T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

WEB SHELL SALDIRI TÜRÜNÜN WİNDOWS FORENSİC TEKNİKLERİYLE ANALİZ EDİLMESİ

Kevser Mehveş DAĞCI

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

Adli Bilişim Mühendisliği Bilim Dalı

TEMMUZ 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

WEB SHELL SALDIRI TÜRÜNÜN WİNDOWS FORENSİC TEKNİKLERİYLE ANALİZ EDİLMESİ

Tez Yazarı
Kevser Mehveş DAĞCI

Danışman
Doç. Dr. Türker TUNCER

TEMMUZ 2022
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Web Shell Saldırı Türünün Windows Forensic Teknikleriyle Analiz Edilmesi
Yazarı:	Kevser Mehveş DAĞCI
İlk Teslim Tarihi:	06.06.2022
Savunma Tarihi:	04.07.2022

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

		İmza
Danışman:	Doç. Dr. Türker TUNCER Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Başkan:	Doç. Dr. Şengül DOĞAN Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Fahrettin Burak DEMİR Bandırma Onyedi Eylül Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi	Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Web Shell Saldırı Türünün Windows Forensic Teknikleriyle Analiz Edilmesi" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

04.07.2022

Kevser Mehveş DAĞCI

ÖNSÖZ

Akademik hayatım ve tez çalışma aşamasında maddi manevi destek ve yardımlarını esirgemeyen sayın danışmanım Doç. Dr. Türker Tuncer ve kıymetli hocam Doç. Dr. Şengül Doğan'a sonsuz teşekkürlerimi sunarım.

Fırat Üniversitesi Adli Bilişim Mühendisliğinde görevli hocalarıma ve bu tez çalışması sürecinin her aşamasında yanımda olup, maddi manevi desteklerini esirgemeyen aileme sevgi ve teşekkürü borç bilirim.

Kevser Mehveş DAĞCI
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Web Shell Saldırı Türünün Windows Forensic Teknikleriyle Analiz Edilmesi

Kevser Mehveş DAĞCI

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı

Temmuz 2022, Sayfa: xi + 32

Günümüzde iletişim teknolojilerinin hızla yaygınlaşması ve internet kullanımının artması ile siber saldırılar gün geçtikçe artmaktadır. Meydana gelen siber saldırılar sonucunda; kurumlar maddi ve itibar kaybı gibi büyük kayıplar yaşamaktadırlar. Siber saldırıların geç tespiti, analistlerin yetkinliği ve verilerin ayrıştırılma sürecinde yaşanan aksaklıklar saldırıların zarar boyutunu arttırmaktadır. Bu yüzden meydana gelen saldırıların erken tespiti önem arz etmektedir. Özellikle sistemlere erişim sağladıktan sonra uzun süre sistem içerisinde yıllarca fark edilmeden kalabilen gruplar bulunmaktadır. Bu gruplar APT (Advanced Persistent Threat: Gelişmiş Kalıcı Tehdit) grupları olarak adlandırılıp web shell saldırı türünü sık olarak kullanmaktadırlar. Saldırganların hedef sisteme birden fazla Shell yükleme yöntemi ile erişme olanağı bulunmaktadır. Shell dosya kodu yüklenen sistemlerde saldırganlar erişim yetkisine sahip olarak sistemler üzerinde kötücül aktiviteler gerçekleştirebilmektedir.

Bu tezin amacı siber güvenlik dünyasında bulunan ve bu alanda ilgili olan kişilerin bir web Shell saldırısı ile karşılaştıklarında ilk olarak hangi işlemleri yaparak sistemleri kontrol edebileceği ve alınabilecek önlemleri içermektedir.

Bu tez çalışmasında bir sistem üzerine web shell yüklemesi yapıldıktan sonra Windows sistemler üzerinde nasıl analiz edilerek tespit edildiği açıklanmış ve adli bilişim açısından analizinin nasıl gerçekleştirilmesi gerektiği ortaya konulmuştur. Tez çalışmasının uygulama bölümünde, saldırı sonrası içerisine file upload yöntemi ile shell yüklemesi yapılmış ve imajı alınmış sistemin analizi gerçekleştirilmiştir. Çalışma sırasında kullanılan analiz yöntemlerinin hepsi açık kaynak kodlu ve ücretsiz yazılımlardır.

Anahtar Kelimeler: Web Shell, Windows Analizi, Sunucu Saldırısı, Adli Bilişim

ABSTRACT

Analyzing Web Shell Attack Type with Windows Forensic Techniques

Kevser Mehveş DAĞCI

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

July 2022, Pages: xi + 32

Today, with the rapid spread of communication technologies and the increase in internet use, cyber attacks are increasing day by day. As a result of cyber attacks; Institutions experience great losses such as financial and reputational loss. The late detection of cyber attacks, the competence of analysts and the disruptions in the data separation process increase the damage size of the attacks. Therefore, early detection of attacks is important. Especially after gaining access to the systems, there are groups that can remain unnoticed for years in the system for a long time. These groups are called APT (Advanced Persistent Threat) groups and frequently use the web shell attack type. Attackers have the opportunity to access the target system with more than one shell installation method. In systems with shell file code installed, attackers can perform malicious activities on systems with access privileges.

The aim of this thesis is to include the precautions that can be taken and what actions can be taken by the people in the world of cyber security and who are interested in this field, when they encounter a web shell attack.

In this thesis, it is explained how it is analyzed and detected on Windows systems after web Shell is installed on a system, and how the analysis should be carried out in terms of forensic computing is revealed. In the application part of the thesis, after the attack, the shell was uploaded with the file upload method and the image of the system was analyzed. All of the analysis methods used during the study are open source and free software.

Keywords: Web Shell, Windows Forensics, Server Attack, Digital Forensics

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Kısaltmalar

API	: Application Programming Interface (Uygulama Programlama Arayüzü)
ASP	: Active Server Pages (Etkin Sunucu Sayfaları)
ASPX	: Active Server Page Extended (Aktif Sunucu Sayfası Genişletildi)
APT	: Advanced Persistent Threat (Gelişmiş Kalıcı Tehdit)
C&C	: Command and Control (Komuta Kontrol)
CTI	: Cyber Threat Intelligence (Siber Tehdit İstihbaratı)
CVE	: Common Vulnerabilities and Exposures (Yaygın Güvenlik Açıkları ve Etkilenme)
DB	: DataBase (Veritabanı)
GUI	: Graphical User Interface (Grafiksel Kullanıcı Arayüzü)
HTML	: Hypertext Markup Language (Hiper Metin İşaretleme Dili)
HTTP	: Hyper-Text Transfer Protocol (Hiper-Metin Transfer Protokolü)
IIS	: Internet Information Services (İnternet Bilgi Servisi)
IOC	: Indicators of Compromise (Uzlaşma Göstergesi)
IP	: Internet Protocol (İnternet Protokol)
IPS	: Intrusion Prevention System (Saldırı Önleme Sistemi)
IDS	: Intrusion Detection System (Saldırı Tespit Sistemi)
JSP	: JavaServer Pages (Java Sunucusu Sayfaları)
LFI	: Local File Inclusion (Yerel Dosya Ekleme)
MFT	: Master File Table (Ana Dosya Tablosu)
NTFS	: New Technology File System (Yeni Teknoloji Dosya Sistemi)
OS	: Operation System (İşletim Sistemi)
PHP	: Hypertext Preprocessor (Hiper-Metin Önişlemcisi)
RDP	: Remote Desktop Connection (Uzak Masaüstü Bağlantısı)
RFI	: Remote File Inclusion (Uzaktan Dosya Ekleme)
SQL	: Structured Query Language (Yapılandırılmış Sorgu Dili)
TSK	: The Sleuth Kit / Sleuth Kiti
TTP	: Tactics Technics Procedures (Taktik Teknik Prosedürler)
URL	: Uniform Resource Locator (Tekdüzen Kaynak Bulucu)
VB	: Visual Basic (Temel Görsel)
WMI	: Windows Management Instrumentation (Windows Yönetim Araçları)

1. GİRİŞ

Tüm kuruluşlar, bilgisayar sistemlerinde ve kurumsal ağlarda meydana gelen siber suçlara hazırlıklı olmalıdır [1]. Windows yapıları, Windows kullanıcısı tarafından gerçekleştirilen etkinlikler hakkında bilgi tutan nesnelerdir. Windows yapıları, adli analiz(forensics) sırasında toplanan ve analiz edilen hassas bilgileri içerir. Windows sistemler üzerinde adli verileri analiz edip, kullanıcı etkinliğini izleyerek ve bulguları düzenleyerek Microsoft Windows işletim sistemleri hakkında derinlemesine ve kapsamlı olarak adli analiz yapmak mümkündür.

