Adli Bilişim Vakası Öncesinde Ağa Yapılan Saldırı ve Anormallik Tespiti: Bir Olay İncelemesi

F. Ertam[1] ve İ. Kılıç[2]

[1]Fırat University, Elazig/Turkey, fatih.ertam@firat.edu.tr
[2]Fırat University, Elazig/Turkey, irfankilic@firat.edu.tr

***Özet*— Kanunsuz bir girişimin adli bilişim suçu olup olmadığının araştırılabilmesi için bu suç girişiminin öncelikle hukuksal boyuta dayandırılması gerekmektedir. Sanallaştırma yapılan sistemlerde, sanal makinelerin kurulması, yapılandırmasının yapılması ve kontrol edilmesi fiziksel makinelere göre daha kolay olmaktadır. Bu çalışmada Fırat Üniversitesi sunucu bilgisayarlarından olan sanal bir makine üzerinde kurulu olup, çalışan ve çalıştığı ağın trafiğini yavaşlatarak istenilmeyen sitelere bağlantı yapan kötücül bir yazılımın tespit edilerek engellenmesi için yapılan bir çalışmanın adli bilişim vakası olmadan önceki durumu incelenecektir. Çalışma adli bilişimin bir alt dalı olarak kabul edilebilecek olan ağ adli bilişimi ile ilgilidir. Çalışma için ağ trafiği izlenerek anormal kabul edilebilecek olan durumların üzerine gidilmiştir. Ağ içerisindeki ve doğrudan sunucu bilgisayar içerisindeki güvenlik duvarı yapılandırmalarının nasıl yapılması gerektiği ve olayın adli bilişim vakası durumuna geldiği zaman elde edilebilecek delillerin nasıl alınacağından bahsedilecektir.**

***Anahtar Kelimeler*—Adli Bilişim, Ağ Adli Bilişimi, Kötücül Yazılım Bilgi Güvenliği, Ağ Güvenliği, Ağ İzleme, Sanallaştırma**

***Abstract-* In order to inquire about whether an illegal interference is Digital Forensic, this criminal interference have to be based on the legal dimension. In the systems that make virtualization, installation, making of configuration and control of virtual machines are easier than physical machines. At this study, a study carried out to determine and prevent a malicious software that makes slow to the traffic of network it works and connect to the unwanted web sites and that is set up on a virtual machine which is from main server computers of Fırat University is scanned the sitution before being Digital Forensic. The study is related to network forensic which can be regarded as a child axis of digital forensic. For this study, by monitoring to the network traffic, it has been put emphasis on the situations that can be considered abnormal. It will be mentioned how to make the security wall configuration within the network and direct main server computer and how to get the evidence which can be gathered when the case turns out to be the digital forensic.**

***Keywords*— Digital Forensics, Network Forensics, Malicious Software-Malware, Information Security, Network Security, Network Monitoring, Virtualization**

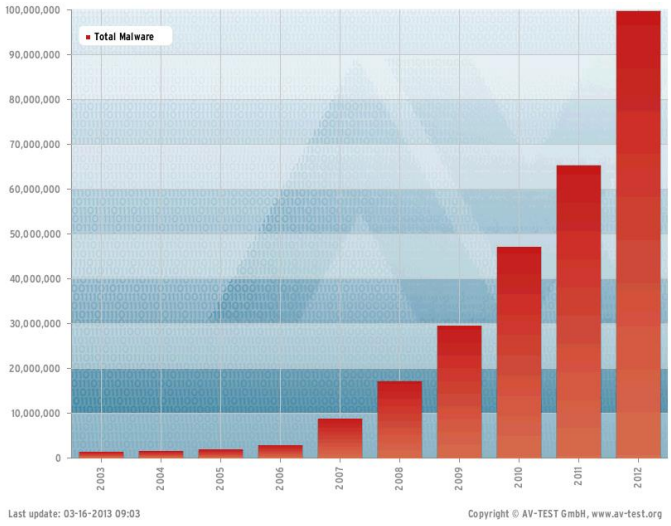
I. GİRİŞ

Kötücül yazılım veya malware (malicious software) bilgisayar sistemlerine zarar vermek, bilgi çalmak veya kullanıcıları rahatsız etmek gibi amaçlarla hazırlanmış yazılımlara genel olarak verilen isim olarak düşünüle bilinir. Genellikle yazılım olarak tanımlanmalarına rağmen bazen basit kodlar halinde de olabilirler[1]. Kötücül yazılımlar, hemen hemen her programlama veya betik (script) dili ile yazılabilmekte ve birçok farklı dosya türü içinde taşınabilmektedirler.

