solucanlar	1.919.333 [3]
6	Win32/Frethog	Parola Çalan Yazılımlar ve İzleme Araçları	1.823.066
7	Win32/Agent	Çeşitli Truva Atları	1.621.051
8	Win32/BaiduSobar	Çeşitli Olası İstenmeyen Yazılımlar	1.602.230
9	Win32/GameVance	Reklam Yazılımları	1.553.646
10	Win32/Hotbar	Reklam Yazılımları	1.476.838

Yıldız işaretleri (*) sahte güvenlik yazılımı ailelerini işaret eder.
Hançer işaretleri (†) sahte güvenlik yazılımı indirdiği gözlemlenen aileleri işaret eder.

- Genel olarak, en büyük tehdidin tespit edilme sayısı 2009'un ilk yarısına göre büyük oranda düşmüştür.
  - 1H09 döneminde, Microsoft masaüstü kötü amaçlı yazılımdan koruma araçları tarafından yedi aile en az 2 milyon bilgisayardan temizlenirken 2H09'da yalnızca dört aile temizlenmişti.
  - 2H09'un en önemli ailesi olan Win32/Taterf bile bu dönemde 1H09'a kıyasla neredeyse 1 milyon daha az bilgisayardan temizlendi.

[3] Aktif Win32/Conficker bulaşma vakalarını izleyen Shadowserver Foundation, 2H09 döneminin son gününde Conficker bulaşan 4,6 milyon bilgisayarın Shadowserver tarafından izlendiğini bildirdi; bu rakam 1H09 döneminin son gününde 5,2 milyondu. Kötü amaçlı yazılımdan koruma yazılımları tarafından bulunan ve temizlenen kötü amaçlı yazılım miktarını hesaplamak, bazen bu yazılımların bulaştığı bilgisayarlar gözlemlenerek yapılan tahminlerden çok farklı rakamlar ortaya çıkarabilir ve hangi yöntemin tercih edilebilir olduğu konusunda yaygın bir mutabakat yoktur.

- 2H09 döneminde 3,9 milyon bilgisayara bulaşan Taterf, 1H09'un en yaygın ailesi olan ve bu dönemde 9,0 milyon bilgisayardan temizlenen Win32/Zlob virüsünden çok daha az sayıda bilgisayara bulaşmıştı.
- Birçok saldırgan; botnet, sahte yazılım ve parola çalan yazılım gibi diğer tehditleri bilgisayarlara yaymak için Win32/Renos ve ASX/Wimad (2H09 döneminde sırasıyla en yaygın ikinci ve on birinci aile) gibi Truva atı yükleyicilerini ve dosya yükleyen Truva atlarını kullanmaktadır.

- Genellikle, 2H09'daki kötü amaçlı yazılım dağılımında orta derecede yaygın olan farklı aileler dikkati çekmekte, büyük oranda temizlenen tekli aileler listenin üst sıralarında daha az yer almaktadır. Microsoft Security Essentials'ın hızla kullanılmaya başlanması da temizlenen virüs sayısındaki düşüşten kısmen sorumlu olabilir.

Örnek Çoğalmasındaki Eğilimler

Kötü amaçlı yazılım yazarları, virüs koruma yazılımı üreticilerinin piyasaya yeni imza sürme hızını geçmek amacıyla sürekli yeni farklı sürümler yayınlayarak virüslerin saptanmasını önlemeye çalışır. En aktif kötü amaçlı yazılım ailelerini veya kategorilerini belirlemenin yolu benzersiz örnekleri saymaktan geçer.

Şekil 7: Kategori bazında MMPC'ye sunulan benzersiz örnekler, 1H09–2H09

Kategori	2H09	1H09	Fark
Virüsler	71.991.221	68.008.496	%5,9 ▲
Çeşitli Truva Atları	26.881.574	23.474.539	%14,5 ▲
Truva Atı Yükleyicileri ve Dosya Yükleyiciler	9.107.556	6.251.286	%45,7 ▲
Çeşitli Olası İstenmeyen Yazılımlar	4.674.336	2.753.008	%69,8 ▲
Reklam Yazılımları	3.492.743	3.402.224	%2,7 ▲
Açıklardan Yararlanmalar	3.341.427	1.311.250	%154,8 ▲
Solucanlar	3.006.966	2.707.560	%11,1 ▲
Parola Çalan Yazılımlar ve İzleme Araçları	2.217.902	7 087 141	%-68,7 ▼
Arka Kapı Yazılımları	812.256	589.747	%37,7 ▲
Casus yazılımlar	678.273	269.556	%151,6 ▲
Toplam	**126.204.254**	**115.854.807**	**%8,9**

- 2H09'da 126 milyondan fazla zararlı örnek saptandı.
- Parola Çalan Yazılımlar ve İzleme Araçları kategorisindeki düşüş büyük ölçüde 1H09'da 5,7 milyon olan örnek sayısı 2H09'da 100.000'in altına inen Win32/Lolyda'dan kaynaklandı.
- Casus Yazılım kategorisindeki artış büyük ölçüde 2H09'da önceki döneme göre yaklaşık beş kat daha fazla benzersiz örneği bulunan Win32/ShopAtHome'dan kaynaklandı.
- Virüs örneklerinin büyük sayılara ulaşmasının nedeni, virüslerin birçok farklı dosyaya bulaşarak her biri benzersiz örnekler oluşturmasıdır. Bu nedenle, virüslerin örnek sayısı bu ailelerin büyük sayıdaki gerçek sürümlerinin sayısı olarak alınmamalıdır.

Sahte Güvenlik Yazılımı

Kurbanın bilgisayarındaki virüsler veya güvenlik açıklarıyla ilgili sahte veya yanlış yönlendirici uyarılar görüntüleyen ve bu sözde sorunları belirli bir ücret karşılığında gidermeyi teklif eden sahte güvenlik yazılımları, saldırganların kurbanlardan para kapmak için kullandıkları en yaygın yöntemlerden biri haline geldi.

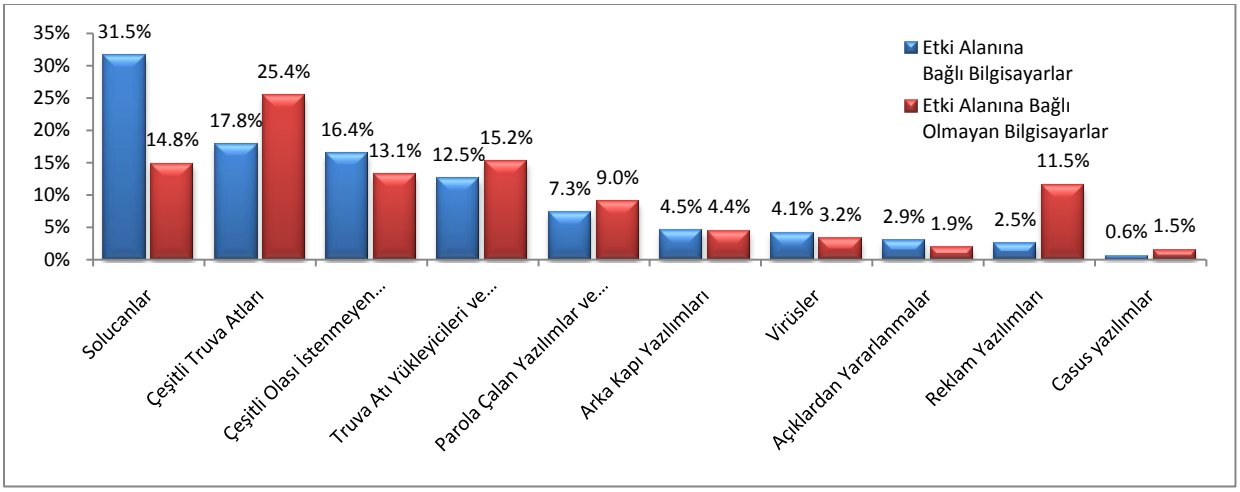
Şekil 8: 2H09 dönemindeki en yaygın sahte güvenlik yazılımı ailesi olan Win32/FakeXPA çeşitlerinden sahte "güvenlik taramaları"

- Microsoft güvenlik ürünlerinin sahte güvenlik yazılımlarıyla ilgili kötü amaçlı yazılımları temizlediği bilgisayar sayısı 1H09'da 5,3 milyonken, 2H09'da artış göstererek 7,8 milyona yükseldi. Yüzde 46,5'lik bu artış, sahte güvenlik yazılımlarının diğer daha az yaygın virüs türlerine kıyasla dağıtıcılarına daha fazla kazanç sağladığını gösteriyor.
- Bir sahte güvenlik yazılımı ailesi olan Win32/FakeXPA, Microsoft masaüstü güvenlik ürünlerinin 2H09'da dünya genelinde saptadığı en yaygın üçüncü tehditti. Diğer üç tehdit olan Win32/Yektel, Win32/Fakespypro ve Win32/Winwebsec sırasıyla on birinci, on dördüncü ve on yedinci sıradaydı.
- Tam *GİR*, Microsoft'un en fazla sahte güvenlik yazılımını bulduğu bölgelerin ve bu tehditlerin her bir bölgedeki en yaygın ailelerinin ayrıntılı coğrafik dökümünü içermektedir.
- Tüketicileri sahte güvenlik yazılımlarının güvenliklerine ve gizliliklerine yönelik artan tehdidi konusunda bilgilendirmek için hazırlanmış üç adet yeni tüketici odaklı video http://www.microsoft.com/protect adresine konulmuştur.

Ev Kullanıcıları ve Kurumsal Kullanıcılar açısından Tehdit Dağılımı

Microsoft masaüstü kötü amaçlı yazılımdan koruma ürünleri ve araçlarının ürettiği bulaşma verileri, virüs bulaşan bilgisayarın bir Active Directory® Etki Alanı Hizmetleri etki alanına ait olup olmadığı bilgisini içerir. Etki alanları neredeyse tamamen kurumsal ortamlarda kullanılır ve bir etki alanına ait olmayan bilgisayarlar genellikle evde veya kurumsal olmayan diğer ortamlarda kullanılan bilgisayarlardır. Etki alanındaki bilgisayarlar ve etki alanında olmayan bilgisayarların karşılaştığı tehditlerin karşılaştırılması, saldırganların kurumsal kullanıcıları ve ev kullanıcılarını hedef aldığı farklı yöntemler ve her bir ortamda hangi tehditlerin başarılı olabileceği hakkında bilgi sağlayabilir.

