Fırat Üniversitesi Müh. Bil. Dergisi
33(2), 471-479, 2021

Araştırma Makalesi
https://doi.org/10.35234/fumbd.865117

Siber Olaylara Müdahale ve Analiz Süreci

Muharrem Tuncay GENÇOĞLU[1*], Çağlar SERT[2]
[1] Teknik Bilimler MYO, Fırat Üniversitesi, Elazığ, Türkiye
[2] Siber Savunma Komutanlığı, Genel Kurmay Başkanlığı, Ankara, Türkiye
[*1] mtgencoglu23@gmail.com, [2] caglarsert26@gmail.com

(Geliş/Received: 20/01/2021; Kabul/Accepted: 03/06/2021)

Öz: Günümüzde siber saldırılar ve bununla birlikte siber güvenlik terimi hayatımızdaki varlığını giderek arttırmaktadır. Her saldırı tekniği karşısında bir savunma mekanizması geliştirilmiş, geliştirilen her savunma mekanizmasına karşı olarakda atak vektörlerinde değişiklikler meydana gelmiştir. Bu çalışmada ilk olarak Türkiye' deki mevcut siber olay müdahale yapısı ve devamında siber olay müdahale süresince dikkate alınması gereken teknik inceleme ve detaylardan bahsedilmiştir. İleri seviye kalıcı tehditlerde (APT) iz ve emarelerin tespiti pek çok farklı kaynağın (Network, registry,ram gibi) detaylı analizi sonucu fark edilmektedir. Bu sebeple güncel saldırılarda kullanılan emare ve izlerin tespitinde yara kuralı tabanlı bir yazılım ve konsept ile şüpheli sistemler üzerindeki olay müdahale süreçlerine farklı bir bakış açısı kazandırma amaçlamıstır. Bu kapsamda literatüre araç (tool)bazlı analizin pratikliğini ve efektifliğini ispatlama noktasında katkı sağlayacaktır. Ayrıca bilgisayar olay analizinde izlenecek yol ve yöntemleri, disk incelemesi, APT şüphesi olan bir sistemde tarama, Windows ve Linux Sistemlerde müdahale ve kayıtların elde edilmesi hakkında kısa bir bilgi verilmiştir. Özellikle olay müdahale ve adli bilişim çalışmalarında mevcut teknolojinin ve basitleştirilmiş adli kılavuzların geliştirilmesine, yerli ve milli araçların oluşturulmasına rehber olabilecek bir çalışma olması hedeflenmiştir.

Anahtar kelimeler: Siber olay müdahale, Disk ve ram inceleme, Siber olay analiz, Uçuculuk

Cyber Incident Response and Process of Analysis

Abstract: Nowadays, cyber-attacks and the term cybersecurity are increasing their presence in our lives. A defense mechanism has been developed against each attack technique, and changes occur in attack vectors against each developed defense mechanism. In this context, the first in Turkey as working "until the current cyber incident response structure and continue the technical review and details were mentioned to be considered during cyber incident response. Detection of traces and signs in advanced persistent threats (APT) is realized as a result of detailed analysis of many different sources (such as Network, registry, ram). For this reason, it aims to bring a different perspective to the incident response processes on suspicious systems with a wound rule-based software and concept in the detection of signs and traces used in current attacks. Also, brief information was given about the methods and ways to be followed in computer event analysis, disk inspection, scanning in a system with APT suspicion, intervention in Windows and Linux systems and obtaining records. Especially in incident response and forensic informatics studies, it is aimed to be a study that can guide the development of existing technology and simplified forensic guidelines and the creation of domestic and national tools.

Key words: Cyber incident response, Disc and ram investigation, Cyber incident analysis, Volatility

1. Giriş

Günümüzde siber saldırılar ve bununla birlikte siber güvenlik terimi hayatımızda ki varlığını giderek arttırmaktadır. Ülkeler, kurumlar ve bireyler pek çok bilgiye internet üzerinde ulaşmakta, kamu ve özel hizmetler bu şekilde gerçekleşmektedir. Bilgi Çağı, her türlü bilginin (veri, görüntü, ses vb.) sayısal olarak ifade edilebilmesine, bir başka deyişle elektronik, optik veya manyetik ortamlar üzerinde saklanabilmesi, işlenebilmesi ve iletilebilmesine imkân tanıyan bilgi ve iletişim teknolojilerinin (BİT) gelişimini temsil etmektedir. Bütün bu imkânların yanında, birey, kurum ve devletlerin siber alandaki bilgilerinin ve hizmetlerin güvenliğinin sağlanması çok önemli bir sorun haline gelmiştir. Zira artık savaşlarda bu bilgiler ve hizmetler hedef haline gelmiştir. Bu durum bilgi toplumu olmayı hem bireysel, hem de kurumsal olarak gelişmeyi zorunlu hale getirmiştir. Türkiye'nin bilgi toplumuna geçiş sürecini çok eskilere dayandırmak mümkün olsa da TBMM'de Bilgi ve Bilgi Teknolojileri Grubunun oluşturulduğu 1998 yılını, bu dönüşümün başlangıcı olarak kabul edebiliriz. Bu tarihten sonra birçok resmi ve gayri resmi toplantılar yapılarak geçiş için altyapı oluşturulmaya çalışılmıştır. Bu gelişmeler ile birlikte siber suçlar kavramıda gündemde yerini fazlasıyla almaya başlamıştır.