Bilgisayar teknolojilerinin gelişmesi ile bilgi ve bilgisayar güvenliği konusunda en ciddi tehditlerin başında kötü amaçlı yazılımlar gelmektedir. En genel kötücül yazılım türleri şunlardır: [2]

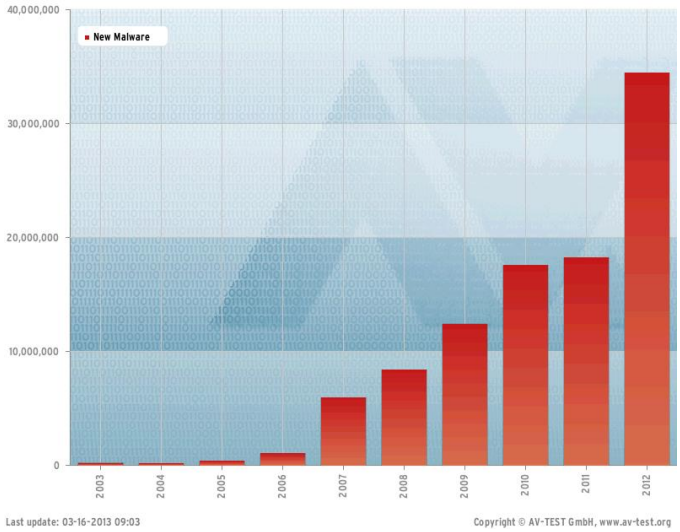
- Bilgisayar virüsü
- Bilgisayar solucanı (worm)
- Truva atı (Trojan horse)
- Arka kapı (backdoor)
- Mesaj sağanağı (spam)
- Kök kullanıcı takımı (rootkit)
- Telefon çevirici (dialer)
- Korunmasızlık sömürücü (exploit)
- Klavye dinleme sistemi (keylogger)
- Tarayıcı ele geçirme (browser hijacking)
- Casus yazılım (spyware)

Son yıllarda sık sık ağ güvenlik problemlerinin meydana gelmesinde, internet dolandırıcılığında, veri hırsızlığında kötücül yazılımlar anahtar suçlu olmuştur [3]. Bağımsız bir bilişim güvenlik enstitüsü olan AV-TEST her gün 200.000 üzerinde yeni kötü amaçlı programı kaydettiğini bildirmiştir. AV-TEST kayıtlarına göre son 10 yılda bilinen toplam kötücül yazılım sayısı şekil-1 de gösterilmiştir [4].



Şekil 1 Son 10 yıldaki toplam kötücül yazılım miktarı

Grafikten de anlaşılacağı üzere 2012 yılında 2011 yılına kadar bilinen toplam kötücül yazılım miktarının yaklaşık %50 oranında arttığı görülmektedir. Şekil-2 de ise son 10 yılda bilinen yeni kötücül yazılım sayısı gösterilmektedir.



Şekil 2 Son 10 yıldaki yeni kötücül yazılım miktarı

Grafikteki verilere göre 2012 yılında yaklaşık 35 milyon kötü amaçlı yazılımın yazıldığı anlaşılmaktadır.

Kaspersky firmasının 2012 verilerine göre internet üzerindeki kötücül yazılımların ilk 10 tanesinin atak miktarı ve toplam içerisindeki yüzdesi Tablo-1 de verilmiştir [5].

Tablo 1: İnternet üzerindeki kötücül yazılımların ilk 10 tanesinin atak miktarı ve toplam içerisindeki yüzdesi

Sıra	Ad	Atak Sayısı	Yüzde
1	Malicious URL	1.393.829.795	87.36
2	Trojan.Script.Iframer	58.279.262	3.65
3	Trojan.Script.Generic	38.948.140	2.44
4	Trojan.Win32.Generic	5.670.627	0.36
5	Trojan-Downloader.Script.Generic	4.695.210	0.29
6	Exploit.Script.Blocker	4.557.284	0.29
7	Trojan.JS.Popupper.aw	3.355.605	0.21
8	Exploit.Script.Generic	2.943.410	0.18
9	Trojan-Downloader.SWF.Voleydaytor.h	2.573.072	0.16
10	AdWare.Win32.IBryte.x	1.623.246	0.10

Tablodan da anlaşılacağı üzere kötücül yazılımların %85 den daha fazla bir miktarı kullanıcının bilgisi olmadan istenmeyen internet adreslerine ulaşmaya çalışan yazılımlardır. Kullanıcı bilgisayarlarında ise tespit edilen ilk 10 kötücül yazılımların etkilediği kullanıcı sayıları ile yüzdeleri Tablo-2 de verilmiştir.