Web kabukları(shell) tehdit aktörleri tarafından sık sık kullanılmaya başlamış, web sunucularının güvenliğini aşmasını ve ek saldırılar başlatmasını sağlayan kötü amaçlı komut dosyalarıdır. Tehdit aktörleri, çeşitli nedenler için web shell saldırı türünü kullanmaktadır. Bunlar;

- Dosya değiştirerek veya ekleyerek web sitelerini bozma
- Hassas bilgileri veya kimlik bilgilerini sızdırma ve toplama.

Microsoft, Web Shell olarak yapılan saldırıları "orman yangınına" benzeterek hızlı yayıldığını duyuran bir açıklama yayınladı. Microsoft tespit ve müdahale ekibi tarafından hazırlanan bu raporda bu saldırıların büyüklüğü ile ilgiliydi. Rapora göre bu saldırı türü geçen döneme göre 2 kat arttı. Raporda Ağustos 2020 ve Ocak 2021 arasında geçen dönem incelendi. 2019-2020 yılları arasında 77 bin civarı olan web shell saldırılarının 2020-2021 yılları arasında 140 bine kadar çıktığı tespit edildi. Yapılan saldırıların kurumsal firmalara, halka açık sistemlere ait yanlış yapılandırılmış ya da güvenlik açığı içeren sunuculara yüklenen web kabukları olduğu belirtildi [2].

Saldırganlar kurum veya kuruluşlara ait kurumsal ağ üzerinde yanal hareket yöntemi ile yayılım gösterebilirler. Bu yanal hareket ile kısa sürede birçok cihaz (bilgisayar, sunucu) saldırganlar tarafından ele geçirilebilir. Web sheller bir saldırı zincirinin ilk adımıdır ve genellikle ağ içerisinde yayılım göstermede ilk adımı oluşturur.

Bu makalede Windows işletim sistemine sahip cihazlar üzerinde meydana gelen bir web shell saldırısının tespit edilme aşamaları ve tespit ettikten sonraki süreç de yer alan analiz adımlarından detaylı olarak bahsedilmiştir.

1.1. Tezin Amacı

Bu tezin amacı siber güvenlik dünyasında sık sık kullanılan web shell atak tipinin Windows sistemler üzerinde saldırı sonrası analiz adımları anlatılmıştır. Analiz için dünya üzerinde en sık kullanılan işletim sistemi olarak Windows işletim sistemi seçilmiştir. Bu tez

çalışması kurum ve kuruluşları büyük zarara uğratabilecek saldırı türünün nasıl analiz edileceği ve hangi noktalardan kısa sürede tespit edilebileceğini gösterecektir. Çalışma içerisinde uygulama adımlarında, incelemeyi yapan kişiye kolaylık olması açısından ücretsiz yazılımlar kullanılmıştır. Bu çalışma bu alanda çalışacak olan kişilere araç seçimi ve analiz adımları için yol gösterecektir.

1.2. Bulgular

Günümüzde işlenen siber suçların ve siber saldırıların miktarı ve çeşitliliği her geçen gün artmaktadır. Shell saldırısının özellikle güncel olmayan bu nedenle açıklıklar bulunan sistem üzerinden saldırganlara erişim kazandırdığı bilinmektedir. Siber saldırının etkisini veya yayılımın hızlıca tespiti için, enfekte olmuş sistemlerden delillerin toplanması ve kötücül aktivitenin analizi sağlanmalıdır. Saldırganlar, kurum veya kuruluş içerisinde yanal hareket sağlayarak birçok cihazı enfekte edebilir, hizmet sağlayan servis/uygulamaları durdurabilir ya da dosyaları şifreleyebilir. Bu tez içerisinde son dönemde saldırganlar tarafından büyük yapı ve kuruluşlarda sık tercih edilen web shell saldırı türü incelenmiş ve bir saldırı sonrası analiz adımları anlatılmıştır. Bir web shell dosyası güvenlik çözümü ürünleri tarafından tespit edildikten sonra analiz adımları sırasında ilk olarak dosyanın oluşma zamanının kontrolü sağlanmıştır. Dosyanın oluşma zamanı tespit edildikten sonra aynı zaman aralığında farklı zararlı yazılımlar yüklenip yüklenilmediği kontrol edilmiştir. Sistem üzerinde çalıştırılan kayıtların analizi gerçekleştirilmiştir. Saldırganın sistem üzerindeki erişim durumunun kontrolü için sunucu logları analiz edilmiştir. Makine üzerinde elde edilen erişim ile kalıcılık sağlanıp sağlanılmadığının analizi yapılmıştır. Elde edilen veriler Windows sistem üzerinde açık kaynak kodlu yazılımlar kullanılarak analiz edilmiştir. Literatür içerisinde var olan analiz yöntemleri kullanılarak, bir saldırı örneği altında birleştirilmiştir.

1.3. Tezin Organizasyonu

Bu tez çalışması toplamda 7 bölümden oluşmaktadır.

Tez çalışmasının ikinci bölümünde web kabuğu(shell) saldırısı, saldırının nasıl gerçekleştiği, sistem üzerine yükleme yöntemleri ve yüklendikten sonra sistem içerisinde elde edilen haklar anlatılmıştır.

Tez çalışmasının üçüncü bölümünde dünya genelinde yaygın olarak kullanılan web shell saldırı örneklerinden bahsedilmiştir.

Tez çalışmasının dördüncü bölümünde, saldırı yapılan web servis sisteminin yapısı anlatılmıştır. Tez çalışmasının beşinci bölümünde bir sunucu makinesi üzerinde herhangi bir saldırı durumu ya da veri kaybı gibi durumlarda elde edilen logların önemi ve elde edilebilecek içerik bilgileri anlatılmıştır.

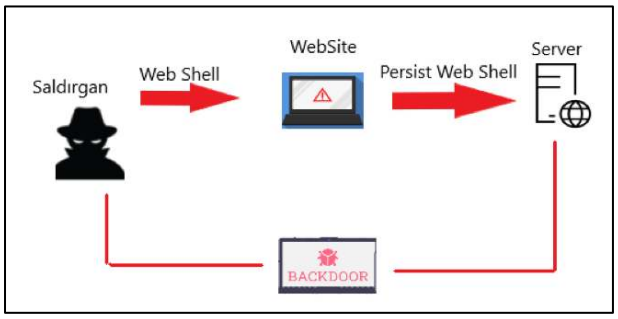
Tez çalışmasının altıncı bölümünde sistem üzerine yükleme yapılan shell kodu ve analiz yöntemlerinden bahsedilmiştir. Analiz sırasında kullanılan yazılımlar açıklanmıştır.
Tezin yedinci ve son bölümünde sonuç ve önerilerden bahsedilmiştir.

2. WEB KABUĞU SALDIRISI

Web shell, Türkçe karşılığı web kabukları saldırısı farklı yazılım dillerinde yazılan kod dosyalarının açığı bulunan hedef sistem üzerine yüklenmesi ile oluşmaktadır. Genellikle bir sunucuda desteklenen herhangi bir programlama dilinde yazılabilir olup PHP'nin web uygulamaları üzerinde yaygın kullanımı nedeniyle en yaygın olarak PHP programlama dilinde yazılır. Ancak ASP.NET, Ruby, Python, Perl gibi dillerde kullanılmaktadır.