[*] Sorumlu yazar: mtgencoglu23@gmail.com. Yazarların ORCID Numarası: [1] 0000-0002-8784-934, [2] 0000-0003-1768-5117

Siber saldırılar ve bu saldırıların istatiksel durumu, kurumların siber saldırı veya saldırı ihtimaline karşı savnmma mekanizmaları ve bakış açıları ile ilgili çalışmada, hem saldırı boyut ve şekıllerine hemde kurumsal olarak yaklaşımlardan detaylı olarak bahsedilmiş, ayrıca bilişim suçu mağdurlarının çok büyük miktarlarda para kaybettiğini, dünyada gerçekleştirilen uyuşturucu ve kara para ticaretinden bile karlı olduğunu ve son bir yılda siber suç oranının %34 arttığı belirtilmiştir [15]. 2017 tarihli bir rapora göreyse, fidye yazılım tehditleri 2016 yılında, 2015 yılına göre %36 artarak günde ortalama 1.270'e ulaşmıştır. Son dönemde yaşanan Covid-19 salgını ile yaşamın tamamına yakını dijital ortama taşınmıştır. Kamu işlevleri için kamu kurumlarına gitmek yerine uzaktan bu işleri halledebilme talep edilmektedir. Türkiye Cumhuriyet e-Devlet Kapısı bu noktada en mahir araç olmaktadır. Tüm vatandaşların girebildiği sistemde bundan sonra çok daha geniş yelpazede uygulamalar bulunabilecektir.

Siber güvenlik ile ilgili; bilgi toplumuna geçiş ve siber güvenlik, Türkiye'de polisin siber suçlarla mücadele politikası, uluslararası ilişkilerde yeni bir kuvvet çarpanı olarak siber savaşlar üzerine bir vaka analizi, Türkiye'nin siber güvenlik politikalarının analizi, siber güvenlik alanında teknik inceleme, Avrupa birliği siber güvenlik kanunu gibi çalışmalarda tüm bu dijital değişim ve dönüşümün yaşandığı ortamda meydana gelebilecek siber olayları teknik olarak inceleme, analiz ve değerlendirme yaklaşımı ortaya konulmaktadır [2, 3, 8-14].

2. Siber Olaylara Müdahale ve Analiz Süreci

Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişebilirliğinin ihlal edilmesi veya teşebbüsünde bulunulmasına siber olay denir. Siber Olay, bilişim sistemlerine ve bu sistemlerin, işleyişine, bütünlüğüne ve işlevselliklerine yapılan saldırılar olarak tanımlanabilir. Bu konuda Türkiye'de bulunan otorite makamlarından Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafndan yaymlanan, Siber Güvenliğe Giriş ve Temel Kavramlar klavuzu tüm bu süreçleri detaylı olarak anlatmaktadır [16]. Siber olaylara müdahale süreci ise aşağıdaki gibi gerçekleşir:

- Siber Olayın Tespiti: Tanı Konması.
- Olayın Risk Tanımlanmasının Yapılması: Çalışan sistemler ve Bilgi İfşası.
- Siber Olay Müdahale Ekibine Bildirim Yapılması: İlk bildirimin kurumsal kurumsal Siber Olaylara Müdahale Ekibine (SOME) daha sonra Ulusal Siber Olay Müdahale Merkezine (USOM) bildirilmesi.
- Siber Olaya Müdahale
- Teknik Analiz Saldırgan IP Tespiti: Sistem log kayıtlarının örneklerinin alınması, vaka öncesi kayıtlar ile karşılaştırılması. Meydana gelen siber olay ile ilgili delil ve kanıtların toplanması.
- Önlem Alma: Tespit edilen IP'lere karşı engelleme işlemi yapılması.

Bu süreç Şekil 1'de gösterilmiştir.

Şekil 1. Siber olaylara müdahale süreci

Tespit edilen zararlı yazılım var ise bunların çalışma işlemleri(proses) durdurularak karantina altına alınmalıdır. Böyle bir tespit sonrasında registry kayıtlarının ve bütünlüğünün korunması gereken tüm alanlarda kontroller yapılması gerekir. Bu tip bir dosya veya çalıştırılabilir bir dosya (.exe) var ise zararlı yazılım incelemesi yapılmalıdır.

3. Güncel Bir Adli Bilişim İncelemesi

Dünyada hemen hemen tüm kolluk kuvvetlerinde, siber olay müdahale ekiplerinde aktif olarak kullanılan Encase programı, bu alanda bilinirliliği ve etkinliği en fazla olan ürünlerden biridir. Bu konu ile ilgili EMT Akademi Encase Eğitim Dokümanında, ürünün kullanımı ve özelliklerinden detaylı olarak bahsedilmektedir [6].