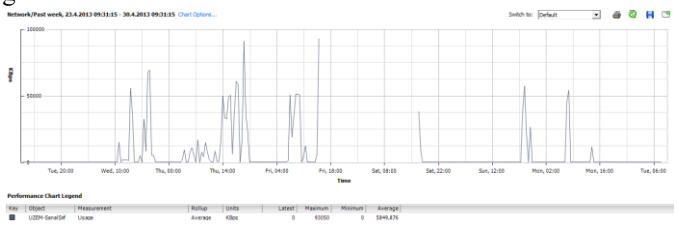
Tablo 2: Kullanıcı bilgisayarlarında en çok görülen kötücül yazılımların ilk 10 tanesinin etkilediği kullanıcı sayısı

Sıra	Ad	Kullanıcı Sayısı	Yüzde
1	Trojan.Win32.Generic	9.761.684	22.1
2	DangerousObject.Multi.Generic	9.640.618	21.9
3	Trojan.Win32.AutoRun.gen	5.969.543	13.5
4	Trojan.Win32.Starter.yy	3.860.982	8.8
5	Virus.Win32.Virut.ce	3.017.527	6.8
6	Net-Worm.Win32.Kido.ih	2.752.409	6.2
7	Net-Worm.Win32.Kido.ir	2.181.181	4.9
8	Virus.Win32.Sality.aa	2.166.907	4.9
9	Hoax.Win32.ArchSMS.gen	2.030.664	4.6
10	Virus.Win32.Generic	2.017.478	4.6

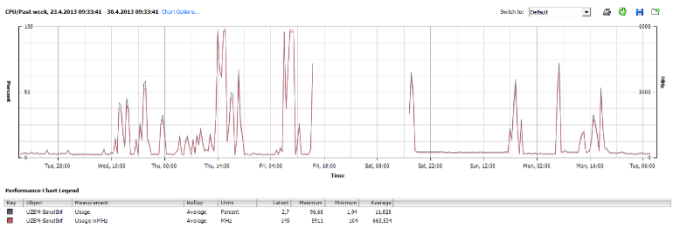
II. YÖNTEM VE METODLAR

Sanallaştırma ile fiziksel kaynaklar birden fazla mantıksal işleme bölerek mevcut fiziksel kaynağın daha verimli kullanılabilmesine olanak sağlar. Sanallaştırılan sunucuların kurulumu, yönetimi ve eğer istenirse daha sonra bellek, işlemci, disk alanı gibi kaynaklarının artırılabilmesi daha kolaydır.

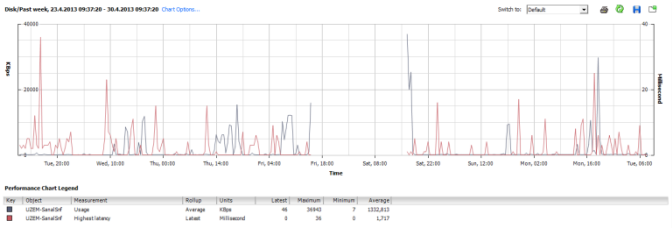
Örnek olay incelememizde Fırat Üniversitesi uzaktan eğitim merkezinin kullanmış olduğu sunucuların birisinde yapılan rutin kontrollerde makinenin çıkış trafiğinin yüksek olduğu, kullandığı işlemci ve bellek miktarının anormal seviyelerde olduğu tespit edilmiştir. Şekil 3-4 ve 5 de bu durum açıkça görülmektedir.