Şekil 9: 2H09 döneminde etki alanına bağlı ve etki alanına bağlı olmayan bilgisayarlar için tehdit kategorisi dökümü



- Etki alanına bağlı olmayan bilgisayarlara kıyasla etki alanına bağlı bilgisayarlar solucanlarla daha fazla karşılaşabilir, bunun birincil nedeni solucanların yayılma şeklidir. Genellikle, solucanlar en etkin şekilde ev ortamlarına kıyasla kurumsal ortamlarda daha yaygın olarak kullanılan güvenli olmayan dosya paylaşımı ve çıkarılabilir depolama birimleri yoluyla yayılmaktadır.
  - Etki alanına bağlı bilgisayarlarda saptanan ilk 10 aileden dördünü solucanlar oluşturuyor.
  - Genel Internet'e göre tipik bir kurumsal ağ ortamında çok daha etkin bir şekilde çalışan birçok yayılma yöntemini kullanabilen Win32/Conficker virüsü listede açık ara birinci.
  - Benzer şekilde, çıkarılabilir sürücüleri hedef alan Win32/Autorun virüsü dosya alıp vermek için bu birimlerin sıklıkla kullanıldığı etki alanı ortamlarında daha yaygın olarak görülmektedir.
- Bunun aksine, Reklam Yazılımı ve Çeşitli Truva Atları kategorileri etki alanına bağlı olmayan bilgisayarlarda daha yaygın olarak görülmektedir.

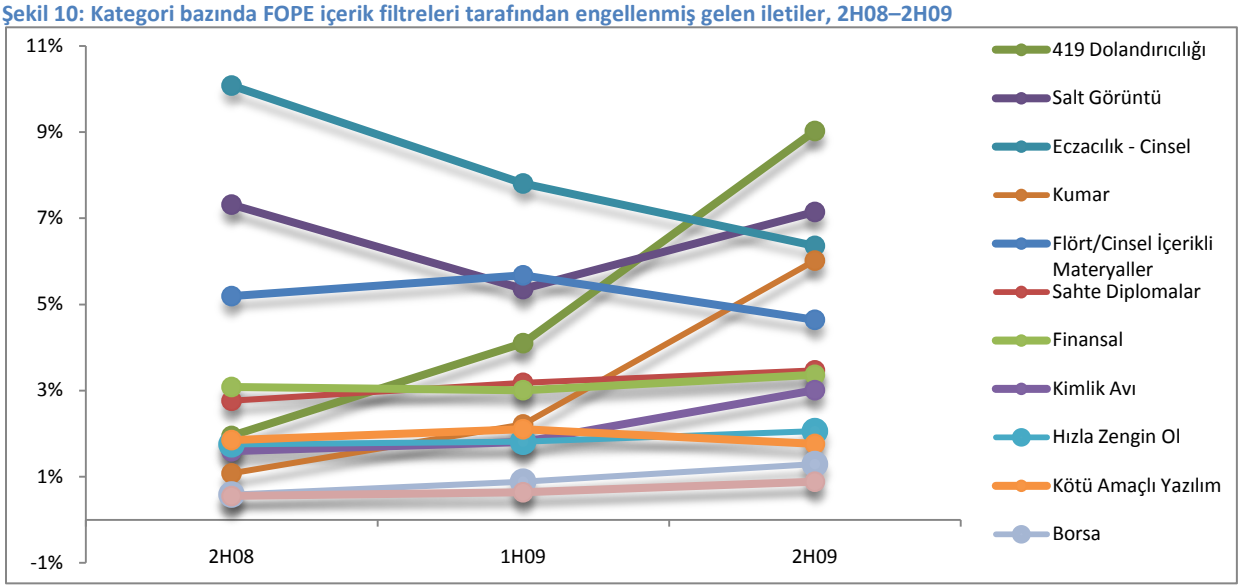
E-posta Tehditleri

Bu bölümdeki veriler, binlerce kurumsal müşteri için istenmeyen e-posta, kimlik avı ve kötü amaçlı yazılım filtreleme hizmetleri sağlayan Microsoft Forefront Online Protection for Exchange (FOPE) tarafından filtrelenmiş e-postalara dayanmaktadır.

Avans ücreti dolandırıcılığı (diğer adıyla “419 dolandırıcılığı”) ve kumarla ilgili istenmeyen e-posta iletileri 2H09 döneminde büyük artış gösterdi. Diğer birçok kategori yüzde cinsinden nispeten değişmeden kaldı.

- Avans ücreti dolandırıcılığı, iletiyi gönderenin büyük miktarda bir paraya hak sahibi olduğunu fakat bazı nedenlerle bu paraya doğrudan erişemediğini öne sürdüğü yaygın bir güven kazanma tuzağıdır. Genellikle, bürokratik formaliteler veya siyasi rüşvet gibi bir neden belirtilir. Gönderen, potansiyel kurbandan memurlara rüşvet vermek veya tutarın tamamını çekebilmek üzere gerekli ücretleri ödeyebilmek için kendisine geçici bir borç vermesini ister. Karşılığında, gönderen hedef kişiye mirastan ilk borçtan çok daha büyük bir miktara tekabül eden bir pay verme sözünü verir.
- Bu iletiler genellikle Nijerya (“419” sayısı, Nijerya Ceza Kanunu'nun dolandırıcılıkla ilgili maddesine işaret eder) ile Sierra Leone, Fildişi Kıyısı (Côte d'Ivoire) ve Burkina Faso gibi diğer Batı Afrika ülkeleriyle ilişkilidir.

Şekil 10: Kategori bazında FOPE içerik filtreleri tarafından engellenmiş gelen iletiler, 2H08–2H09

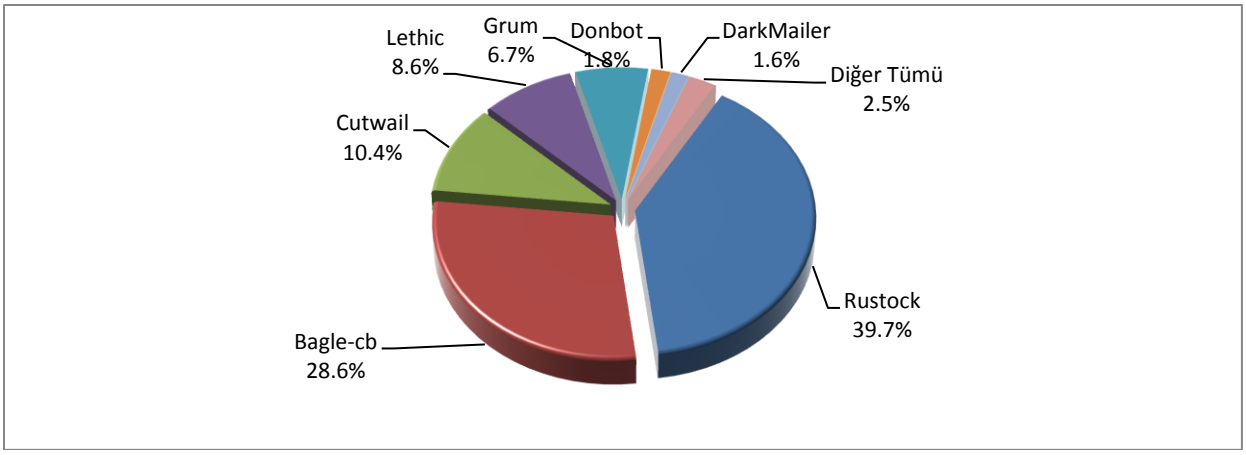


Şekil 11: Gönderilen tüm istenmeyen e-postalar içindeki yüzdesi bazında en fazla istenmeyen e-posta gönderen ilk 5 bölge, 2H09 dönemi

	Ülke	Yüzde
1	Amerika Birleşik Devletleri	%27,0
2	Kore	%6,9
3	Çin	%6,1
4	Brezilya	%5,8
5	Rusya	%2,9

Bir saldırgan tarafından uzaktan kontrol edilebilen kötü amaçlı yazılımların bulaştığı bilgisayarların botnet'leri ve istenmeyen e-posta ağları, günümüzde gönderilen istenmeyen e-postaların büyük bir bölümünden sorumludur. Botnet'lerin istenmeyen e-posta yayılımındaki etkisini ölçmek için, FOPE bilinen botnet'lerle ilişkili olduğu bildirilen IP adreslerinden gönderilen istenmeyen e-posta iletilerini izler.

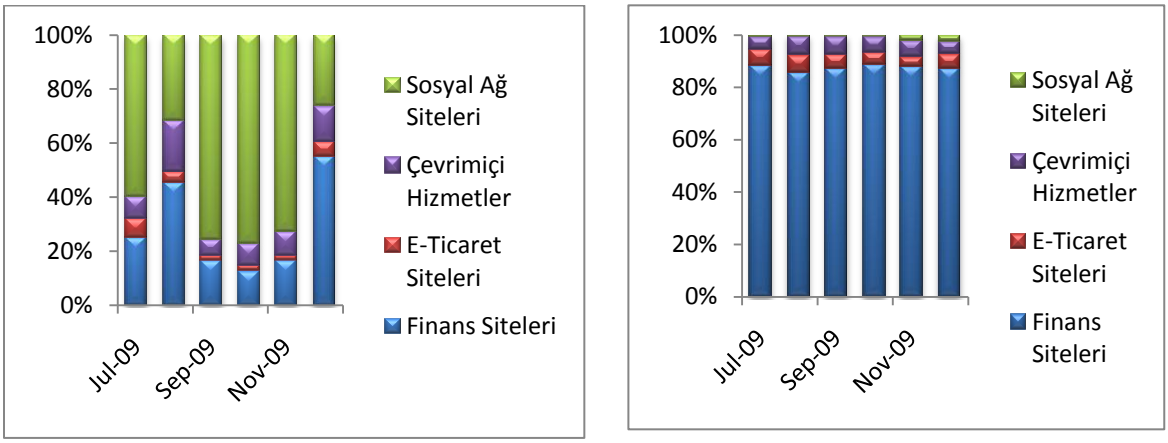
Şekil 12: 2H09'da gözlemlenen hemen hemen tüm botnet istenmeyen e-postalarından birkaç botnet sorumludur (tam *GİR* raporu daha fazla bilgi içermektedir)