Web shell'in ana işlevi, web sayfası dosyalarını ve veritabanını değiştirmektir. Örneğin bir ASP Web shell genellikle web sayfasının içeriğini gözden geçirmek ve web sitesini kontrol etmek için diğer tekniklerle birlikte dosya ve veritabanı bileşenlerini çağırır [3]. Saldırgan web shell dosyasını sunucu içerisine yükledikten sonra yazılan kod dosyası içeriğine göre uzaktan, sunucu üzerinde işlemler gerçekleştirebilmektedir. Bu işlemler sunucu üzerinde, sunucu dizin içeriklerini listeleme, dosya yükleme, komut terminali açma, kimlik doğrulama portallarına karşı kaba kuvvet parolası denemeleri yapabilme gibi özelliklerdir.

Web Shell saldırı yönteminin tespiti zor olduğu için saldırganlar tarafından son dönemlerde sıkça kullanılmaktadır. Saldırgan hedef sistem üzerine bir web shell'i enjekte etmeden önce sistem hakkında araştırmalar yaparak web shelli yükleyebileceği güvenlik açığı bulunan web sunucusu seçmektedir. Şekil 2.1.'de saldırganın sunucu üzerine kod yükleme adımı gösterilmiştir.



Şekil 2.1. Saldırı Kodu Yükleme Adımı

Bir sunucu üzerine birden fazla web shell yükleme yöntemi bulunmaktadır.

Bunlar;

- SQL enjeksiyonu
- Uzaktan dosya ekleme veya yerel dosya ekleme güvenlik açıkları
- Uzaktan kod çalıştırma
- Uygulamalar ve hizmetlerdeki güvenlik açıkları [4].

2.1. Geleneksel Web Shell Yükleme Teknikleri

Bu başlık altında bir sistem üzerine web kabuğu yükleme yöntemleri, nasıl yüklendiği vb. gibi bilgiler anlatılacaktır.

2.1.1. SQL Enjeksiyonu

Bir SQL enjeksiyon(injection) saldırısı yalnızca bir veritabanını elde etmekle sınırlı değildir, aynı zamanda saldırganın uzaktaki sunucuya dosya yüklemesine ve bir web shell aracılığıyla uzaktan erişim elde etmesine izin verebilir.

SQL enjeksiyonu , web'de karşılaşılan en yaygın güvenlik açıklarından biridir ve aynı zamanda en tehlikelilerinden biri olabilir. Saldırganlar, hassas bilgileri çıkarmak, mevcut verileri değiştirmek veya yok etmek ya da sunucuya sahip olmak amacıyla saldırıyı yükseltmek için kötü amaçlı SQL kodu enjekte edebilir [5].

Web sitesi içerisinde SQL atağına yönelik gerekli vektörleri deneyerek ilgili zafiyetin bulunduğu belirlendikten sonra web sheller, saldırganlardan komutları başlıca 2 yöntem kullanarak alabilir:

- Komutlar URL'de göründüğü için GET isteklerine dayalıdır. GET isteklerine dayalı olarak web shell erişimi otomatik olarak sağlamak için sqlmap kullanılabilinir.
- Komutlar yükte gönderildiğinden biraz daha gizli olan POST'a dayalıdır. POST'a dayanan özel ve daha gelişmiş bir web shell yüklemek için sqlmap kullanılabilinir.

Bu yöntemde kullanılan Sqlmap, açık kaynak kodlu SQL Injection açıklığı tespit ve istismar etme aracıdır. Kendisine sağlanan hedef web uygulamasının kullandığı veritabanı sistemine gönderdiği çeşitli sorgular/komutlar ile sistem üzerindeki SQL injection tipini tespit eder yine kendisine sağlanan parametrelere göre çeşitli bilgileri hedef veritabanından alır [6].

2.1.2. Dosya Ekleme Güvenlik Açığı

Hedef bir site üzerine dosya yükleme ya da erişim sağlanılmak istenen bir dosyaya erişmemize olanak sağlayan bir açık türüdür. PHP dili ile kodlanan sistemlerde görülen bir güvenlik açığıdır. Yerel Dosya Ekleme (LFI) ve Uzaktan Dosya Ekleme (RFI) açığı olarak ikiye ayrılır.

LFI açığı yerelden, PHP sayfasını sunan web sunucusundan(server) sunulmayan/sunulmaması gereken fakat zafiyetten ötürü erişebilinen dosya ya da dosyaları erişebilme izni olduğu sayfaya ekleme olayıdır. Örneğin bir web sunucu üzerinde içerisinde merhaba yazan bir hello.php dosyası olduğu ve buna erişme izni olduğu düşünülsün. Sunucu

üzerinde /etc/passwd dosyasına erişim izni olmadığı düşünülsün. LFI zafiyeti ile URL üzerinden girilen değer ile hello.php gibi /etc/passwd ye de erişim sağlanabilir.

RFI açığı ise uzaktaki bir web sunucusuna uzaktan dosya ekleyerek kod çalıştırmaktır. PHP web programlama dili ile kodlanmış uygulamalarda, yazılımcıların tanımladıkları değişkene değer atamaması veya atanan değerlerin filtrelenmemesinden kaynaklanmaktadır [7].

Yerel Dosya ekleme açığına örnek bir kod yapısı aşağıda gösterilmiştir.

<php include($_GET['konu']) ?> gibi bir yapı içeren bir web sayfası olsun. Bu sayfa URL'den gelen isteğe göre cevap dönecektir. Örneğin urlden abc.def/?konu=hello.php komutu incelendiğinde en basit ve yaygın LFI açığı olarak bilinir. Çünkü burada varolan bir dosya URL yoluyla sunucudan çağırabilinir. Örneğin sitenin root dizininde bir yapılandırma dosyası olduğunu tahmin edildiğinde root dizini bulunur. "../../../etc/passwd" gibi dizin çağırma işlemi ile sunucu üzerinde yer alan ve erişilmemesi gereken bilgileri görüntüleyebilmektedir.

Bu işlem ile sunucunun üzerinde yer alan sunucu bilgilerinin tutulduğu (erişim yapan ip, web tarayıcı (browser) bilgisi) adrese erişim yapılarak web shell parçacığı yüklenebilir. Web shell içerisinde yazılan zararlı kod ile sunucu içerisinde yapılmak istenilen işlemler uygulanır.

2.2. Modern Web Shell Yükleme Teknikleri

Gelişmiş Kalıcı Tehdit (Advanced Persistant Threat) bir kişi veya grubun bir ağa yetkisiz erişim sağladığı ve uzun bir süre boyunca algılanamadığı bilgisayar ağı saldırısıdır. Bu tür saldırılar genel olarak ticari veya politik amaç güden devlet desteği ile yapılan saldırılar olmasına rağmen, son birkaç yıl içerisinde devlet sponsorluğunda olmayan belirli hedeflere yönelik geniş çaplı APT saldırıları da yaşanmıştır [8].

APT gruplarının hedefleri geniş ölçüde değişir, ancak geniş bir kümede toplanır. Saldırılar şunları içerebilir:

Jeopolitik ilişkiler: Komşu ülkeleri ile kaygıları olan devletler, APT gruplarını ekonomik veya askeri faaliyetler, niyetler veya stratejiler hakkında istihbarat elde etmek için yakındaki ulusları izlemek veya sızmak için kullanırlar.

Fikri mülkiyet hırsızlığı: APT gruplarının saldırıları genelde ev sahibi devletin ekonomik veya askeri hedeflerini ilerletmeye yardımcı olmak için fikri mülkiyetleri çalma hedefine sahiptir. Tescilli teknolojiyi çalmak, araştırma ve geliştirme maliyetlerinde milyarlarca dolar tasarruf sağlayarak, pazarda rekabet avantajı sağlayarak ya da askeri hazırlıktaki boşluğu kapatarak avantaj sağlanmasına yardımcı olabilir. Başka bir ülke veya işletmenin gizli iletişimlerini çalarak, APT grupları hükümetler ile müzakerelerde veya görüşmelerde üstünlük sağlayabilir.