Şekil 3 Sunucu Ağ Trafiği

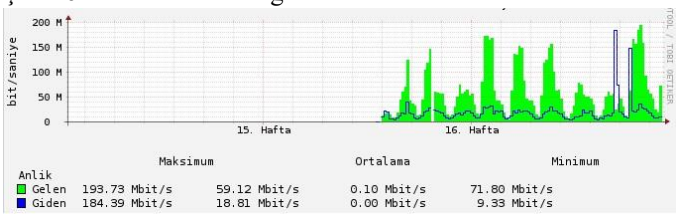


Şekil 4 Sunucu İşlemci Kullanımı



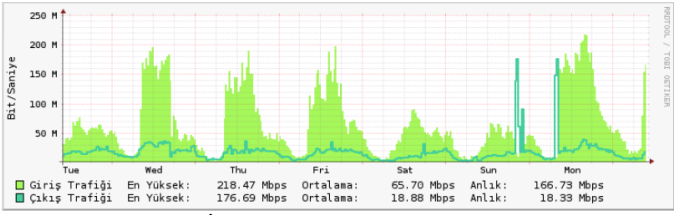
Şekil 5 Sunucu Disk Kullanımı

Şekillerden de anlaşılacağı üzere bazı anlarda işlemci ve disk kullanımının %100 seviyelerine yaklaştığı, mevcut trafiğin ise olması gerekenin çok üzerinde olduğu açıkça görülmektedir. Bu anormal durumun incelenmesi için öncelikle mevcut trafiğin dışarıdan sunucuya doğru mu, yoksa sunucudan dışarıya doğru mu olup olmadığının anlaşılması gerekmektedir. Bunun için üniversite güvenlik duvarı kullanılarak mevcut sununun trafiğinin durumu izlenmiştir. Şekil 6 da trafik durumu görülmektedir.

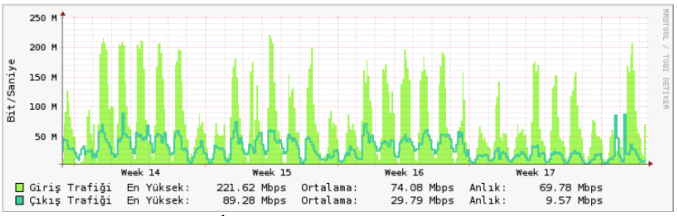


Şekil 6 Güvenlik Duvarında görülen sunucu trafiği

Şekil 6 dan da anlaşılacağı üzere bazı anlarda giden trafiğin neredeyse üniversite için ayrılan toplam bant genişliği miktarına ulaşacak kadar yüksek bir trafik oluşturduğu gözlemlenmektedir. Yapılan trafikten emin olunabilmesi için ULAKBİM (Ulusal Akademik Ağ ve Bilgi Merkezi) tarafında oluşan trafik de kontrol edilmiştir. Şekil 7 ve Şekil 8 de bu durum gösterilmektedir.[7]



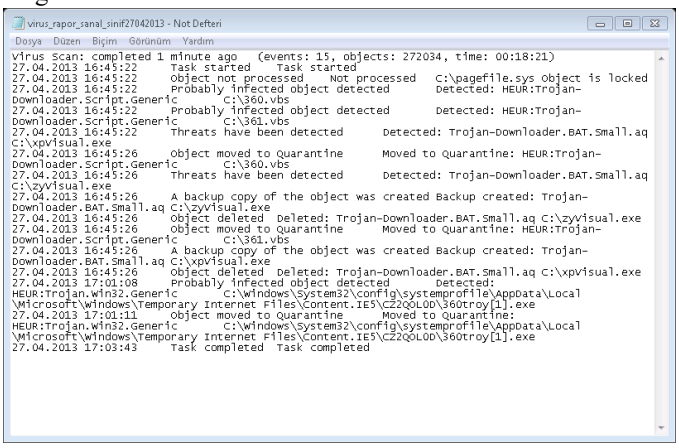
Şekil 7 ULAKBİM tarafında görülen haftalık sunucu trafiği



Şekil 8 ULAKBİM tarafında görülen aylık sunucu trafiği

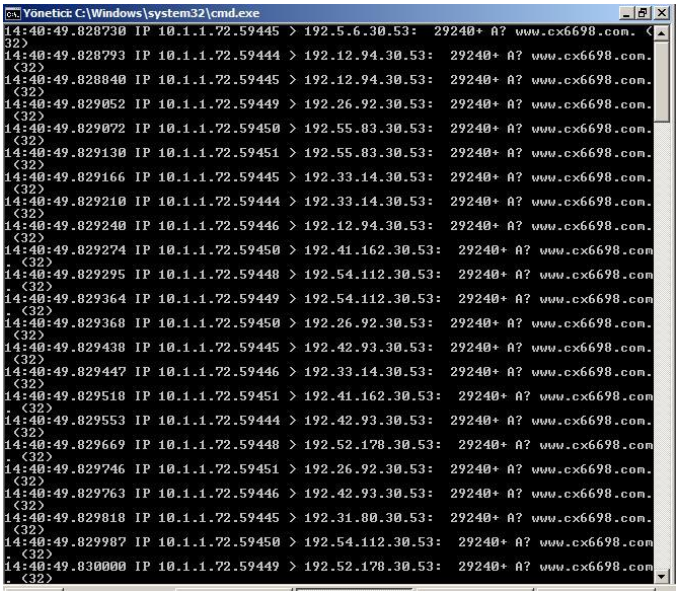
Şekil 7 ve Şekil 8 den de giden trafiğin (çıkış trafiği) bazı anlarda oldukça anormal şekilde yükseldiği görülmektedir.