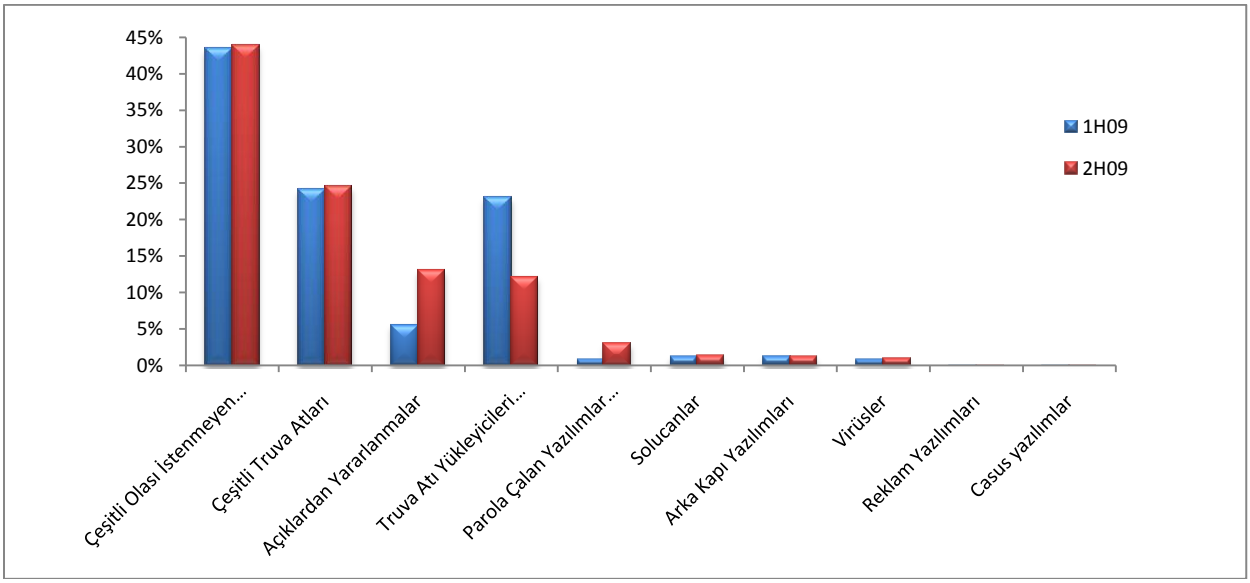
Kötü Amaçlı Web Siteleri

Önceki GİR sayılarında yayınlandığı üzere, sosyal ağlar en yüksek toplam engellenmiş bağlantı isteği hacmine ve kimlik avı sitesi başına en yüksek engellenmiş bağlantı isteği oranına maruz kaldı. Finansal kurumlar, site başına en düşük engellenmiş bağlantı isteği alırken toplamda en yüksek hacimli farklı dolandırıcılık sitelerine engellenmiş bağlantı isteği aldı. Aşağıdaki şekilde, en çok hedef alınan kurum türlerinden her biri için Microsoft tarafından 2H09 döneminin her ayında kaydedilen engellenmiş bağlantı isteği yüzdesi gösterilmektedir.

Şekil 13: Sol: 2H09'un her ayında her türde kimlik avı sitesi için engellenmiş bağlantı isteği Sağ: 2H09'da hedef türüne göre her ay izlenen aktif kimlik avı siteleri



Şekil 14: 1H09 ve 2H09 dönemlerinde SmartScreen Filtresi tarafından engellenmiş URL'lerde barındırılan tehditlerin kategorilere göre dökümü



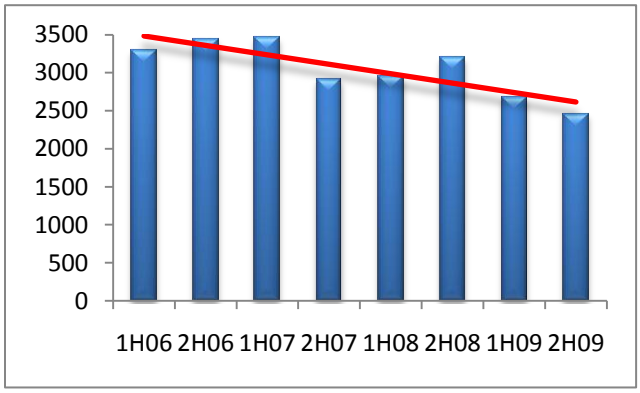
- Çeşitli Olası İstenmeyen E-posta Yazılımı ve Çeşitli Truva Atları kategorilerinin her iki dönemde de listeye hakim olduğu görülüyor.
- 1H09'da neredeyse Çeşitli Truva Atları kategorisi kadar yaygın olan Truva Atı Yükleyicileri ve Dosya Yükleyiciler kategorisi yılın ikinci yarısında yaklaşık yüzde 50 düşüş yaşarken Açıklardan Yararlanmalar kategorisi yüzdesini iki katının üstüne çıkardı.

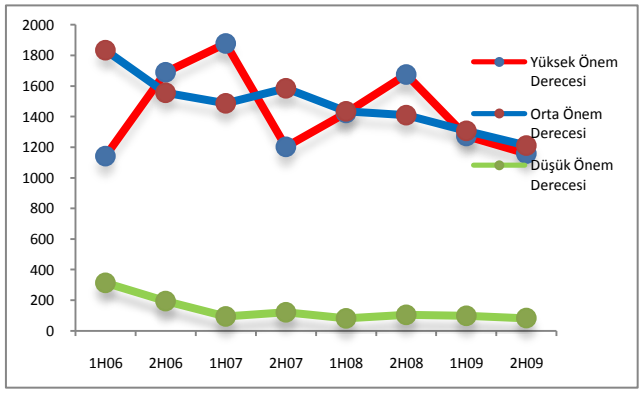
Microsoft Güvenlik Yanıt Merkezi'nden Önemli Bulgular

Sektör Genelindeki Güvenlik Açığı Açıklamaları

Güvenlik açıkları, yazılımlarda bulunan ve bir saldırganın yazılım bütünlüğünü, kullanılabilirliğini veya gizliliğini tehlike altına sokmasına izin veren zayıf noktalardır. En kötü güvenlik açıklarından bazıları, saldırganların tehlike altındaki bilgisayar üzerinde isteğe bağlı kodlar çalıştırmasına izin verir. Bu raporda kullanılan açıklama terimi, bir yazılım güvenliği açığının kamuoyuna duyurulmasıdır. Gizli bir açıklama veya sınırlı sayıda kişiye açıklama anlamına gelmez.

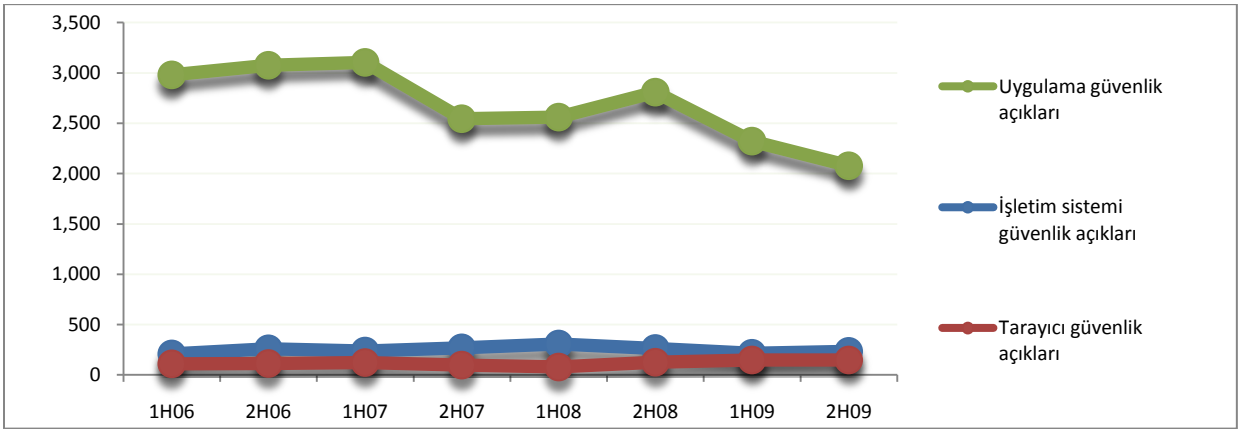
Şekil 15: Sol: Yarı yıl bazında sektör genelindeki güvenlik açığı açıklamaları, 1H06–2H09 | Sağ: Önem derecesine göre sektör genelindeki güvenlik açığı açıklamaları, 1H06–2H09





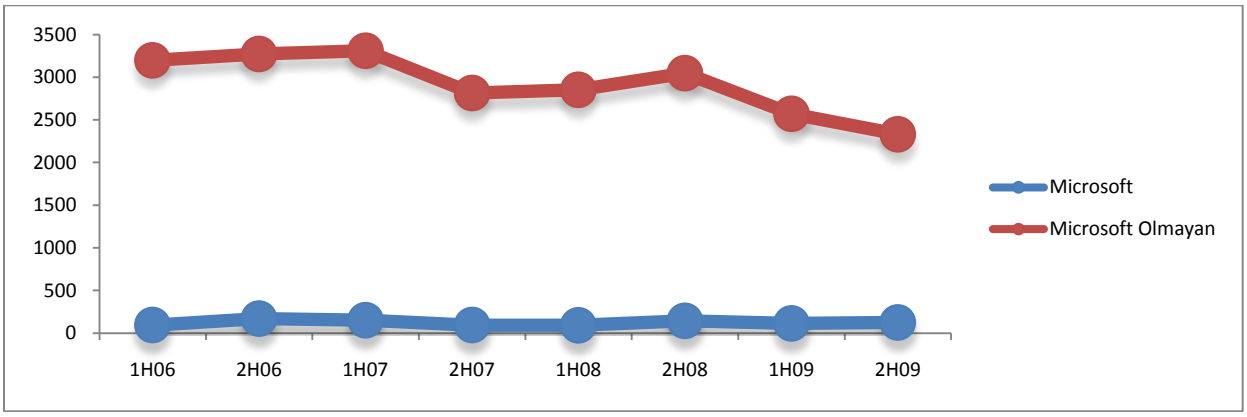
- 2H09'da güvenlik açığı açıklamaları, 2006'dan beri süregelen genel orta derecede düşüş eğilimini sürdürerek yılın ilk yarısına göre yüzde 8,4 düşüş gösterdi.
- Düşük önem dereceli güvenlik açıkları yılın ilk yarısında görülen yüzde 4,1'in altına inerek 2H09'da tüm güvenlik açıklarının yüzde 3,5'ini oluşturdu.
- 2H09'da açıklanan yüksek önem dereceli güvenlik açıkları yılın ilk yarısına göre yüzde 9,0 ve 2H08 dönemine göre yüzde 30,7 düşüş gösterdi.
    - Yüksek önem dereceli ve Orta önem dereceli güvenlik açığı açıklamalarının ağırlığını hissettirmeye devam etmesi kısmen de olsa hem saldırganların hem de yasal güvenlik araştırmacılarının en önemli güvenlik açıklarına öncelik vermesinden kaynaklanıyor.