Encase Adli İnceleme Programı; adli incelemeyi, aynı anda birden fazla imajın incelemesini, hedef imajı mount ederek ağ üzerinden paylaşımını, hash değeri aynı olmayan benzer dosyaların tespit edilmesini, tespit ettiği şifreli dosyaların şifrelerinin kırılmasını, indexleme yapmasını, İEF ile bütünleşik çalışabilmeyi, USB yazma koruma yapmayı, yazılımsal imaj almayı ve canlı inceleme USB'si oluşturmayı sağlamaktadır.

Encase Timeline İnceleme: Encase incelemede en büyük kolaylığın başında dosyaların tarih ve saat özelliğine göre sorgulama imkânı bulunmasıdır. Eğer bilinen hedef dosyaların herhangi bir tarihi biliniyorsa, o dosyaya kısa sürede ulaşmak mümkün olmaktadır.

Encase Galeri İnceleme: Yine resimlerin hepsinin bir arada görülebileceği Gallery özelliği bulunmaktadır. Bu özellik sayesinde çok sayıda resmi kısa sürede incelemek mümkündür. Encase programı bilgisayar ile ilgili dünya genelindeki dosya türlerini tanıyarak içeriğini kullanıcıya gösterebilecek viewer özelliğine sahiptir. Eğer özel bir dosya tipi tespit edilmişse bu dosya türünü programa tanıtma imkânı bulunmaktadır.

Dava Dosyası Oluşturma Sıralaması: Encase programının kurulumundan sonra bazı ayarlar (options) bir kez, diğer ayarların ise her dava dosyasında yeniden yapılması gerekmektedir.

- İlk defa başlatıldığında Tools > Options altındaki seçeneklerin ayarlamaları yapılmalıdır. Bu ayarlar sonraki zamanda ihtiyaç duyulması halinde güncellenmelidir.

- Firma/kuruma ait logonun dava dosyası veya raporda görülmesi isteniyorsa uygun büyüklükte logo programa yüklenebilir.
- New Case ile yeni bir dava dosyası oluşturulmalıdır. Dava dosyasının hızlıca tamamlanması hedefleniyorsa imaj ve dava dosyası bir SSD disk üzerinde oluşturulmalıdır.
- İnceleme esnasında, bilgisayarın hızı ve boş alan durumuna göre, birden fazla imajı programa yüklemek mümkündür. Bu uygulamanın proses işleminin bitirilmesinin de zaman alacağı unutulmamalıdır.

EncasePathways: Encaseversion 7'den itibaren kullanıcılarına daha rahat kullanım imkânı sunan Pathways (Hazır İnceleme Şablonları) sistemi geliştirilmiştir. Bu sayede Encase Adli inceleme yazılımı hiç bilmeyen veya çok az bilen kişilerin de Encase ile inceleme yapabilmesine imkân verilmiştir. Kullanıcının yeterli eğitimi var ise Pathwyas'leri kullanmadan da doğrudan incelemeye devam edebilecektir.

FastBlock SE ile yazılım koruma sağlama: Encase'in en iyi özelliğinden bir tanesi yazılımsal olarak yazma-koruma sağlama sisteminin programa dâhil edilmiş olmasıdır. Bu sayede herhangi bir yazma koruma donanımına gerek kalmadan diskleri bilgisayara takmak mümkün olabilmektedir.

ProsesEvidence: Encase'in en önemli özelliğinden bir tanesi de Proses işlemidir. Bu özellik yapılmadan başlanacak inceleme eksik yapılmış olacak ve sonuçlara tam olarak ulaşılamayacaktır. Yeni proses işleminde kullanıcılara kolaylık olması açısında kredi kart numaralarına ait grep kodları hazır olarak gelmektedir. Kullanıcı yine isterse buradaki numaralara ilaveten kendi soruşturma özelliğine uygun grep kodlarını hazırlayarak sisteme yükleyebilecektir. Proses'in süresi imajın büyüklüğü ve proses için seçilen menülerin çokluğu ile doğru orantılıdır. Uzun zaman geçmesine rağmen proses çubuğu ilerlememiş olsa bile, proses'in son durumu hakkında EvidenceProseserStatus menüsünden prosesin ilerleme durumu kontrol edilebilir.

BookMark Sistemi: Bookmark sistemi ile inceleme sırasında önem arz eden, delil niteliği taşıyan bulguları rapor hazırlama ekranına yönlendirmek ve tüm kritik bulguları bir araya toplamakta kolaylık sağlar.

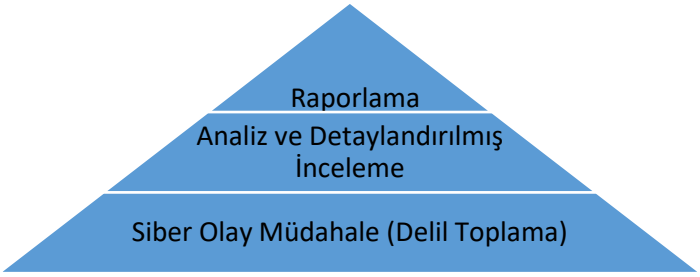
Hash ve Entropy: Aynı hash değerine sahip dosyaları bulmak bütün adli inceleme programlarında bulunmaktadır. Ancak Encase programına konan Entropy özelliği sayesinde, hash değeri değişmiş olsa bile bir dosyanın içeriğinin aynı olma olasılığına göre dosyaları arayabilmektedir.