Bozulma ve yıkma: APT grupları ayrıca iletişim sistemlerinde, endüstrileşmiş kontrol sistemlerinde ve kamu hizmetlerinde yıkıcı eylemlerde bulunabilirler. Bunlar ayrıca ekonomik olarak motive edilmiş saldırıları da içerebilir. Bazı devletler, başka bir devlette hasara yol açacak

güce sahip olduklarını göstermenin, bir düşman ya da rakibin eylemlerinden caydırmak için yeterli bir tehdit olacağını umuyorlar [9].

APT gruplarının kullandıkları saldırı vektörleri ve tekniklere ilişkin çıkarımlar Mitre ATT&CK Framework'ü kullanarak yapılmaktadır. Bu Framework bugüne kadar gerçekleştirilmiş saldırıların atak vektörlerinin tutulduğu bir matristir. Bu matris hem kırmızı takım (red-team) hem de mavi takım (blue-team) tarafından kullanılmaktadır.

Saldırı sürecinde sosyal mühendislik ve sıfırıncı gün (zero-day) açıklarını kullanan zararlı yazılımlar geliştirilip hedefe sızma gerçekleştirilebilir. APT saldırıları çok dikkatli bir hazırlık sürecinden geçirilerek gerçekleştirilir. Saldırı mevcut güvenlik önlemlerini atlamak üzerine kuruludur.

APT'ler, çok farklı hedeflere yönelik saldırılar düzenleyebilir. Bu hedefler genellikle telekomünikasyon, enerji, teknoloji, finans gibi ülkeler için önemli sektörlerden oluşmaktadır [10].

APT ve suç grupları tarafından web shellerin sıklıkla kullanımı, önemli siber olaylara yol açmıştır. Web sheller, uzaktan erişim ve saldırı boyutunun genişletilmesinde olan etkili rolü ile sıklıkla saldırılarda kullanılmaktadır. Basit web sheller bile önemli bir etkiye sahip olabilir ve çoğu zaman minimum düzeyde varlığını sistem üzerinde sürdürebilir. APT grupları tarafından sıklıkla tercih edilen bu saldırı vektörünün sistem üzerinde kullanımına yönelik bazı yöntemleri bulunmaktadır.

Aşağıda bazı APT grupları tarafından web shell kullanılarak gerçekleştirilen saldırı yöntemleri anlatılmıştır.

2.2.1. Sıfırıncı Gün Açıklıkları

Sıfırıncı gün açıklıkları daha önceden bilinmeyen veya tespit edilmemiş ancak ciddi saldırılara yol açacak zafiyetler barındıran yazılım veya donanım kusurlarıdır. Zero-day açıklıkları çoğunlukla saldırı gerçekleşene kadar tespit edilmesi zor olan zafiyetlerdir. Zero-day saldırısı ise geliştiricilerin bir yama veya düzeltme yayınlamaya fırsat bulamadan saldırganın zafiyeti istismar etmesi ve zararlı yazılımı yaymasıyla gerçekleşir. Bu nedenle bu zafiyet sıfırıncı gün açıklığı olarak isimlendirilmiştir [11].

APT saldırılarında virüs, Truva atı, casus yazılım, sosyal mühendislik gibi güvenlik açıklarından yararlanan çeşitli saldırı araçları ve teknikleri kullanılabilir. Bu saldırıların amacı, genellikle belirli görevler için bir veya daha fazla bilgisayara kötü amaçlı kod yerleştirmek ve mümkün olan en uzun süre boyunca tespit edilmeden sistem üzerinde kalmaktır. APT grupları bu güvenlik açıklıklarından sıfırıncı gün güvenlik açığından da yararlanır.

2.2.1.1 başlığı altında yakın zamanda gerçekleşen APT grubu tarafından zero-day açıklığı kullanılarak yapılan web shell saldırısı anlatılacaktır.

2.2.1.1. Exchange Sunucu Saldırısı

2020 yılında Microsoft müşterisi tarafından Exchange sunucusunu hedef alan gelişmiş bir siber saldırı tespit edildi. Saldırıda kullanılan teknikler, araçlar ve prosedürlerdeki (TTP'ler) benzerliklere dayanarak saldırının Hafnium APT grubu tarafından yapılmış olduğu değerlendirildi.

Saldırganlar bu saldırıda China Chopper web shell'ini kullanarak yanal hareketler gerçekleştirdi.

HAFNIUM APT grubu, ilk erişimi elde etmek için Microsoft Exchange üzerindeki güvenlik açıklarından yararlandıktan sonra, güvenliği ihlal edilmiş sunucuya web shelleri yerleştirdi. Bu web shell ASP dili ile yazılmıştır. Dağıtılan web sheller, sistem üzerindeki verileri .zip dosyasına sıkıştırma daha sonra ise sıkıştırılan verileri dışa aktarmak için komutlar yürütmekte fayda sağlamıştır. Hedefe ulaşan China Chopper web shelli, işletim sistemi komutlarını uzaktan yürütmek, ek araçlar yüklemek, diğer sistemlere erişim kazanma ve verileri sızdırmak gibi faaliyetleri yürütmek için kullanılabilir. Sunucunun nerede olduğunu, neye bağlı olduğunu ve ağ içinde nereye dönüleceğini kontrol edebilir [12].

Microsoft bu olay sonrası birden fazla yama kodu yayınlamıştır. Bu yaygın güvenlik açıkları ve etkilenmeler (CVE) yamaları ile grubun sistem yetkisi ile yapabileceği etkinlikleri kontrol etme, rastgele dosya yazma yetkinliğinin kontrolleri gibi zafiyetlerin giderileceği belirtilmiştir.

Bazı saldırganlar, Exchange Server saldırılarında olduğu gibi zero-day açıklığı kullanır, ancak daha sıklıkla Web'e yönelik sunucularda çalışan eski yazılım sürümlerini de hedeflemektedirler.

Bu tez çalışmasında analizi yapılan sunucu üzerine aspx dilinde yazılmış olan web kabuğu, file upload yöntemi ile enjekte edilmiştir.

Web kabukları, saldırganlar tarafından izinsiz giriş yaşam döngüsünün farklı aşamalarında farklı amaçlar için kullanılmaktadır. Bunlardan bazıları;

- Uzaktan kalıcı erişim elde etme
- Ağı keşif etmek
- Ayrıcalık yükseltmek

Saldırganın hedef sistem üzerinde yapabileceklerine ait bazı durumlar detaylı olarak aşağıda anlatılmıştır.

2.3. Uzaktan Kalıcı Erişim Hakkı

Bir web shell dosyası, saldırganın hedef sunucuya uzaktan erişmesine ve kontrol etmesine izin veren bir arka kapı içerir. Bunun asıl nedeni, saldırganı güvenliği ihlal edilmiş sunucuya her

erişim gerektiğinde tekrardan bir güvenlik açığından yararlanma durumundan kurtarmaktadır. Saldırganın hedef amaçlarından bir tanesi de erişim sağladığı sunucu üzerinde kalıcı olarak barınabilmektir. Bir sunucuya kurulduktan sonra, web kabukları bir kuruluşta kalıcılığın en etkili yollarından biri olarak hizmet eder [2].

Analizi yapılan birkaç web Shell komut dosyasının, yalnızca web shell dosyasını yükleyen saldırganın erişebilmesini sağlamak için parola doğrulama gibi özelleştirilmiş teknikler kullandığı da belirlenmiştir. Bu tür teknikler, komut dosyasını belirli bir HTTP başlığına, IP adresine veya belirli tanımlama değerleri ile çalıştırılabilmeyi sağlamaktadır.

2.4. Ağı Keşfetme

Saldırgan sistem üzerinde erişim elde ettikten sonra bağlı olduğu ağ trafiğini izlemek isteyebilmektedir. Ağ içindeki güvenlik duvarlarını, ana bilgisayarları, bağlı olan başka sistemlere erişimin olup olmadığının kontrolünü sağlayabilir. Saldırganın bu adımı günler-aylar alabilir çünkü saldırgan içeride bulunduğu süre boyunca az miktarda dikkat çekmesi ve sistem üzerinde uzun süre boyunca keşif yapmaya devam edebilmesi gerekmektedir.