Şekil 16: Sektör genelindeki işletim sistemi, tarayıcı ve uygulama güvenliği açıkları, 1H06–2H09



- Toplam uygulama güvenliği açığı sayısının 2H08 ile 1H09 arasında önemli ölçüde düşüş göstermesine rağmen uygulama güvenlik açıkları 2H09 döneminde en yüksek sayıdaki güvenlik açığı kategorisi olmayı sürdürdü.
- İşletim sistemi ve tarayıcı güvenlik açığı hemen hemen aynı kaldı ve her biri toplam sayının küçük bir kısmını oluşturdu.

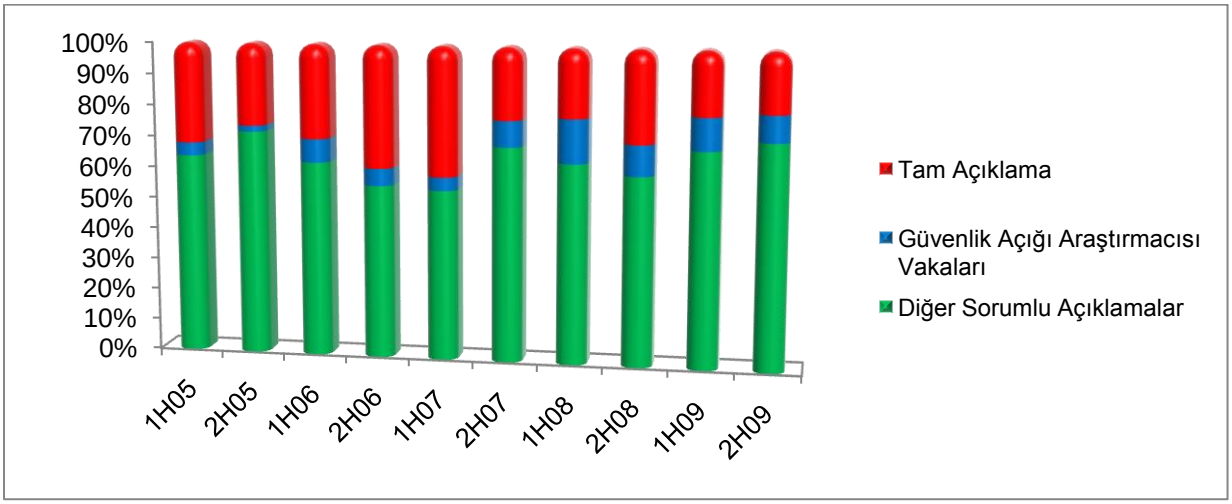
Şekil 17: Microsoft ürünleri ve Microsoft harici ürünler için güvenlik açığı açıklamaları, 1H06–2H09



- Microsoft ürünleri için güvenlik açığı açıklamalarının sayısı 1H09'da 113'ken 2H09'da 127 olarak gerçekleşti.
- Genellikle, 2H06-1H07 ve tekrar 2H08 döneminde zirve yapan Microsoft güvenlik açığı açıklamalarının eğilimi sektörün genelindeki eğilimi yansıtıyor.
- Son dört yılda, Microsoft güvenlik açığı açıklamaları sektör genelindeki tüm açıklamaların yüzde 3 ile 5'i arasında istikrarlı bir seyir çizdi.

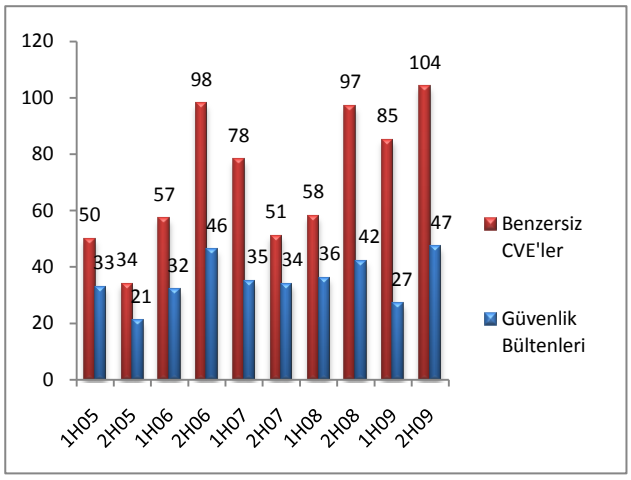
Sorumlu açıklama, ayrıntılar kamuoyunca öğrenilmeden önce güvenlik açıklarını giderebilecek kapsamlı bir güvenlik güncellemesi geliştirmesi için güvenlik açıklarını gizli bir şekilde yalnızca etkilenen satıcıya açıklamak anlamına gelir.

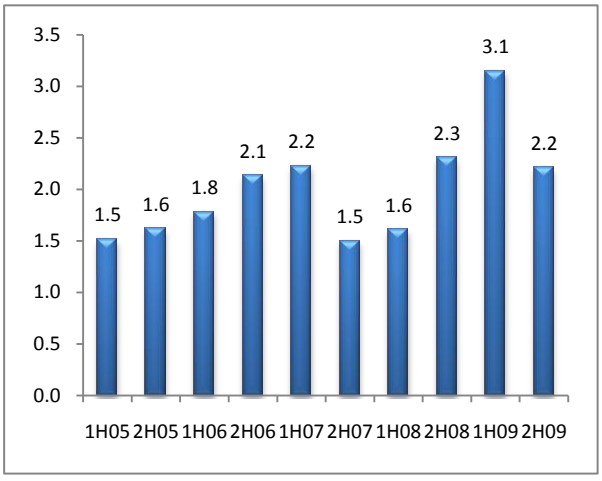
Şekil 18: Microsoft yazılımlarıyla ilgili sorumlu açıklamaların tüm açıklamalar içindeki yüzdesi, 1H05–2H09



- 2H09 döneminde Microsoft güvenlik açığı açıklamalarının yüzde 80,7'si sorumlu açıklama uygulamalarına uygun şekilde gerçekleştirildi, bu rakamla 1H09'daki yüzde 79,5'lik değerin üzerine çıkıldı ve önceki izlenen tüm dönemlerden daha yüksek bir oran elde edildi.
- Güvenlik açığı araştırmacıları tarafından sunulan açıklama yüzdeleri, yılın ilk yarısında görülen yüzde 10,5'e kıyasla 2H09'da küçük bir düşüşle yüzde 8,6'ya geriledi.

Şekil 19: Sol: Yarı yıl bazında Microsoft tarafından yayınlanan güvenlik bültenleri ve ele alınan CVE'ler, 1H05–2H09 | Sağ: Güvenlik bülteni başına ele alınan ortalama CVE sayısı, 1H05–2H09

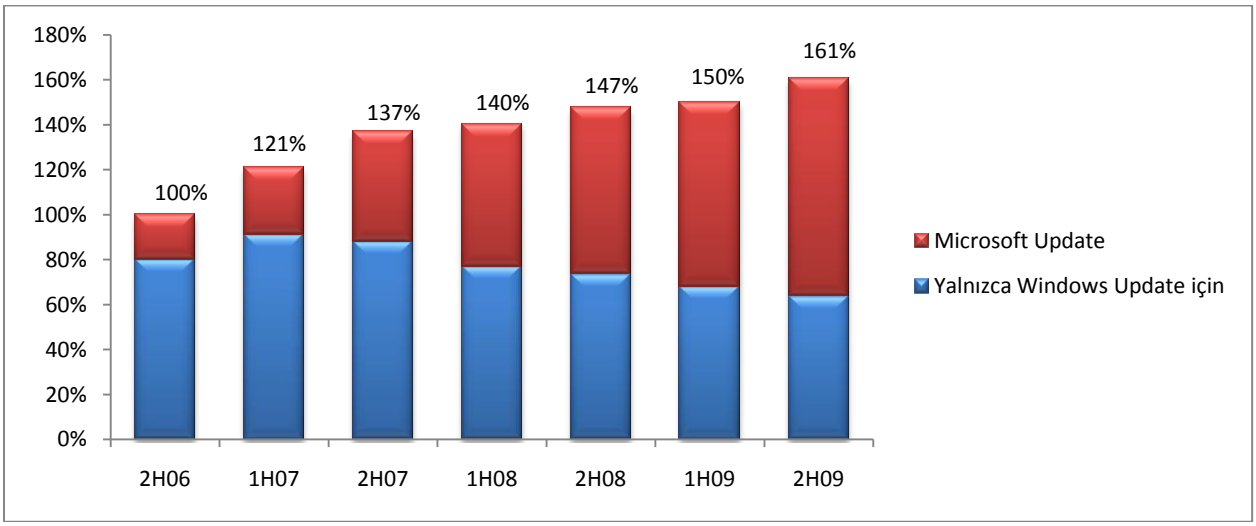




- Microsoft 2H09'da Genel Güvenlik Açıkları ve Zaafları (CVE) listesinde belirlenmiş 104 ayrı güvenlik açığını ele alan 47 güvenlik bülteni yayınladı.
- 1H09'da 27 olan yayınlanan toplam bülten sayısının artmasına rağmen, bülten başına ele alınan güvenlik açığı sayısı 3,1'den 2,2'ye düştü.