Canlı İnceleme Modülü Oluşturma: Bu modül sayesinde imaj içeriği görsel olarak canlandırılarak veri üzerinde canlı çalışma imkanı sağlar. Bu modül genellikle adli birimlerde olayın görsel olarak anlatılmasında kolaylık sağlar.

Raporlama: Tüm bulguların ve delil niteliği kazanan materyallerin (resim, video, doküman vb) sonuçlandırıldığı tasnif edildiği alandır.

4. Adli Bilişim Çalışma Şekli (Olay Müdahale ve İnceleme Hiyerarşisi)

Siber olay veya şüpheli bilgi sistem olaylarına müdahale ve sonrasındaki süreçler Şekil 2'de özetlenmiştir.



Şekil 2. Olay Müdahale ve İnceleme Hiyerarşisi

4.1. Siber Olay Müdahale ve Delil Toplama Safhası

Yaşanan siber olayda bildirimden sonra yapılacak ilk iş sistemin ve sistemin kontrol ettiği verilerin ve diğer ağda bulunan kullanıcıların güvenliğinden emin olmaktır. Bundan sonra yapılacak iş, sistem açık ise ilk olarak uçucu verileri almak ile başlar. (Ram imajı, Network kayıtları gibi). Daha sonrasında kalıcı veriler (Non volatile data) diskin imajı alınır, alınan bu imajların 3 adet olması gerekir. Hash değeri ile sonrasında yapılacak kontrol ve araştırmalar için bütünlük değeri elde edilir, yani mühürlenir. Diskin 1 kopyası bilgisayarın kullanıcısına veya

yöneticiye bırakılır. Orijinali disk inceleme ekibinde bulunur; çünkü o gerçek delildir ve ilk iş güvenli, şifreli statikken arındırılmış bir kasaya koyarak emniyeti sağlanır. Yapılan tüm çalışma kopya imajlar üzerinden yapılmalıdır. Kopya imajlar üzerinden farklı bir çalışma veya çoğaltma istenilmesi durumunda write-blocker özellikli bir imaj alma cihazı ile imaj yeniden alınmalıdır. Olay müdahale ve imaj alma aşamalarının tamamında bir yetkilinin bulunması şahit olunması bakımından çok önemlidir. Yapılacak tüm çalışmalarda savunma yapacak kişi veya kurumların tek savunması" ben koymadım, biz koymadık, biz indirmedik, biz yüklemedik" olacaktır. Bu bakımdan tanıklık edecek kişilerin olması ve hash değerinin kayıt altına alınması çok önemlidir. Yapacağımız çalışmadaki hatalar suçluyu suçsuz, hiçbir suçu ve ihmali olmayan kişileri ise suçlu yapabilir.

SSD disk üzerinden alınacak imajlarda her imaj alındığında hash değeri farklı çıkabilmektedir. Bunun sebebi basitçe, elektrik sinyali ile yazılıp silinmesinden kaynaklanmaktadır. İmajı alınan disklerin her biri için ayrı tutanak tutulmalı, "SSD disklerin yapısı gereği her diskin hash (Bütünlük kontrol) değeri farklı çıkmıştır" şeklinde tutanakla kayıt altına alınmalı, böylece vakayı takip eden ve konuya hâkim olmayan insanlar vaka ile ilgili farklı süreçlerde önlerine gelecek itiraz veya farklı durumlarda bilgi sahibi olmuş olurlar.

4.2. Analiz ve İnceleme

Analiz ve inelemede ilk yola çıkılacak husus; olay bildirim raporunun iyi tutulmasıdır. Bahsi geçen şüpheli olay nasıl olmuş, belirli zaman aralıklarında mı olmuş, diğer servislerin veya kullanıcıların çalışmasını engelleyen bir durum mu olmuş. Bu ve benzer yaşanmış, yaşanabilecek kayıtlar inceleme esnasında büyük kolaylık sağlayacaktır. Bunların dışında olay müdahale ekiplerinin ilk sorusu yapılan son pentest rapordur. Bu rapor, mevcut son açıklıkların sömürülüp sömürülmediği üzerinden yola çıkıldığında, süreci hızlandıracaktır. Yapılan çalışma mevcut açıklıklardan yola çıkılarak çözümü hızlandıracaktır.