Güvenliği ihlal edilmiş sistem, ağ dışında bulunan hedeflere saldırmak veya bunları taramak için de kullanılabilir [13].

2.5. Ayrıcalık Yükseltme

Bir sunucu çalışma mantığında yazılım, kullanıcı izinleriyle çalışacaktır. Saldırgan, bir web kabuğu kullanarak, Linux ve diğer UNIX tabanlı işletim sistemlerinde süper kullanıcı olan root ayrıcalıklarını üstlenmek için sistemdeki yerel güvenlik açıklarından yararlanarak ayrıcalık yükseltme saldırıları gerçekleştirmeye çalışabilir.

Saldırgan, kök hesaba erişimle, yerel dosyaları yönetme, yazılım yükleme, izinleri değiştirme, kullanıcı ekleme ve kaldırma, parola çalma, e-posta okuma ve daha fazlası dahil olmak üzere sistemde temelde her şeyi yapabilir [13].

3. YAYGIN OLARAK KULLANILAN WEB SHELL DOSYALARI

2021 yılında Microsoft tarafından yayınlanan web shell durum raporuna göre bir önceki yıla göre web shell saldırı vakalarında 1 yıl içerisinde 2 katı daha fazla saldırı olduğu gözlemlenmiştir. Web shellerin artan yaygınlığı, saldırganlar için basit ve etkili olabildiğine bağlanabilir. Web Shell saldırıları, saldırganların savunmasız durumda olan web sunucularından yararlanmaları için başvurulan yöntem olmuştur. Basit bir yöntem olması, etki alanının güçlü olması saldırganlar için popüler bir teknik olmaya devam edeceğini göstermektedir. Bu başlık altında saldırganların kullanmış oldukları tehdit istihbarat raporlarında da sık sık yer alan web kabukları saldırı içerikleri detayları anlatılmıştır.

3.1. China Chopper Web Shell Saldırısı

China Chopper, ilk olarak 2012'de keşfedilen yaklaşık 4 kilobayt boyutunda bir web shelldir. Bu web shell, web sunucularını uzaktan kontrol etmek için gelişmiş kalıcı tehdit (APT) grupları da dahil olmak üzere kötü niyetli Çinli aktörler tarafından yaygın olarak kullanılır. China Chopper, parola kaba kuvvet saldırısı seçeneği, kod gizleme, dosya ve veritabanı yönetimi ve grafik kullanıcı arabirimi gibi birçok komut ve kontrol özelliğine sahiptir. Başlangıçta şu anda kapalı olan www.maicaidao.com web sitesinden dağıtıldığı bilinmektedir [14].

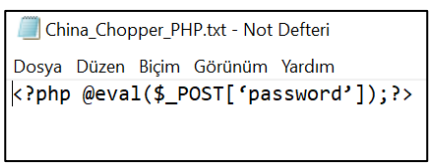
China Chopper, sistemde bir arka kapı görevi görmektedir. Yapısal olarak iki temel bileşeni vardır.

- Web kabuğu komuta ve kontrol (C&C) dosyası (web kabuğu istemcisi).
- Metin tabanlı bir Web kabuğu kod kümesi(payload) (sunucu bileşeni).

Metin tabanlı payloadın içeriği basit ve kısadır, karmaşık bir yapısı yoktur. Saldırgan payloadı doğrudan hedef sunucuya elle yazabilir, dosya aktarımı yapmasını gerektirmez. Bu nedenle metin içeriğinin analistler tarafından fark edilmesi zor olmaktadır.

Aşağıda iki farklı dilde yazılan içeriği bulunmaktadır:

Şekil 3.1'de güvenliği ihlal edilmiş sunucu tarafı için yazılmış PHP kodu örneği gösterilmiştir.



Şekil 1.1. China Chopper PHP dili örneği

Şekil 3.2.'de güvenliği ihlal edilmiş sunucu tarafı için yazılmış Aspx kodu örneği gösterilmiştir

Şekil 3.2. China Chopper .Aspx dili örneği

China Chopper, hedef yönetimi ve uygun saldırı özellikleri olan menü odaklı bir GUI'dir. İstemciyi açtıktan sonra, başlangıçta Web kabuğunun bileşenlerini barındıran ve ilk olarak dağıtımı yapılan www.maicaidao.com'a erişim sağlayan adres görülür.

Ancak istemci, uzaktan erişimin yarısıdır ve ağ üzerinde tespit edilecek kısım değildir. İletişimi Web uygulaması biçimindeki bir kod kümesine dayanır. Bu kod kümesi, ASP, ASPX, PHP gibi çeşitli dillerde yazılabilmektedir. Hazır olarak var olan, indirilebilen orijinal dosyalar bulunabilmektedir. Web kabuğu istemcisi, payloaddan bağımsız olarak saldırgana, kimlik doğrulama portallarına karşı kaba kuvvet parola tahmininde bulunma/kullanma özelliği içeren bir "Güvenlik Taraması" seçeneği sunar. Ayrıca istemci ve kod kümesini birleştirirken mükemmel komuta ve kontrol özellikleri sunmaktadır. Bunlar;

- Veritabanı Yönetimi (DB istemcisi)
- Dosya Yönetimi (Dosya gezgini)
- Sanal Terminal (Komut kabuğu)

Son olarak China Chopper, işletim sistemi düzeyinde etkileşim için komut kabuğu erişimi sağlar.

3.2. TwoFace Web Shell Saldırısı

TwoFace (ikiyüz), ilk olarak 2017'de ortaya çıkan kötü niyetli bir ASPX web shellidir. İki yüz olarak isimlendirilmesindeki neden, İranlı hacker grubu APT34 tarafından kullanılan HighShell ve HyperShell'dir. Bir TwoFace saldırısı iki aşamada gerçekleştirilir. İlk aşama olan HighShell boyut olarak küçüktür ve bir ASP.NET web sunucusuna yerleştirildiğinde legal bir oturum açma sayfası gibi görünür. İkinci aşama olan HyperShell, uzaktan etkinleştirilene kadar uykuda ve tespit edilemez durumda kalır. Saldırganlar daha sonra yükleyiciye ikinci aşama kabuğunun şifresini çözmesi ve etkinleştirmesi talimatını verebilir [15]. Yükleyici web kabuğu ile etkileşim kurmak için tehdit aktörü, güvenliği ihlal edilmiş sunucuya HTTP POST isteklerini kullanır. Adından da anlaşılacağı gibi yükleyici bileşeni, esas olarak yük bileşeninin aynı sunucuya kaydedilmesi ve yüklenmesinden sorumludur ve aktörün, yükleyiciden çok daha fazla

işlevselliğe sahip olan yük bileşeni ile etkileşime girmesine izin verir. Yükleyici kabuğunun temel amacı, isteğe bağlı olarak ikincil bir web kabuğu yüklemektir. Yük olarak adlandırdığımız ikincil web kabuğu, yükleyicinin içine şifrelenmiş biçimde gömülüdür [16].

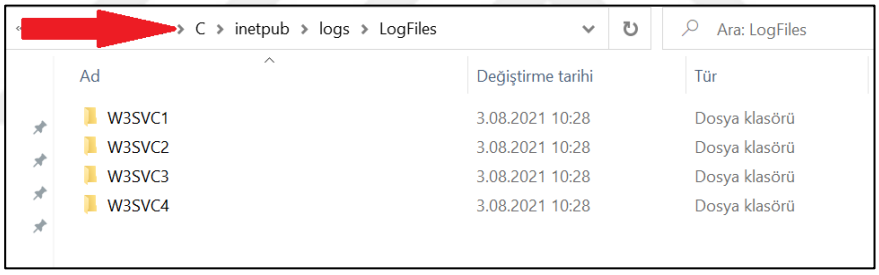
TwoFace etkinleştirildiğinde, bir saldırganın güvenliği ihlal edilmiş sunucuyu kontrol etmesine, kullanıcı kimlik bilgilerini toplamasına, kötü amaçlı dosyalar yüklemesine veya hassas verileri çıkarmasına olanak tanır [15]. Şekil 3.3'de TwoFace web shell'i komut çalıştırılma arayüzü sayfası gösterilmiştir.