Mevcut incelemelerden anlaşılacağı sunucu üzerinde ağ trafiği oluşturan bir problem görülmektedir. Bu problemin tespiti ve giderilebilmesi için öncelikle sunucu üzerinde üniversitede lisanslı olarak kullanılan Kaspersky Anti virüs yazılımı ile tarama yapılmıştır. Yapılan tarama sonucu Şekil 8 de gösterilmektedir.



Şekil 8 Antivirus yazılımı tarama raporu

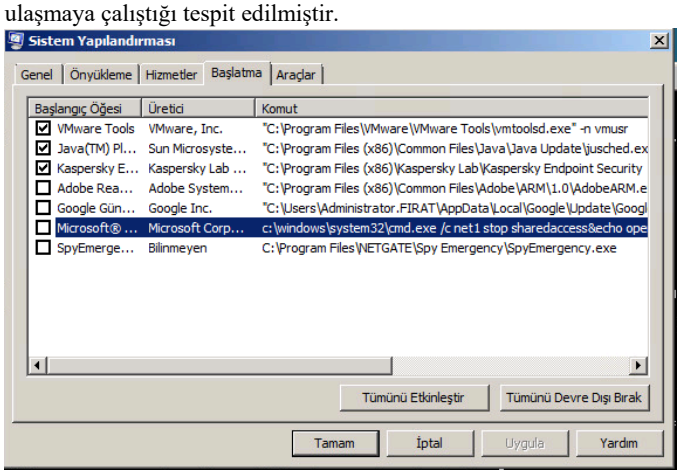
Şekil 8 den de görüleceği üzere sunucu üzerinde bazı kötücül yazılımlar bulunarak etkisiz hale getirilmiştir. Buna karşın mevcut problemin henüz çözülmediği, sunucudan çıkan trafiğin hala anormal bir trafik oluşturduğu gözlemlenmiştir. Kötücül yazılımların tümü antivirus yazılımları tarafından bulunamayabilir. Sunucu üzerinde yapılan trafiğin dinlenebilmesi için BSD lisanslı windump[6] yazılımı kullanılmıştır. Windump yazılımı oldukça popüler bir trafik dinleme yazılımı olan Tcpdump yazılımının Windows işletim sistemi üzerinde çalışan bir kopyası olarak düşünülebilinir. Sunucu işletim sistemi Windows 2008 Server olduğu için Windump ile trafik izlenmiştir. Windows komut isteminde "windump.exe –ni 1 src 10.1.1.72" komutu verilerek trafik izlenmiş ve sisteme bulaşmış zararlı yazılımın belli IP adreslerine haber verdiği ve bundan sonra faaliyetine başladığı Şekil 9 da gösterilmektedir.



Şekil 9 Sunucu içerisinde dinlenilen ağ trafiği

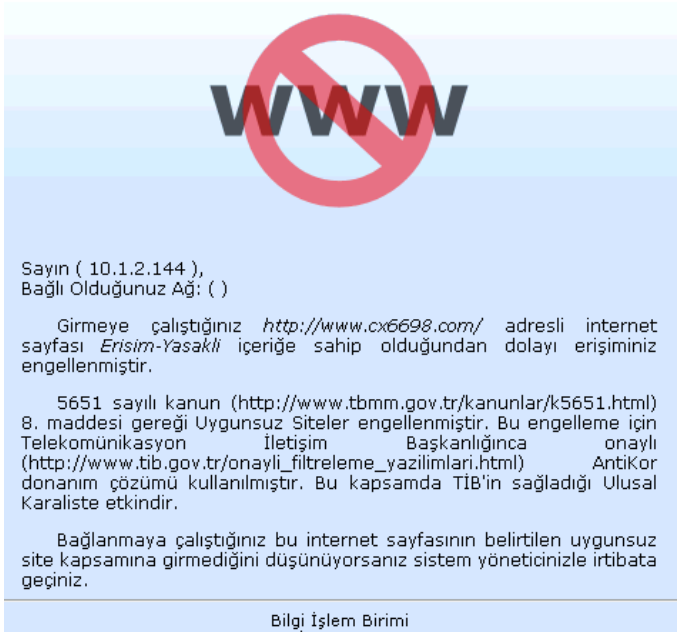
Şekil 9 da ki trafik kayıtları incelendiğinde sunucudan çıkan trafiğin farklı IP adresleri ile internette bulunan bir kaynağa erişmeye