4.3. Raporlama

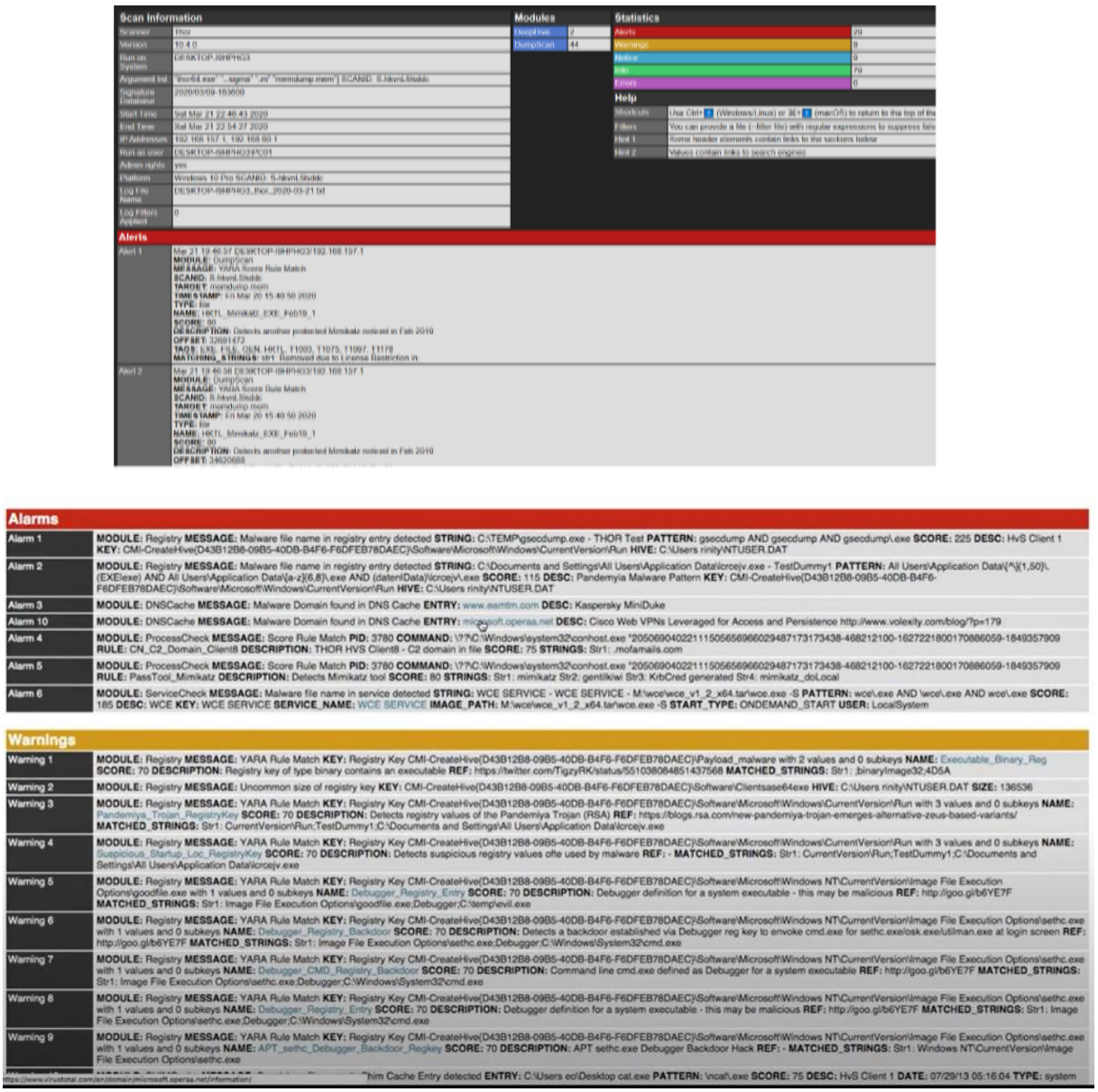
Raporlama, yapılan tüm çalışmanın özetidir. Raporlama yapılırken teknik konular ile sonuç kısmının birbirinden farklı olması önemlidir. Sonuç kısmı teknik detaylara boğulmamalıdır. Sonuç raporu hem adli merciler hem de kurumlarda yöneticilerin anlayabileceği şekilde hazırlanmalıdır. Teknik detaylar; görülen aksaklıklar ve hatalar gibi ayrı başlıklar altında belirtilebilir. İlk giriş kısmı çözümlerin ve bu çözümlere götüren dellilerin ekran görüntülerinden oluşabilir. Bu kısımda yorum asla olmamlıdır, görünen bilinen açık bir şekilde sunulmalıdır. Rapor, sonuç ve siber olayın yaşanmasına neden olan gerekçelerle birlikte kapatılmalıdır. Sonuç kısmında önceki bölümde tespit edilen delil ve sistem durumlarının özet analiz bilgileri yer almalıdır. Siber olayın yaşanmasına neden olan eksiklik ve aksaklılar da yine aynı şekilde kapanış bölümünde yer almalıdır. Yine bu bölümde ispatlı tespitlere yer verilme ve görüş belirtmekten uzak durulmalıdır.