Şekil 3.3. TwoFace Komut çalıştırılma AraYüzü

HighShell, güvenlik açığı bulunan sunucu üzerine yüklenildikten sonra tehdit aktörü tarafından DO IT alanına, doğru parola yazılarak sistem üzerinde çalıştırılacak komutlar girilir. TwoFace webshelli doğru parola girilmediği sürece güvenlik analistleri tarafından fark edilmemektedir. Nedeni ise doğru parola girilmediği müddetçe herhangi bir çıktı üretmemekte ve komut çalıştırılamamaktadır.

4. IIS WEB SUNUCUSU

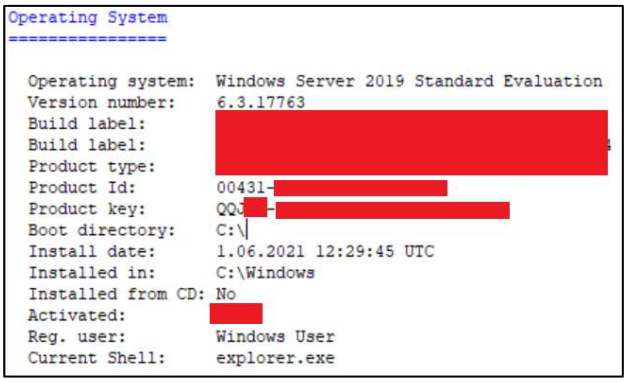
Web sunucuları, web sitelerine gelen isteklere cevap dönerek ziyaretçilere istenilen sayfanın gönderilmesini sağlarlar. IIS açılımı Internet Information Service, Microsoft firmasının Windows işletim sistemlerinde ve sunucularında kullandığı, web servisi sunan yazılımdır [17]. IIS sunucuları Asp.Net diliyle yazılan web yazılımlarının daha kolay görüntülenmesine yardımcı olur. Sunucular, web sitesine yapılan istekleri belirli log dosyalarında tutmaktadır. Web sitesine yapılan isteklerin ne zaman, hangi metot kullanarak (GET, POST), hangi IP üzerinden geldiği kayıt altına alınmaktadır. Ayrıca bu log kayıtları daha ayrıntılı tutulacak şeklinde ayarlanabilmektedir. Sunucu üzerinde yer alan erişim log dosyalarının detaylı analizleri ile olası bir saldırının tespiti gerçekleştirebilinmektedir. Saldırganın dosyayı hangi zamanda çalıştırdığı, hangi IP adresi/adresleri üzerinden gerçekleştirdiği gibi bilgileri erişim log dosyaları analiz ederek öğrenilebilinir. Standart bir Windows sunucusu üzerinde IIS logları **"%SystemDrive%\inetpub\logs\LogFiles"** dizini altında tutulmaktadır. Şekil 4.1.'de IIS loglarının standart bulunma dizini gösterilmiştir.



Şekil 4.1. IIS Log Dosyası Kayıt Dizini

IIS her web sitesi için ayrı log dosyası oluşturmakta ve bu logları ayrı klasörler altına kayıt etmektedir. Log dosyasının hangi periyotlarla kaydedileceği belirlenebilmektedir genellikle sistem uzmanları tarafından günlük olarak kayıt edilmesi tercih edilmektedir.

Bu tez içerisinde saldırı için yükleme yapılan .aspx uzantılı web Shell dosyası bir IIS sunucusu üzerine yüklenmiştir. Sunucuya ait bilgiler Şekil 4.2.'de gösterilmiştir.



Şekil 4.2. Sunucu Bilgisi

5. SUNUCU ÜZERİNDE LOGLAMANIN ÖNEMİ

Web sunucuları tarafından kaydedilen log dosyaları, sistem hakkında istatistiki bilgi çıkarımında oluşabilecek sorunların çözümünde kullanılabilmektedir. Ayrıca siber saldırıların tespitinde ve ispatlanmasında önemli rol oynamaktadır. Gerçekleşen bir saldırıda bu logların kanıt olarak kullanılabilmesi için güvenilirliği de önem taşımaktadır. İçeriğinde detaylı bilgi olması ve bu bilgilerin doğru, değiştirilmemiş olması önem arz etmektedir. Genellikle bir log dosyası içeriğinde kayıt edilebilecek özellikler varsayılan olarak sınırlı şekilde loglama seçenekleri ile oluşturulmaktadır. Bu seçenekler içerisinde tarih, saat, istemci IP adresi, kullanıcı adı, sunucu IP adresi, sunucu adı, sunucu bağlantı portu, protokol durumu, referer gibi bilgiler yer almaktadır. Bütün log bilgilerinin kayıt edilmesi performans ve kapasite miktarının olumsuz etkilenebileceğinden dolayı doğru bir yapılandırma olmadığı için hangi ayrıntıların kayıt edileceği önceden planlanmış olmalıdır.

5.1. Log Dosyası İçeriğindeki Bilgiler

Bir log dosyasının varsayılan olarak yapılandırılması sonrası kaydettiği içerik bilgileri aşağıda Tablo 5.1.'de belirtilmiştir.

Tablo 5.1. Log Dosyası İçerik Detayları

İçerik	Kullanımı
Tarih/Saat	Web sitesine yapılan isteğe ait zaman bilgisi
İstemci IP Adresi	Web sitesi üzerine hangi IP'den gelindiği bilgisi
Sunucu IP Adresi	Hangi IP adresine istek yapıldığı
Sunucu Bağlantı Noktası	Hangi port üzerinden istek yapıldığı bilgisi
Yöntem	Hangi method kullanıldığı bilgisi(Get/Post/Delete)
URL Sorgusu	Sayfaya yapılan istek bir parametre ile çağrılıyorsa parametre komutu(querystring)
URL Kökü	Hangi sayfa üzerine istek yapıldığı
Protokol Durumu	Web sunucusunun karşı tarafa gönderdiği sonuç kodudur.
Gönderilen Bayt Sayısı	Sunucu üzerinden karşı tarafa gönderilen veri miktarı
Referrer	Sunucu üzerine nereden gelindiğinin bilgisi

6. MATERYAL VE METOT

Web kabuklarının artan yaygınlığı, saldırganlar için ne kadar basit ve etkili olabileceklerine bağlanabilir. Bir web kabuğu, tipik olarak saldırganların sunucu işlevlerine uzaktan erişim ve kod yürütme sağlamak için web sunucularına yerleştirdiği, tipik web geliştirme programlama dillerinde (örneğin, ASP, PHP, JSP) yazılmış kötü amaçlı kod parçasıdır. Web kabukları, saldırganların verileri çalmak için sunucular üzerinde komutlar çalıştırmasına veya sunucuyu kimlik bilgisi hırsızlığı, yanal hareket, ek yüklerin konuşlandırılması veya uygulamalı klavye etkinliği gibi diğer etkinlikler için başlatma rampası olarak kullanmasına izin verirken, saldırganların etkilenen bir ortamda kalmaya devam etmesine izin verir [2].
Web kabukları, saldırgan komutlarını diğer sistemlere yönlendirmek için kalıcı arka kapılar veya geçiş düğümleri olarak hizmet edebilir [18].

Saldırganlar tarafından kolayca değiştirilebildiklerinden ve genellikle şaşırtmaca kullandıklarından, web kabuklarının algılanması ve tespiti zor olabilmektedir. Çok yönlü olay, tespit müdahale ürünlerini kullanarak, web kabukları tespiti kolaylaşabilmektedir. Bugüne kadar yapılan web kabuğu saldırıları incelendiğinde saldırganların kodun içerisinde bazı standart kalıplar kullandıkları görülmüştür. Yanlış-Pozitif (False-positive) sonuç getirmesine de bağlı olarak sık sık kullanılan bu kalıpların sistemler üzerinde eklemesi yapılarak taramalar yapılabilir.