Aşağıdaki şekilde görüldüğü üzere, Microsoft Update kullanımı son birkaç yılda önemli ölçüde artış gösterdi. Kapsamlı hizmeti kullanan bilgisayar sayısı 1H09'dan beri yüzde 17'den fazla arttı.

Şekil 20: Windows Update ve Microsoft Update kullanımı, 2H06–2H09, 2H06 toplam kullanımına endekslenmiştir



- **Windows Update**, Windows bileşenleri ile Microsoft ve diğer donanım satıcıları tarafından tedarik edilen aygıt sürücüleri için güncellemeler sağlamaktadır. Windows Update aynı zamanda Microsoft kötü amaçlı yazılımdan koruma ürünleri için imza güncellemeleri ve MSRT'nin aylık sürümünü dağıtmaktadır.
- **Microsoft Update** (http://update.microsoft.com/microsoftupdate), Windows Update yoluyla sunulan tüm güncellemelerle birlikte diğer Microsoft yazılımları için de güncellemeler sağlar. Kullanıcılar, yazılım güncellemelerini Microsoft Update yoluyla almayı veya Microsoft Update Web sitesinden yüklemeyi seçebilir. Microsoft, kullanıcıların Microsoft ürünlerinin güvenlik güncellemelerini zamanında alabilmeleri için bilgisayarlarını Windows Update yerine Microsoft Update hizmetini kullanacak şekilde yapılandırmasını önerir.

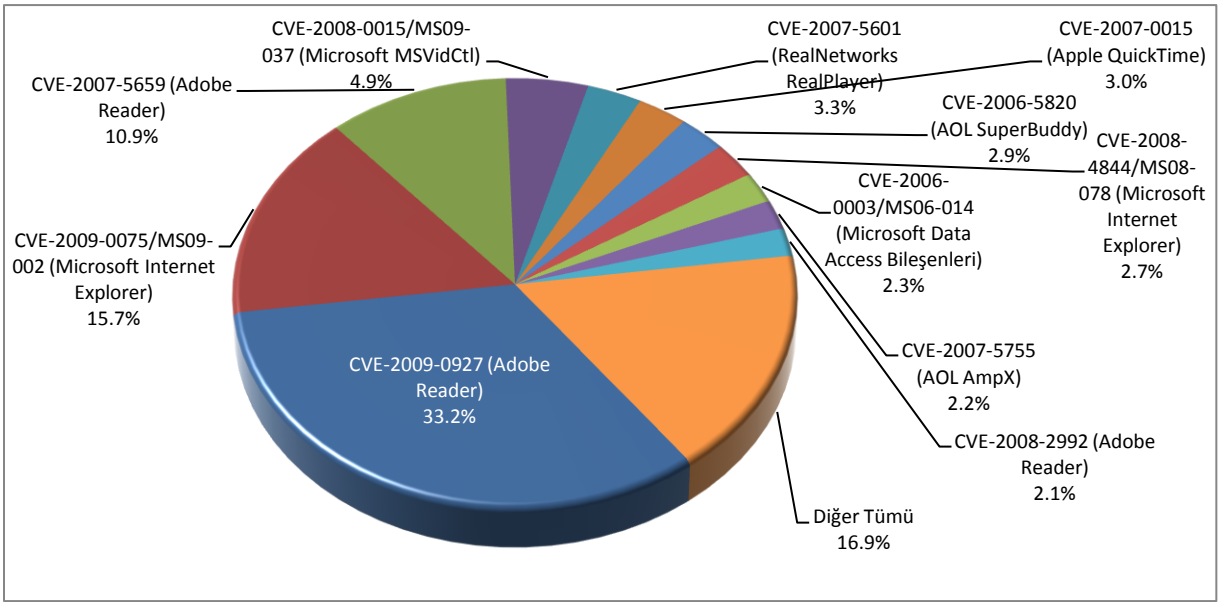
Microsoft Güvenlik Mühendislik Merkezi'nden Önemli Bulgular

Güvenlik Bilimi: Açıklardan Yararlanma Eğilimleri

Kullanıcının onayı ve genellikle bilgisi olmaksızın bir bilgisayara bulaşmak üzere tasarlanmış kötü amaçlı kodlara *açıklardan yararlanma* adı verilir. Açıklardan yararlanan kodlar genellikle Web sayfaları üzerinden dağıtılır; fakat saldırganlar e-posta ve anlık mesajlaşma (IM) hizmetleri gibi birçok farklı dağıtım yöntemini de kullanmaktadır. Saldırganların tarayıcıları ve eklentileri nasıl sömüreceği hakkında bilgi sahibi olunması, güvenlik araştırmacılarının kaçak karşıdan yükleme ve diğer tarayıcı tabanlı saldırıların neden olduğu riskleri daha iyi anlamasını sağlayacaktır.

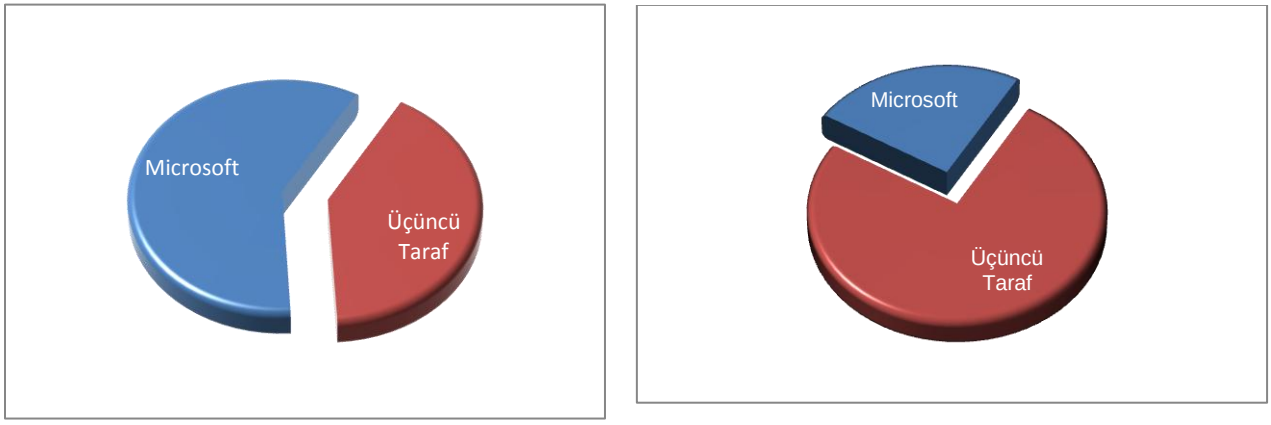
- Geçmişte, açıklardan yararlanma kiti yazarları kit başına dört ile altı kod yerleştirme eğilimi göstererek saldırının başarı olasılığını artırmaya çalışıyordu.
  - Bu ortalama, saldırganların çok sayıda kodu gereksiz kılan üçüncü taraf bileşenlerindeki birkaç yaygın güvenlik açığından yararlanmalarıyla birlikte 2009'un ilk yarısında paket başına 3,2 açıklardan yararlanan koda düştü.
  - Bu eğilim 2H09 döneminde de devam etti; paket başına açıklardan yararlanan kod sayısı 2,3'e düştü.
  - Ancak, bazı saldırganlar hala çok sayıda açıklardan yararlanan kod kullanmayı tercih ediyor, 2H09'da gözlemlenen en büyük açıklardan yararlanma kiti 23 kod içeriyordu.

Şekil 21: Yüzde bazında 2H09'da karşılaşılan tarayıcı tabanlı açıklardan yararlanan kodlar



- 1H09'da en yaygın şekilde istismar edilen tarayıcı güvenlik açığı olan Adobe Flash Player'ın kaçak karşıdan yükleme güvenlik açığı CVE-2007-0071, yılın ikinci yarısında yirmi üçüncü sıraya geriledi ve açıklardan yararlanmanın yalnızca yüzde 0,4'lük bir bölümünü oluşturdu.
  - Bu gibi önemli değişiklikler açıklardan yararlanma kiti yazarlarının eski kodları sık sık yenileriyle değiştirme eğilimlerinden kaynaklanıyor olabilir.
  - Şekil 21'de sağdaki grafikle gösterildiği üzere, çoğu yaygın açıklardan yararlanmanın ortaya çıkışı 2H09'da aydan aya önemli değişiklikler gösterdi.
- Şekil 21'de listelen güvenlik açıklarından biri için 2006'da bir yama paketi geliştirildi.
- Şekil 21'deki tüm güvenlik açıkları için GİR raporlama döneminden önce güvenlik güncellemeleri geliştirildi.

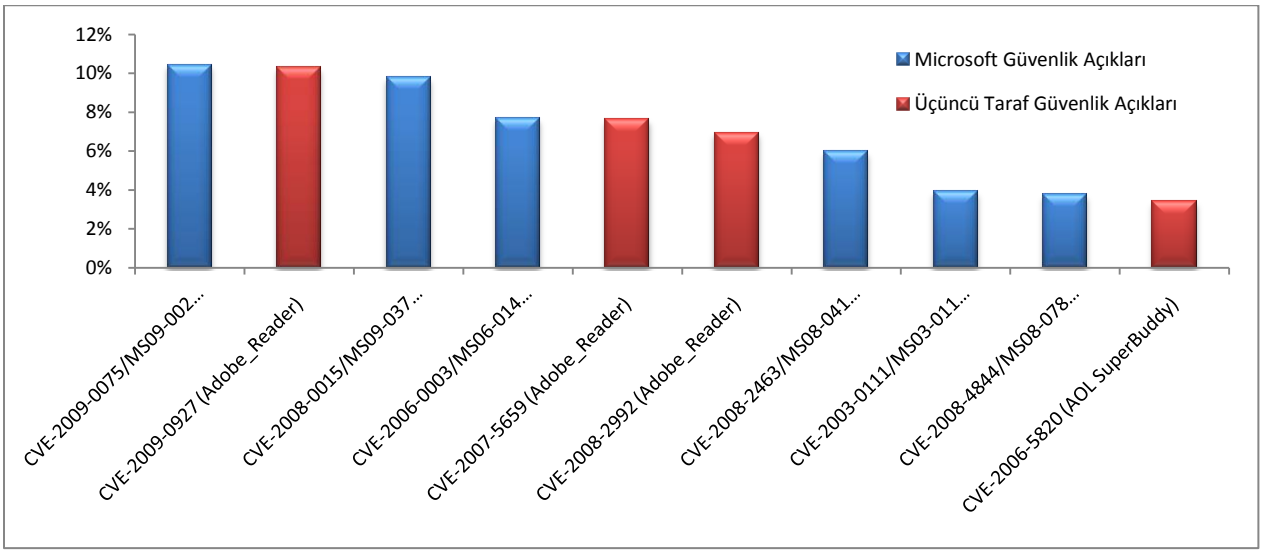
Şekil 22: Sol: 2H09'da Microsoft yazılımlarını ve Windows Xp tabanlı bilgisayarlardaki üçüncü taraf yazılımlarını hedef alan tarayıcı tabanlı açıklardan yaralanmalar | Sağ: 2H09'da Microsoft yazılımlarını ve Windows Vista ve Windows 7 tabanlı bilgisayarlardaki üçüncü taraf yazılımlarını hedef alan tarayıcı tabanlı açıklardan yararlanmalar