5. Gelişmiş Kalıcı Tehdit (APT) Taraması

Gelişmiş kalıcı tehditler genellikle, sistemlere farklı yollar ile bulaşıp (Otalama saldırısı ve USB bağlantısı gibi) sistemde kendini gizleyerek ya planlanan zamanda sistemi devre dışı bırakmak ya da bilgi sızdırmak (casusluk) amacıyla sistemde kalırlar. Bu saldırılar sistemde normal işleyen yazılımlar üzerinden kendini gizleyerek uzun süre varlığını korumaya çalışırlar. Bu durumun önüne geçebilmek amacıyla SIEM sistemler, IOC incelemeleri veya ileri seviye APT taraması yapılması gerekmektedir. Kısaca bu çalışmalardan bahsedecek olursak,

- *SIEM Sistemler:* Bu sistemler korelasyon çalışma kuralları ile sistem çalışmasını inceler, denetler olağanın dışında meydana gelecek durumlarda alarm üretir ve önlem alırlar.
- *IOC İncelmeleri:* Bu incelmeler de sistem günlükleri ve kayıt defterlerindeki olaylardan, ilişkilerden anormal olduğu değerlendirilenler vurgulanır.
- *APT Taraması:* APT taraması için aslında ileri seviye yazılımlar olması gerekmektedir. APT saldırılarından korunmak için ağ ve firewall yapılandırmasının düzgün yapılması gerekmektedir. Bu özellik veri sızıntısı kaynaklı saldırları engelleyecektir. Bunun dışında sistemde anormallik veya APT şüphesi var ise bunu kapsamlı yara kuralları üzerinden tarayarak gerçekleştirmek gerekir. Bu konuda yaygın olarak kullanılan programlardan biri " Thor Apt Scanner" yazılımıdır. Bu program kullanılırken; dll yapısı, çalışma şekli, verilerin olması gereken boyutta ve buna göre şüpheli bir durum olup olmadığının tespiti oldukça önemlidir. Bu işlemlere ait bir örnek rapor,

Şekil 3'te görülmektedir [1]. Thor Apt Scanner Dökümanında belirttiği üzere, bu yazılım 15.000 den fazla YARA kuralını sistem üzerinde tek tek uygulayarak anormallikleri tespit eder.



Şekil 3. Thor Apt Scanner Result

5.1. Linux Forensic

Son yıllarda, Linux işletim sistemi yüksek performansı ve güvenilirliği nedeniyle Adli bilişimde oldukça önemli hale gelmiştir. Çok geniş bir alana uygulanması sebebiyle, Linux işletim sistemi adli tıp, bilgisayar adli bilimi gibi alanlarda oldukça hayati konumdadır. Madencilik ve analiz, Linux işletim sisteminin öne çıkan özelliklerindendir [17].

Linux sistemler ile ilgili yapılacak müdahalelerde özellikle sistem açık halde ise alınacak kayıtları aşağıdaki gibi listeleyebiliriz;

- Kullanıcı Bilgisi
- Network İstatistik Durum Bilgisi

- Prosesler ve Durumları
- Dosya Değişiklik Durum Kodu ve Ekranı
- Açık Dosya Ekranı
- Yüklenen Modüller
- Soket Bağlantı Durumu
- Takas Alan Durum

Kısaca bu sekiz maddeden bahsedecek olursak kimlik bilgilerinin elde edilmesi ile başlayan inceleme süreci uçucu verilerin toplanması ve daha sonra kalıcı verilerin elde edilmesi ile sonlandırılır. İlk inceleme ve gerekli durumda müdahale işlemi sonrası inceleme safhasına geçilir.

İlk olarak kullanıcı kayıt bilgileri ve işletim sistemi mimari bilgisi elde edilmelidir. Söz konusu bilgiler ekran kaydı olarak alınabileceği gibi uname –a > kullanıcıbilgisi.txt komutu ile kayıt altına da alınabilir.

Netstat daha açıklayıcı hali ile net statistics; network bağlantısı var ise bunun hangi yoldaki dosya tarafından açıldığını gösterir.**netstat > netstat.txt** ile netstat kaydı alınabilir.

Tespit edilen pid değerleri incelenir ve "kill -9 Pid numarası" şeklinde sonlandırma yapılır.Sonlandırma yapılmadan önce trafiği yaratan prosesi export ederek gerekli incelemelerin yapılması sağlanmalıdır.

Dosya değişiklik durumunun takibi için. **" find /etc -type f –printf '%TY -%Tm -% TT %P\n' | sort –r > son değişen.txt**" komutunu girerek son değişiklik dosyları listelenmeli, detaylı inceleme ve raporlama için kayıt altına alınmalıdır. Son yapılan değişikliği,açılan dosya ve bunların network bağlantılarını listelemekte incelemede büyük kolaylık sağlayacaktır. Komutu lsof dur. **lsof > acıkdosyalar.txt** komutukullanılarak kayıt altına alınabilir. Burada, lsof komutundan sonra akılda kalması kolay olacağı için lsmod komutuna da değinelim; lsmod komutunun görevi ise yüklü modülleri ve çalışmalarını listelemektir. Yüklenen modül ve kullanan kaynak detaylı olarak boyutu ile listelenmektedir. "**lsmod > lsmod.txt"** komutu kullanılarak kayıt altına alınabilir. Ayrıca, yine önemli bir komut olan "ss" soket statics'den de bahsetmek gerekir. Bu komut ile açılan bir soket bağlantısı listelenir. Daha önce çalışması yapılan proses listeleri ile özel inceleme yapmak mümkündür. "**ss –l –p –n | grep pid** " değeri girilerek spesifik olarak bir proses listelenir.