çalıştığı görülmektedir. Farklı IP adresleri ile ulaşılmaya çalışılan sitenin bir kumar sitesi olduğu tespit edilmiştir. Kötücül yazılımın aynı zamanda Şekil 10 da gösterildiği gibi işletim sisteminin başlangıç yapılandırma dosyasına kendisine ait bir kayıt girdiği ve burada bazı komutlar yardımıyla belli sitenin belli IP adreslerine ulaşmaya çalıştığı tespit edilmiştir.



Şekil 10 Kötücül yazılımın başlangıç dosyasına eklediği komutlar

Tespit edilen IP adresleri üniversitenin güvenlik duvarı üzerinden engellenmiştir. Aynı zamanda doğrudan bu siteye erişimlerde engellenmiştir. Şekil 11 de bu kumar sitesine üniversite içerisinden doğrudan girilmeye çalışıldığında kullanıcıların karşısına engellendiğine dair bir mesaj gösterilmektedir.



Şekil 11 Kötücül yazılımın ulaşmaya çalıştığı siteye girilmesi durumunda kullanıcılara gösterilen mesaj

III. SONUÇLAR VE TARTIŞMA

Kanunsuz olarak yapılan bir saldırı yöntemi engellenip pasif hale getirilmiş olmasına rağmen, olayı adli boyuta getirerek hukuki yollara gitmenin zorlukları karşımıza çıkmaktadır. Özellikle saldırının gerçekleştiği adreslerin ya da kötücül yazılımın ulaşmaya çalıştığı adreslerin yabancı bir ülkeden oluyor olması ve her ülkenin bilişim ile ilgili kendisine ait kurallarının olması başvuru aşamasında dahi problem çıkarmaktadır. Bu problemlerin engellenebilmesi için tüm ülkelerin ortak olarak uymak zorunda kalacağı bir standart geliştirici kurum oluşturulması artık bir zorunluluktur. Aksi halde özellikle bilişim hukuku çok fazla gelişmemiş ülkelerden gelen saldırılara karşı yapılabilecek neredeyse hiçbir adli işlem bulunmamaktadır. Yapılabilecek olan ağ trafik kayıtlarının kaydedilmesidir. Özellikle üniversiteler gibi büyük bilgisayar ağlarına sahip sistemlerde 23 Mayıs 2007 Tarihli ve 26530 sayılı resmi gazete gazetede ayrıntıları verilen 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"[8] da belirtilen kayıtların alınması yasal bir zorunluluktur. Fırat Üniversitesinde de 80 numaralı port üzerinden geçen trafik dinlenilerek hangi IP (Internet Protocol) adresinin hangi sürelerde hangi IP adreslerine istek de bulunduğunun bilgisi tutulmaktadır. Bu kayıtlar adli mercilerden gelecek olan taleplerde zaman damgalı olarak kaydedilerek ilgili makamlara verilmek için saklanmaktadırlar. Mevcut kayıtlar aynı zamanda olası bir ağ atağının tespit edilmesine de yardımcı olmaktadır.

KAYNAKLAR

[1] http://en.wikipedia.org/wiki/Malware (30.04.2013 tarihinde girildi)
[2] G. Canbek, Ş. Sağıroğlu, Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri, Grafiker Yayıncılık, ISBN 975-6355-26-3 (2006)
[3] Hsien-De Huang ; Chang-Shing Lee ; Hung-Yu Kao ; Yi-Lang Tsai ; Chang, Jee-Gong, Malware behavioral analysis system: TWMAN Intelligent Agent (IA), 2011 IEEE Symposium on Digital Object Identifier: 10.1109/IA.2011.5953604 , Page(s): 1 - 8 (2011)
[4] http://www.av-test.org/en/statistics/malware/ (30.04.2013 tarihinde girildi)
[5] https://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012 (30.04.2013 tarihinde girildi)
[6] http://www.winpcap.org (27.04.2013 tarihinde girildi)
[7] http://istatistik.ulakbim.gov.tr (30.04.2013 tarihinde girildi)
[8] http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm (15.04.2013 tarihinde girildi)