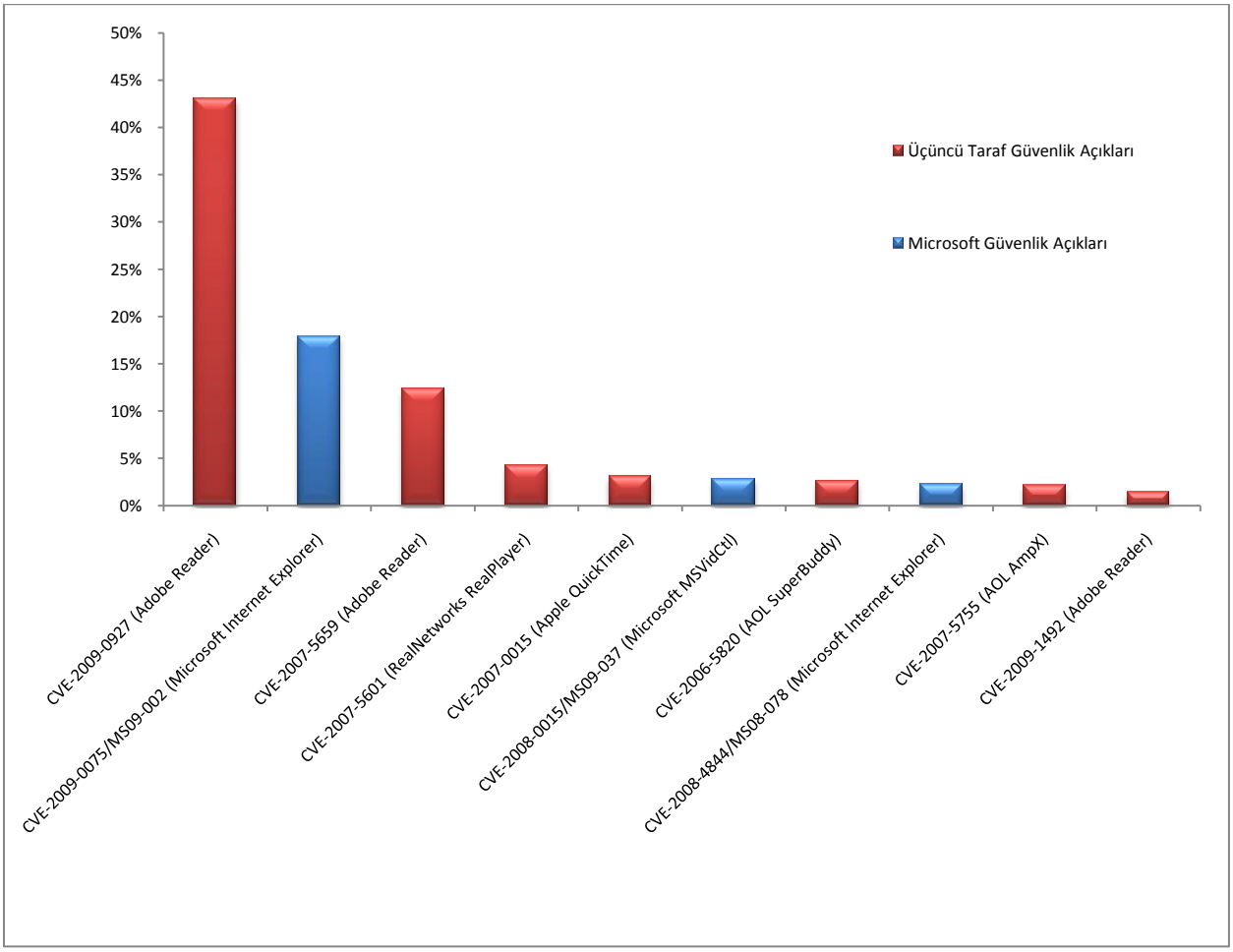
- Microsoft yazılımlarını hedef alan açıklardan yararlanmalarla üçüncü taraf açıklardan yararlanmaların (diğer satıcılar tarafından geliştirilmiş yazılımlardaki güvenlik açıklarını hedef alan açıklardan yararlanmalar) karşılaştırılması, Windows Vista ve Windows 7'de Windows XP'den çok farklı bir güvenlik açığı dağılımının olduğu görülüyor.
  - Windows XP'de, Microsoft güvenlik açıkları araştırılan örnekteki tüm saldırıların yüzde 55,3'üne karşılık geliyor.
  - Windows Vista ve Windows 7'de, Microsoft güvenlik açıklarının oranı önemli ölçüde daha düşük gerçekleşerek araştırılan örnekteki saldırıların yalnızca yüzde 24,6'sına karşılık geliyor.
    - Bu rakamın 1H09'daki yüzde 15,5'lik (yalnızca Windows Vista için) değere göre artış göstermesinin nedenleri CVE-2009-0075/MS09-002 üzerindeki saldırıların artması, Internet Explorer 7'daki Windows Vista RTM'yi ve SP1'i etkileyen (Windows Vista SP2 veya Windows 7 etkilenmemektedir) bir güvenlik açığıdır. Bu sorun, Microsoft güvenlik güncellemesi tarafından Ocak 2009'da ele alındı.

Bir sonraki sayfada bulunan Şekil 23 ve Şekil 24'te, Windows XP (Şekil 23) ile Windows Vista ve Windows 7'de (Şekil 24) en çok faydalanılan 10 güvenlik açığı gösterilmektedir.

Şekil 23: Windows XP'de en çok faydalanılan 10 tarayıcı tabanlı güvenlik açığı, tüm açıklardan yararlanmalar içindeki yüzdeleriyle, 2H09



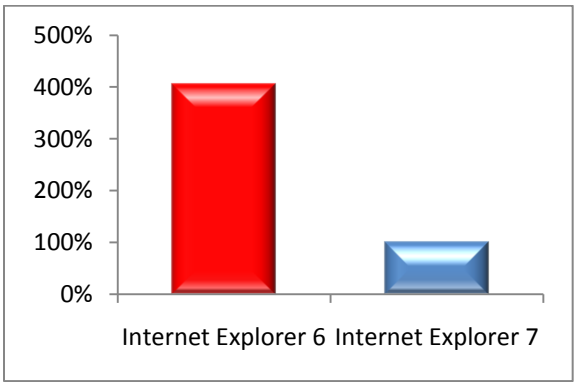
Şekil 24: Windows Vista ve Windows 7'de en çok faydalanılan 10 tarayıcı tabanlı güvenlik açığı, tüm açıklardan yararlanmalar içindeki yüzdeleriyle, 2H09



Kaçak karşıdan yükleme sayfaları genellikle bir saldırganın açıklardan yararlanan kodları gönderdiği yasal Web sitelerinde barındırılır. Saldırganlar izinsiz erişim yoluyla veya bir blogdaki yorum alanları gibi güvenliği zayıf bir Web formuna kötü amaçlı kodlar göndererek yasal sitelere erişebilir.

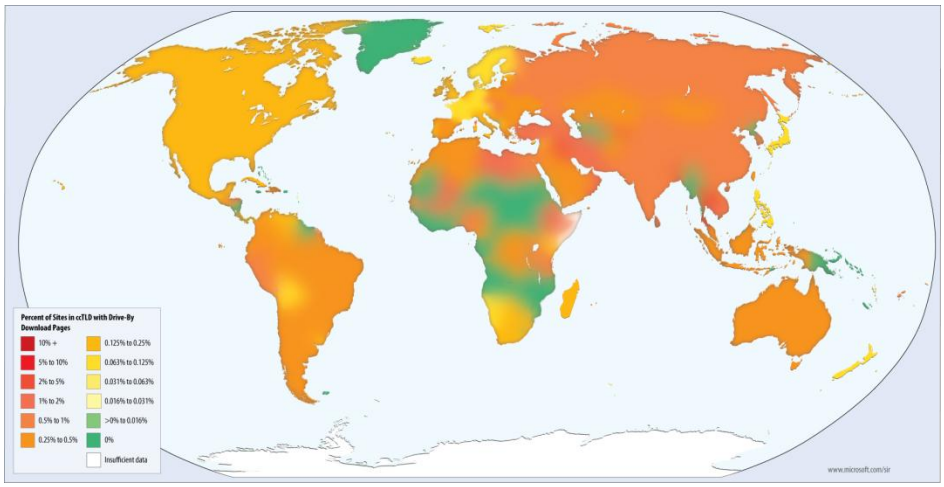
- Kaçak karşıdan yükleme sitelerinin hedef aldığı belirli güvenlik açıkları analiz edildiğinde, bu gibi kötü amaçlı siteler tarafından en çok kullanılan açıklardan yararlanmanın eski tarayıcıları hedef aldığı ve yeni tarayıcılarda etkisiz olduğu görülmektedir. Aşağıdaki şekilde gösterildiği üzere, 2H09'da Internet Explorer 6'yı etkileyen açıklardan yararlanan kodlar, daha yeni olan Internet Explorer 7'yi etkileyen açıklardan yararlanan kodlara göre kaçak karşıdan yükleme sitelerinde dört kat daha fazla görüldü.