Son olarak Swap alanından da bahsetmekte fayda vardır. Sanal belleğin yeterli kalmadığı durumlarda işletim sistemi disk üzerinde faydalanacağı bir alan yaratır. Buna swap alanı (takas) alanı denir. Swapon –s komutu ile listelenir.

5.2. Windows Forensic

Bu kısımda, windows sistemlerinde kullanılacak ilk müdahale komutları ve müdahalede alınması gereken bilgiler ve kayıtlardan bahsedilecektir. Olay müdahalede yapılması gereken işlemlerden en önemlisi canlı sistemde ilk olarak uçucu (volatile) kayıtların elde edilmesidir. Uçucu veriler anlık değişiklik gösterebilecek, hatta erişilmez noktaya gelebilecek verilerdir. Bu sebeple, bir sıra dâhilinde, kritiklik seviyesine göre bu verileri elde etmekte büyük fayda vardır. Siber olay müdahale ekiplerinde yer alan kişilerin, hem olay müdahale hem de inceleme aşamalarında kendilerine aşağıdaki bir kontrol listesi yapması (Check List) ve bu aşamaları takip ederek hareket etmesi olayın çözümlenmesinde hayati öneme sahiptir. İnceleme yapma noktasında da yine kullanılan komut, araç ve yöntemler ile ilgili elimizde bir uygulama formu (Cheat –Sheet) bulunması faydalı olacaktır.

- Sistem Bilgisi
- Login Kullanıcı Bilgisi
- Network Durumu Hakkında Bilgi
- Network Bağlantı Durumu
- Proses Bilgileri
- Proses Port Eşleşmeleri (Port Mapping)
- Proses Hafıza İşlemleri (Proses Memory)

Sistem zamanı, inceleme sürecine başlarken delilleri mukayese etmede, süreci değerlendirmede referans noktasını teşkil edecektir. Windows komut ekranı (Command Prompt) açılarak bu parametreler girilir. Komut "date /t & time /t" şeklinedir. Kullanıcı bilgileri ve oturum bilgilerinin listelenmesi vakanın şekillenmesinde en önemli adımlardan biridir. Bu bilgiler PsloggedOn – Net Sessions –Logon Sessions.Pslogged on uygulması için sysinternals araçlarını indirmiş olmak gerekmektedir. Sürükle bırak olarak komut satırına aktarılarakta çalıştırılabilir.

5.3. Network İşlemleri

Siber saldırganlar sistemlere erişim sağladıklarında ilk erişim aldıkları noktadan daha ileriye gitmek isterler. Bunun asıl amacı yetki alanını genişletme ve daha fazla etkili olabilmektir. Tüm bu hareketleri de network üzerinden yapmaktadırlar. Bu sebepledir ki, şüpheli olayın meydana geldiği noktada derin bir network araştırması, kayıtların incelenmesi de önemli aşamalardan birini teşkil etmektedir. Newtork ile ilgili inceleme esasları aşağıdaki gibi olmalıdır:

- Network protokol ve topolojisi öğrenilmeli
- IPS / IDS log kayıtlar
- Firewall log kayıtları
- Switch ve Router üzerinden alınacak kayıtlar
- Olayın Tespit zamanındaki oturum kayıtları

6. Ram İmaji Üzerinde Analiz Yapma

Ram imajı, inceleme yapan kişi açısından büyük bir öneme sahiptir. Çalışır sistemden alınmış ram imajı veya sistem kapansa bile elde edilen pagefile.sys, swapfile.sys ve hibernfile.sys dosyaları bu konuda önemli fayda sağlamaktadır. Ram imajı incelemede en yaygın kullanılan uygulama, volatility programıdır. Bu program içerisinde barındırdığı çeşitli modüller sayesinde ram imajını en sağlıklı şekilde incelemeye olanak sağlar. Ram İmaj Kayıtlarına ait tüm örnekler ve kullanım kılavuzu bulunmaktadır [7]. Bu program Debian Linux sistemlerde komut satırı üzerinden çalışmakta olup, Windows işletim sistemleri için Volatility Workbench uygulaması bulunmaktadır.

7. Lisanslı Yazilim Kullanarak Muhtemel Zararlı Yazılım Tespiti

Responder Pro. Yazılımı mevcut memory imajlarını statik olarak inceler. Disassemble işlemine tabi tutar ve muhtemel zararlı şüphelileri listeler. Kısaca Responder Pro. Programının işlevlerinden bahsetmek gerekirse, Responder Pro yazılımı hafıza imajını aldıktan sonra, yaptığı statik inceleme sonrası şüpheli prosesleri listeler. Responder Pro Eğitim Dökümanında konu ile ilgili detaylı açıklamalara yer vermiştir [5].

Adli bilişim çalışmalarında en önemli ve detaylı araştırma konularından biriside networkte yaşanmış olayların incelenmesidir. Bu araştırmalarda zorluk derecesi sistemdeki kullanıcı sayısı, sistem işletiminde yürürlükte olan politika (kurallar), ve olayın gerçekleşme biçimidir. Network üzerinde çalışmalar yapabilmek için network yapısına hakim olmak, cihazların nasıl konuştuğunu bilmek kesinlikle şarttır. Bu nedenle de Hub, Switch, Router, Bridge, Firewall gibi network cihazlarının temel yapılarına hakim olmak oldukça önemlidir. Bu ağ cihazlarının kayıtlarının elde edilmesi, konfigürasyonlarının kontrolü ve eksikliklerinin tespiti network analizlerinde ilk başlangıç için çok önemlidir.