Bir web kabuğu tespit edildikten sonra sırası ile analiz aşamaları şu şekildedir:

- Dosyanın Tespiti
- Siber Tehdit İstihbaratı
- Dosya Sistem Kayıtları($MFT) ve Meta Verilerin Analizi
- Sunucu Erişim Loglarının Analizi
- Amcache Kayıtlarının Analizi
- Güvenlik (Security) Loglarının Analizi
- Kalıcılık Mekanizmalarının Kontrolü

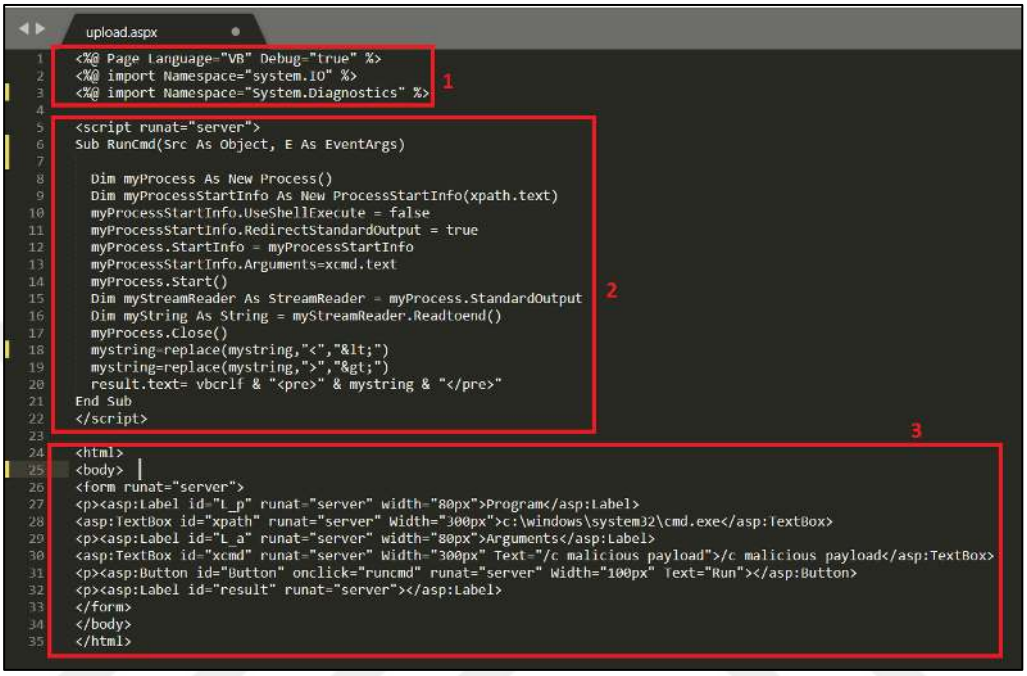
Bu başlık altında bir web Shell saldırısı sonrası analiz adımları açıklanacaktır.

6.1. Upload.Aspx

Bu tez çalışması için sunucu üzerine “upload.aspx” isimli web Shell dosyası yüklenmiştir. Aspx dilinde yazılmış Shell dosyası içeriği Visual studio ile oluşturulmuştur. Yazılan web shell dosya içeriği 3 aşamada aşağıda detaylı olarak anlatılmıştır.

Şekil 6.1.’de yer alan kod içeriğinde, 1 numara ile gösterilen alanda ilgili kütüphanelerin girişi yapılmıştır. 2 numara ile belirtilen alanda Runcmd fonksiyonun yaptığı işlem saldırganın 3 numara içerisinde aldığı argümanı sistem komutu olarak çalıştırılmasını sağlayan kod

parçacığıdır. 3 numara da yer alan <html> ile başlayan kod parçacığı içerisinde, saldırgan tarafından girilen komutlar zararlı kod(malicious payload) kısmından alınır. Kod içerisinde yer alan cmd.exe yoluna gönderilerek burada 2 numarada yazılan runcmd fonksiyonu yardımı ile çalıştırılır.



Şekil 6.1. Upload.aspx dosya içeriği

6.2. Dosyanın Tespiti

Web Shell tespitinde imza tabanlı algılama yöntemini kullanmak bir web Shell saldırısı için güvenli olmayabilir bunun nedeni web kabuklarının değiştirilmesinin kolay olmasıdır. Bununla birlikte, bazı siber aktörler, minimum değişiklikle popüler web kabuklarını kullanır (China Chopper, R57) [18].

Saldırganlar çeşitli nedenlerle web kabuklarında çok az değişiklik yapabilir veya hiç değişiklik yapmayabilir. Bu durumlarda, YARA kuralları gibi kalıp eşleştirme tekniklerini kullanarak yaygın web kabuklarını tespit etmek mümkün olabilir. YARA kuralları, çeşitli güvenlik ürünleri tarafından içe aktarılabilir veya bağımsız bir YARA tarama aracı kullanılarak çalıştırılabilir [19].

Potansiyel bir web kabuğu tespit edildiğinde, yöneticiler dosyanın kaynağını ve orijinalliğini doğrulamalıdır.

Bu web kabuklarını algılamanın en iyi yöntemi, web uygulamasının doğrulanmış, iyi bir sürümüyle karşılaştırmaktır. Tespit edilen dosyanın IOC değeri ve dosya içeriği false-positive olması durumuna karşı doğruluğu için detaylı olarak incelenmelidir.

6.3. Siber Tehdit istihbaratı

Tehdit istihbaratı, birden fazla kaynak aracılığıyla ortama yönelik tehditler hakkında bilgi toplamayı amaçlayan bir süreçtir. Bu süreçte ilk olarak olası olayların erken tespit edilebilmesi ve önlenebilmesi için elde edilen bilgilerin doğru analiz süreçlerinden geçirilmesi beklenmektedir [20].

Güvenlik çözümü ürünleri tarafından bir web shell saldırısı tespit edildikten sonra öncelikli olarak elde edilen saldırı göstergeleri (IOC) verilerinin kaynaklarda sorgulaması yapılır.

Elde edilen IOC'lerin daha önce herhangi bir yer de analizi gerçekleştirilmiş mi kontrol edilir. Siber Tehdit İstihbaratı (CTI) kaynaklarında sorgulama yapılır. Kurum içerisinde yapılan bir sorgulama ise kurumun CTI kaynakları veritabanına eklenir.

Shell kodu içerisinde tespit edilen, kötü amaçlı zararlı yazılım ile iletişim kuran komuta ve kontrol sunucusu(C&C) adresi tespit edilebilmektedir. Elde edilen verilerin shodan, virüstotal gibi CTI kaynaklarında sorgulaması yapılır. Saldırgan aktivitesi daha önce CTI kaynaklarında tespiti yapılan bir dosya/içerik ise analiz adımları buna göre şekillendirilebilir.

6.4. Dosya Sistem Kayıtları ve Meta Verilerin Analizi

Sistem üzerine yüklenen web Shell dosyasını imza tabanlı saldırı önleme veya saldırı tespit (IPS/IDS) gibi sistemler ya da herhangi kullanılan bir güvenlik çözümü ürünü ile tespit ettikten sonra bakılması gereken noktalardan biri dosyanın adı, oluşum zamanı, boyutu ve bulunduğu dizin bilgilerinin yer aldığı MFT dosyasını incelemektir.

Ana Dosya Tablosu ($MFT), bir NTFS (New Technology File System) dosya sistemindeki en önemli dosyadır.

Örneğin; MFT' de 100 giriş varsa ve bir birimde bulunan dosya X silinirse, daha sonra yeni 1000 tane dosya oluşturulursa, oluşturulan dosya, silinen X dosyasına ait MFT kayıt alanının üzerine yazılmaktadır. Dosyanın içeriği sabit sürücüde bulunsada, adı, meta verileri vb. içeren veriler MFT tablosunun üzerine yazılmaktadır. NTFS dosya sisteminin analiz edilebilmesi için, dosya sistemi hakkında verilerin fiziksel ve mantıksal konumları gibi önemli bilgiler araştırılmalı, birimin veri yapısının ve gizli verilerin incelenerek daha iyi deneyim elde edilmesi sağlanabilir [21].