Şekil 25: Internet Explorer 6'yı ve Internet Explorer 7'yi hedef alan kaçak karşıdan yükleme siteleri, Internet Explorer 7'nin toplam değerine endekslenmiştir, 2H09



- Bing Web sayfalarını endekslerken, sayfalar kötü amaçlı öğe veya kötü amaçlı davranışlara karşı değerlendirilir.
  - Bing, aktif kaçak karşıdan yükleme sayfalarını barındıran ve her an izlenen birkaç yüz bin sitede her ay çok sayıda kaçak karşıdan yükleme sayfası saptamaktadır.
  - Genellikle tehdit altındaki sitelerin sahipleri kurban olduğu için, siteler Bing endeksinden çıkarılmamaktadır. Bunun yerine, arama sonuçları listesinde bağlantı tıklandığında sayfanın kötü amaçlı yazılım içerebileceği uyarısı görüntülenir.
    - 2H09'da, Bing tarafından kullanıcılara sunulan arama sonuçları sayfalarının yaklaşık yüzde 0,3'ü kötü amaçlı siteler konusunda uyarılar içeriyordu.
  - Toplamda, Bing tarafından takip edilen etkilenmiş Web sitesi sayısı 1H09'da yüzde 0,16 iken, 2H09'da artış göstererek tüm Web sitelerinin yüzde 0,24'ünün en az bir kötü amaçlı sayfa barındırdığını ortaya koydu. Bu artış, Bing'in 2009'un ikinci yarısında uygulamaya koyduğu birçok yeni, gelişmiş saptama mekanizmalarından kaynaklanıyor olabilir.
- Bing'in tüm dünya genelinde kaçak karşıdan yükleme sitelerini saptamasına rağmen, söz konusu risk dünya genelindeki Internet kullanıcıları arasında eşit bir şekilde yayılmamıştır. Dünyanın bazı kesimlerindeki kullanıcılar diğerlerine göre daha yüksek risk altındadır. Aşağıdaki şekilde, 2H09'da kaçak karşıdan yükleme sayfası barındırdığı tespit edilen her bir ülke kodlu üst düzey etki alanındaki (ccTLD) Web sitelerinin oranı gösterilmektedir.
  - .th ccTLD (Tayland) etki alanındaki sitelerin yüzde 2,1'inde ve .cn ccTLD (Çin) etki alanındaki sitelerin yaklaşık yüzde 1'inde kaçak karşıdan yükleme sayfaları bulundu.

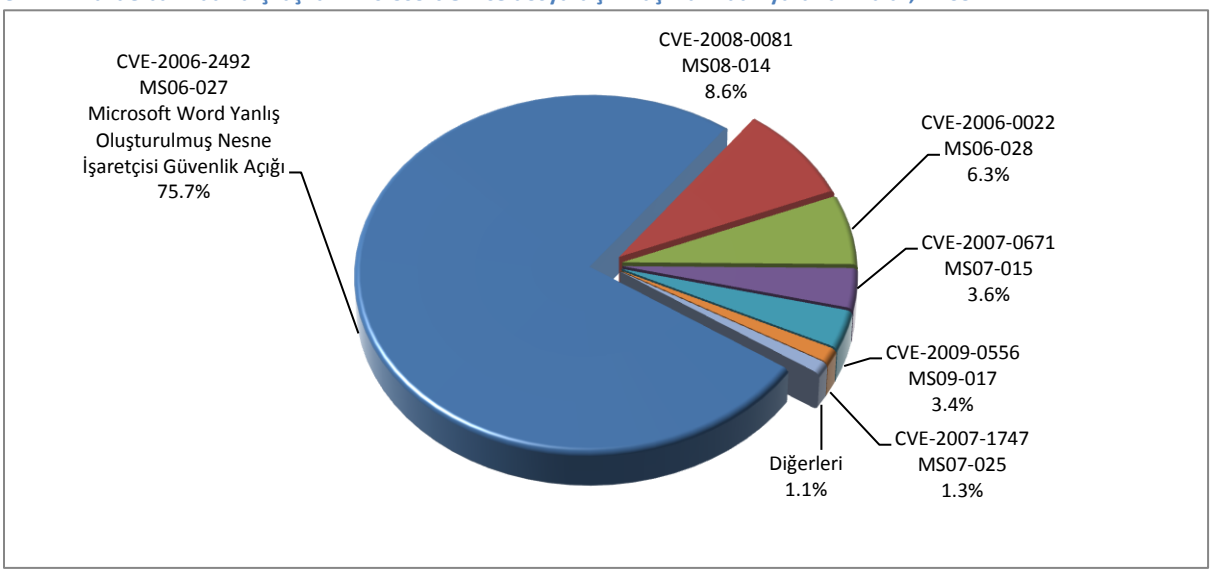
Şekil26: [BingGeo_Heatmap] 2H09'da her bir ülke kodlu üst düzey etki alanında (ccTLD) kaçak karşıdan yükleme sayfaları barındıran Web sitelerinin yüzdesi



- Karşılaştırma yapıldığında, belirli ülke/bölgelere hizmet vermeyen genel etki alanları ve sponsorlara sahip üst düzey etki alanları ccTLD etki alanlarıyla aynı düzeyde değişkenlik göstermiyor.
    - İşletmelere yönelik tasarlanmış .biz TLD etki alanı, kaçak karşıdan yükleme sayfası barındıran en yüksek site yüzdesine sahip; aktif tüm .biz sitelerinin yüzde 0,76'sının bu gibi sayfalar içerdiği tespit edildi.
- Birçok genel, sponsorlu ve ülke kodlu TLD'lerde kaçak karşıdan yükleme sayfalarının bulunmasına rağmen, açıklardan yararlanma sunucuları başta .com (yüzde 33,2) ve .cn (yüzde 19,0) etki alanları olmak üzere çok daha az sayıda TLD üzerinde yoğunlaşmaktadır.
    - 2H08'de, dünya genelinde en çok kullanılan açıklardan yararlanma sunucusu yaklaşık 100.000 sayfaya ulaşıyordu. Bu rakam, 1H09'da 450.000 sayfaya ve 2H09'da yaklaşık 750.000 sayfaya yükseldi.
        - Bu artışa rağmen, 1H09'da listenin üst sıralarında yer alan çok az sayıda sunucu 2H09'da yerini koruyabildi.
- Kötü amaçlı yazılım dağıtım ağlarının, sürekli farklı konumlarda görünen ve ortadan kaybolan sunucularla bir hedef değiştirme eğiliminde olduğu belirlendi.

Saldırganlar, açıklardan yararlanma için iletim vektörü olarak gün geçtikçe daha fazla yaygın dosya biçimlerini kullanıyor (örneğin .doc, .pdf, .ppt ve .xls biçimleri). *Ayrıştırıcı güvenlik açıkları*, saldırganın kodun dosya biçimini işleme veya ayrıştırma yöntemindeki bir hatadan yararlanan özel olarak geliştirilmiş belgeler oluşturduğu bir güvenlik açığı türüdür. Bu biçimlerden birçoğu karmaşık niteliktedir ve performans için tasarlanmıştır, saldırgan programdaki bir güvenlik açığından faydalanan yanlış oluşturulmuş bir bölüme sahip dosyalar oluşturabilir.

Şekil 27: Yüzde bazında karşılaşılan Microsoft Office dosya biçimi açıklarından yararlanmalar, 2H09



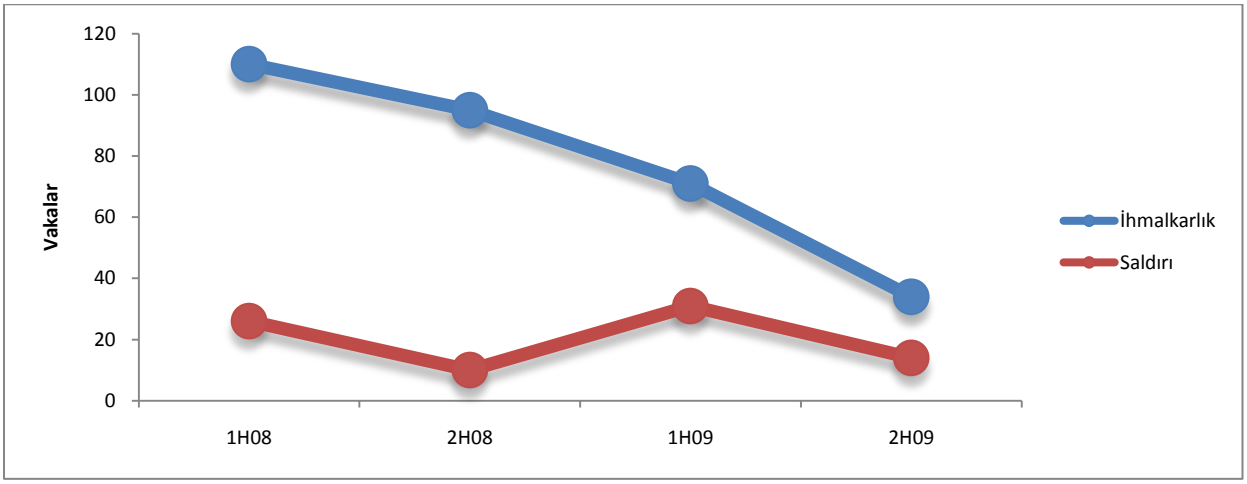
- Veri örneğinde faydalanılan güvenlik açıklarının çoğu birkaç yıl kadar eskidir ve bunların tümü açıklardan yararlanmaya karşı koruma sağlayan güvenlik güncellemelerine sahiptir; bunların üçte biri ilk kez 2006'da belirlendi.
- Saldırıların yüzde 75,7'si, 2009'un sonuna gelindiğinde üç yıldan fazla bir süredir güvenlik düzeltmesi sunulmakta olan tek bir güvenlik açığından (CVE-2006-2492, Microsoft Office Word'deki Yanlış Oluşturulmuş Nesne İşaretçisi Güvenlik Açığı) yararlanıyordu.
- Office program yüklemelerini hizmet paketleri ve güvenlik güncellemeleriyle güncellemeyen kullanıcılar daha yüksek saldırı riskiyle karşı karşıyadır. Saldırıların çoğu son derece eski Office program yüklemelerini hedef aldı.
    - Saldırıların çoğu (yüzde 56,2'si), 2003'ten beri güncellenmemiş Office program yüklemelerini etkiledi.
    - Bu saldırıların çoğu, Office 2003'ün Ekim 2003'te piyasaya sürülmesinden beri tek bir hizmet paketi yüklememiş veya hiçbir güvenlik güncelleştirmesi yapmamış Office 2003 kullanıcılarını vurdu.
    - Office programı açıklardan yararlanma saldırıları kurbanlarının çok daha güncel Windows yüklemeleri olması nadir görülen bir durum değil. 2H09'da gözlemlenen Office saldırılarının yaklaşık üçte ikisi (yüzde 62,7'si), Windows'un son 12 ayda güncellenmiş sürümlerinin kullanıldığı bilgisayarları etkiledi.
    - Örnekteki bilgisayarların son işletim sistemi güncellemesinden beri geçen ortalama süre yaklaşık 8,5 aydır ve en son Office programı güncellemesine kadar geçen 6,1 yıllık süre ise bundan neredeyse dokuz kat daha uzundur.
        - Bu veriler, kullanıcıların Windows'u büyük bir gayretle güncel tutmasına rağmen diğer programları da düzenli olarak güncellemedikleri sürece açıklardan yararlanma riski taşıyacaklarını gösteriyor.