8. Sonuç ve Çıkarımlar

Bilgi teknolojilerinin gelişmesi ve yaygınlığının hayatın merkez noktasına gelmesi, bu alanda mağduriyetleride saldırı, dolandırıcılık vb. pek çok başlık altında arttırmıştır. Bu konuda hem kurumsal olarak hem bireysel olarak önlemlerin alınması gerektiği fikri kabul görmüştür. Bu nedenle öncelikle kapsam, farkındalık ve güvenlik anlamında gelişimin tamamlamasının gerekliliği anlaşılmıştır. Tüm bu gelişmelerin yanında teknik anlamda yapılan çalışmalar da siber olay yaklaşımının inceleme ve analizinin bu alanda çalışacak kişiler açısından da sürekli olarak gelişmelerin takip edilmesi, bu alanda kulllanılan yazılım ve donanımlara hakimiyet kazanılması zorunlu hale gelmiştir. Bu bağlamda siber olay ve siber olay müdahale süreçlerinin düzgün bir şekilde belirlenmesi gerektiği vurgulanmıştır. Siber olaylarda ilk müdahaleden yatay ve dikey koordinasyona kadar pek çok etken vardır. Tüm kurumlarda bu olgunun oturması büyük önem taşımaktadır. Kurumsal müdahale ve konseptten farklı olarak teknik açıdan şüpheli durumların kıymetlendirilmesi, siber olay olduğu değerlendirilen durumlarda bahsi geçen tüm prosedürlerin tekniklerin ve araçların kullanılması sonuca ulaşmada hayati önem taşımaktadır.

Olay müdahale ve adli bilişim çalışmalarında bilgi ve tecrübenin yanı sıra, araç kullanımının doğrudan etkili olması, seçilecek yazılım ve donanımlarda hassas olmayı mecbur kılmıştır. Bu sebeple sektöre yeni girecek kişilerin, sektörde aktif olarak kullanılan yazılım ve donanımları meslek hayatlarına girmeden önce tecrübe etmeleri önem kazanmaktadır. Bu bağlamda çalışmamızda; hem ürünü elde etmenin zorluğu hemde eğitim dokumanına ulaşmada yaşanabilecek sorunlar sebebiyle, tüm bu süreç ve yazılımların pratik kullanım şekilleri ve ara yüzleri anlatılmıştır.

Bu çalışma olay müdahale ve adli bilişim çalışmalarında gelecekte mevcut teknolojinin ve basitleştirilmiş adli kılavuzların geliştirilmesine, yerli ve milli araçların oluşturulmasına rehberlik edecektir.

Kaynaklar

[1] ADEO Bilişim Danışmanlık Hizmetleri (2020). Thor Apt Scanner Dökümanı, https://adeo.com.tr/

[2] Aliusta, C., Benzer, R., (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 4(2), 35-42.

[3] Yılmaz, E., Halil, U., Gönen, S. (2015). Bilgi toplumuna geçiş ve siber güvenlik. Bilişim Teknolojileri Dergisi, 8(3), 133.

[4] Yılmaz, O. (2020). Covıd-19 Salgını Sonrası Dönemin Dijital Kodları ve Siber Güvenlik, TASAV. tasav.org.tr

[5] Difose Adli Bilişim Hizmetleri (2019) Responder Pro Eğitim Dökümanı. www.difose.com.tr

[6] EMT Elektronik (2019) EMT Akademi Encase Eğitim Dokümanı. https://www.emtakademi.com.tr/

[7] Ram İmaj Kayıtları (2020) https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples

[8] Ünver, M., Canbay, C., Mirzaoğlu, A. G. (2009). Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara, 8, 2018.

[9] Darıcılı, A. B. Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli için Öneriler. TESAM Akademi, 6(2), 11-33.

[10] Yenal, S.,Akdemir (2020), N. Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi. Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11(1), 414-450.

[11] Taşcı, U., Can, A. (2015). Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014. Firat University Journal of Social Sciences/Sosyal Bilimler Dergisi, 25(2).

[12] Daricili, A. B. (2019). Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli için Öneriler. TESAM Akademi, 6(2), 11-33.

[13] Koşan, M. A., Benzer, R. (2019). Siber Güvenlik Alanında Derin Öğrenme Yöntemlerinin Kullanımı. 6. International Management Information Systems Conference 2019.

[14] Nezgitli, S., Benzer, R. (2020). Avrupa Birliği Siber Güvenlik Kanunu. Journal of Information Systems and Management Research, 2(1), 10-17.

[15] Yıldırım, E. Y. (2018). Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması. International Vocational Science Symposium, IVSS 2018.

[16] Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT). (2014). Siber Güvenliğe İlişkin Temel Bilgiler.

[17] Zhang, R. Yu, M. Yu, W. (2007). Linux file system kernel mechanism analysis and research, Computer and Modernization, no. 12, pp. 14-21.