Güvenlik İhlali Eğilimleri

Gizlilik Sonuçları Doğuran Güvenlik Olayları

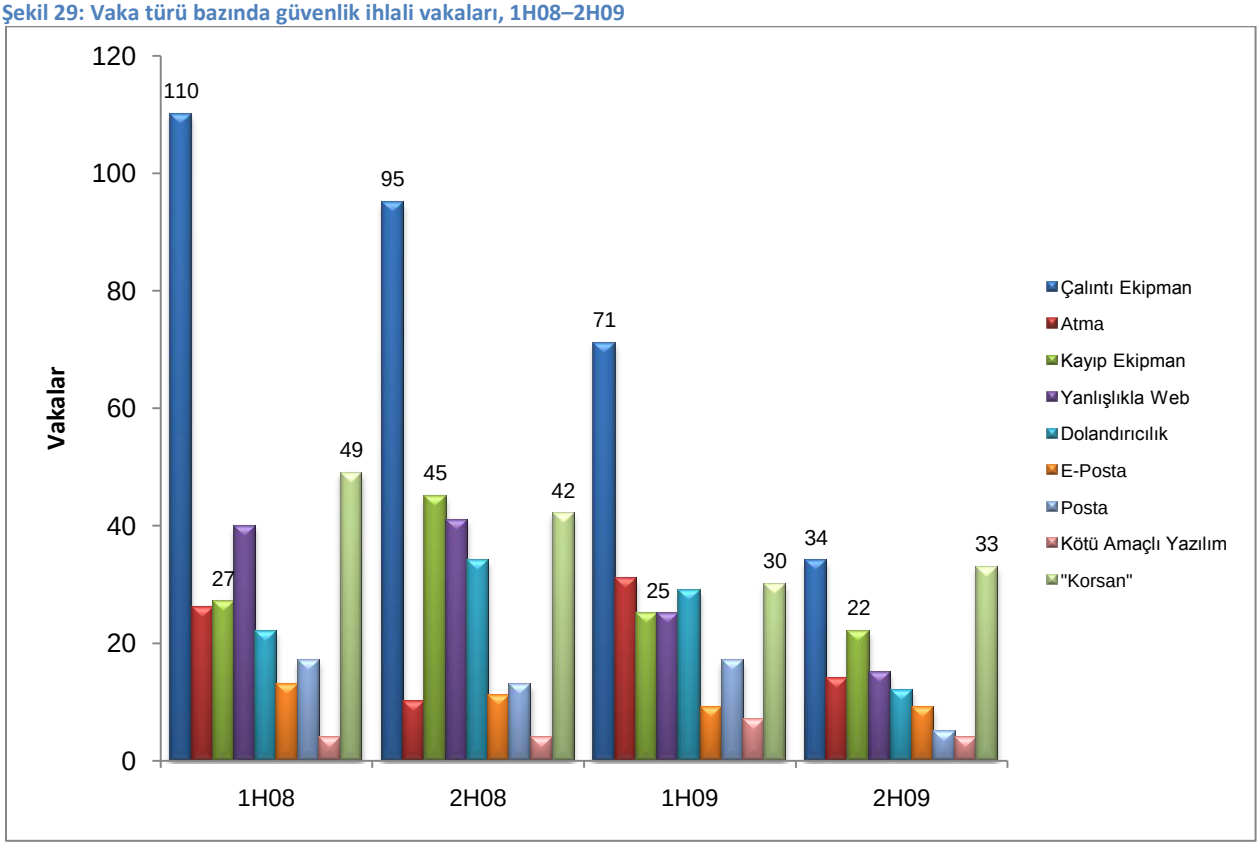
Son birkaç yılda, dünya genelindeki pek çok yasama organı tarafından bir şirketin kendisine emanet edilen kişisel tanımlama bilgilerinin (PII) kontrolünü kaybettiğinde etkilenen bireyleri bilgilendirmesini zorunlu kılan yasalar yürürlüğe kondu Son birkaç yılda, dünya genelindeki pek çok yasama organı tarafından bir şirketin kendisine emanet edilen kişisel tanımlama bilgilerinin (PII) kontrolünü kaybettiğinde etkilenen bireyleri bilgilendirmesini zorunlu kılan yasalar yürürlüğe kondu. Bu zorunlu bildirimler, bilgi güvenliği çalışmalarında ihmal ve teknoloji gibi konuların nasıl ele alınması gerektiği yönünde benzersiz bir kavrayış sağlıyor[4].

Şekil 28: Saldırı ve ihmalden kaynaklanan ihlal vakaları, 1H08–2H09



[4] 2005'ten beri, gönüllü güvenlik araştırmacıları dünya genelinde bu gibi veri güvenliği ihlallerini takip etti ve bunları http://datalossdb.org adresindeki Veri Kaybı Veritabanına (DataLossDB) kaydetti.

Şekil 29: Vaka türü bazında güvenlik ihlali vakaları, 1H08–2H09



- Sabit kalan kötü amaçlı yazılım saldırıları kategorisinin dışında hemen her kategorideki mutlak vaka sayısında açık bir düşüş eğilimi bulunmaktadır.
- En büyük düşüş, çalıntı ekipman ve ortamlar ile yanlışlıkla meydana gelen Web kayıpları kategorilerinde yaşandı.
- Birçok vaka, iş kayıtlarının yanlış bir şekilde atılmasından kaynaklanıyor. Kuruluşlar bu tür veri ihlallerini, hassas bilgiler içeren kağıtların ve elektronik kayıtların yok edilmesine ilişkin etkili politikalar izleyerek kolaylıkla çözebilir.
- Pek çok kişinin güvenlik ihlallerini hassas verilere yasa dışı yollarla erişmeye çalışan kötü amaçlı taraflarla ilişkilendirmesine rağmen, saldırı vakaları (korsanlık, kötü amaçlı yazılım ve dolandırıcılık) son yıllarda ihmalkarlık vakalarının (kayıp, çalıntı veya bulunamayan ekipman, yanlışlıkla açıklama veya yanlış bir şekilde atma) önemli ölçüde gerisinde kaldı.
- İhmalkarlıktan kaynaklanan vakalar, 1H08'de 110 iken 2H09'da 34'e inerek son iki yılda sert bir düşüş gösterdi.
    - Kuruluşlar, hassas ekipmanların güvenliğini sağlamak için tesis kapılarında güvenlik kontrolleri gerçekleştirme veya çalışanları güvenli uygulamalar konusunda eğitecek programlar düzenleme gibi daha fazla adım atabilir.
    - Windows BitLocker® Sürücü Şifrelemesi gibi güçlü şifreleme çözümlerinin kullanılması da düşüşü etkilemiş olabilir. Birçok yargı yetki alanında açıklama yasaları, şifrelenmiş veriler kaybolduğunda veya çalındığında hırsızın veya bulan kişinin verileri çıkarması çok daha zor olacağı için bildirimde bulunulmasını gerektirmiyor.

Korunma Stratejileri

Microsoft BT Bölümünün Microsoft'ta Uyguladığı Risk Yönetimi

Microsoft BT bölümü, günlük işlemlerden ve Microsoft küresel ağının güvenliğinden sorumludur. Bu yeni GİR bölümünde, Microsoft BT bu son derece karmaşık ortamda risk yönetimi için kullandıkları belirli hafifletme stratejilerini paylaşıyor, BT ve güvenlik uzmanlarının kendi ortamlarını güvende tutmalarına yardımcı olacak yol gösterici pratik bilgiler sağlıyor. Bir kuruluşun ağ altyapısının nasıl korunabileceği ve kuruluş genelinde bilincin artırılması ve güvenli bilgi işlem uygulamalarının teşvik edilmesi için neler yapılabileceği gibi konular ele alınıyor.

Microsoft aynı zamanda Microsoft ürünleri için güvenlik güncellemelerini değerlendirme, öncelik atama ve dağıtma sürecinde BT uzmanlarına yardımcı olacak kapsamlı yol gösterici bilgiler sunmaktadır. Microsoft Güvenlik Güncellemesi Kılavuzu www.microsoft.com/securityupdateguide adresinden ücretsiz olarak yüklenebilir.

Tam *GİR*, kuruluşların *GİR* içinde belirtilen birçok güvenlik riskini hafifletmesine yardımcı olabilecek hafifletme stratejilerini ve en iyi uygulama bilgilerini içermektedir.

Tam *GİR* www.microsoft.com/sir adresinden yüklenebilir.

Microsoft'un İstihbarat Raporunu geliştirmesine yardımcı olun

Microsoft İstihbarat Raporu'nun en son sayısını okumaya vakit ayırdığınız için teşekkür ederiz. Bu raporun müşterilerimiz için mümkün olduğunca faydalı ve yol gösterici olmasını sağlamak istiyoruz. Bu raporun herhangi bir sayısı hakkında bir geri bildirimde bulunmak isterseniz veya gelecekteki sayıları nasıl geliştirebileceğimize ilişkin önerileriniz varsa, lütfen e-posta yoluyla sirfb@microsoft.com adresinden bize ulaşın.

Teşekkürler, saygılarımızla,

Microsoft Güvenli Bilişim