Silinen dosyaların kurtarılıp kurtarılamaması, yeni eklenen dosyaların üzerine yazılıp yazılmadıklarına bağlı olabilmektedir.

Şekil 6.2.'de MFT tablosu içeriğinde yer alan veriler ve sıralaması hakkında bilgi verilmektedir.

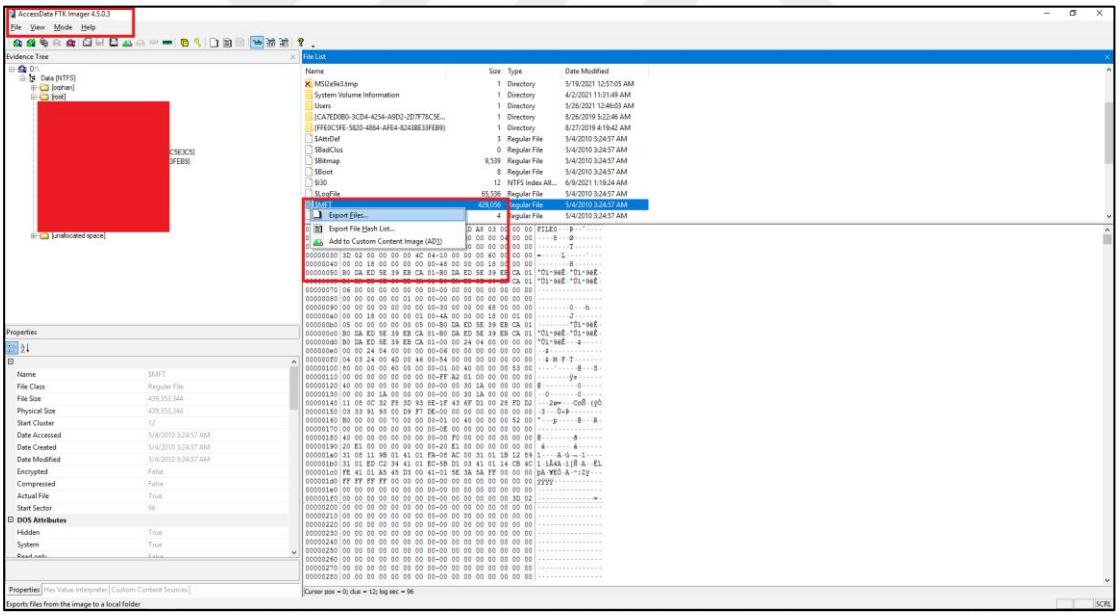
Şekil 6.2. MFT Tablosundaki Veriler

Dosyanın sunucu üzerinde oluşma bilgisine ait MFT kayıtlarının elde edilmesi bir sonraki başlık da açıklanmıştır.

6.4.1. MFT Dosya Sistem Kaydının Elde Edilmesi

$MFT dosyası, her birimin root dizini altında bulunur ve FTKImager ücretsiz yazılımı kullanılarak çıkarılabilir [22].

Şekil 6.3.'de FTKImager yazılımı kullanılarak sistemden MFT dosyası dışarı çıkartılma adımı gösterilmiştir.



Şekil 6.3. FTKImager Yazılımı Dosya Çıkarım İşlemi

Ayrıca "The SleuthKit" (TSK) aracı kullanarak da canlı, uzak bir sistemden $MFT kaydı elde edilebilinir.

Şekil 6.4.'de $MFT dosyasını masaüstüne çıkarttıktan sonra EricZimmerman aracı olan MFTECmd.exe yazılımı ile ayrıştırma(parse) yapılmıştır.

Şekil 6.4. $MFT Dosyası Parse Etme Komutu

MFT dosyasının parse işlemi sonrası belirtilen dizinde excel dosyası oluşur. Excel içerisinde web kabuk dosyasına ait bilgiler Şekil 6.5.'de gösterilmiştir.

	A	B	C	D	E	F	G
1	ParentPath	FileName	FileSize	NameType	Created0x10	Created0x30	LastModified0x10
138587	.\Users\kevser\AppData\Local\Pack	0.1.filtertrie.interm	5	Windows	2021-08-15 10:14:58.1196616		2021-08-15 10:14:58.1196616
138588	.\Users\kevser\AppData\Local\Pack	0.2.filtertrie.interm	5	Windows	2021-08-15 10:14:58.1196616		2021-08-15 10:14:58.1196616
138589	.\Users\kevser\AppData\Local\Pack	Apps.ft	20714	DosWindows	2021-08-15 10:14:58.1347452		2021-08-15 10:14:58.1502915
138590	.\inetpub\wwwroot	upload.aspx	2822	Windows	2021-08-15 10:17:59.8832758		2021-08-15 12:28:21.9029378
138591	.\Windows\debug	Dfsr00017.log.gz	3617	Windows	2021-08-15 10:47:20.8239803		2021-08-15 10:47:20.8239803

Şekil 6.5. MFT Dosyası İçeriği

Upload.aspx web kabuk dosyasının "inetpub/wwwroot" dizini altında 15.08.2021 10:17:59 tarihinde sistem üzerinde oluştuğu görülmüştür. MFT dosyasından saldırganın IIS sunucusu üzerinde dosyaların oluşum zamanları görülebilmektedir. Ayrıca, bir web kabuğu tespit edildiğinde, web kabuğunun zamanlarında oluşturulan/değiştirilen veya web kabuğunu oluşturan kullanıcı tarafından diğer dosyaların da kontrol edilmesi gerekmektedir. Böylece saldırgan tarafından sisteme kötü amaçlı yazılımlar yüklenildiyse daha hızlı aksiyon almayı sağlayacaktır.

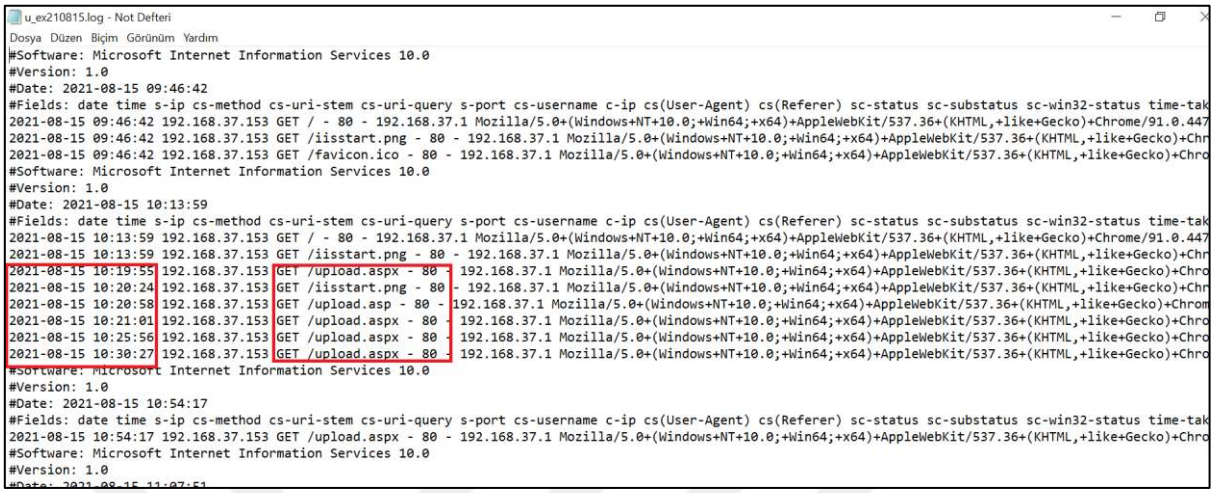
6.5. Sunucu Erişim Loglarının Analizi

Standart bir Windows sunucusu üzerinde IIS logları **"%SystemDrive%\inetpub\logs\LogFiles"** dizini altında tutulmaktadır. Oluşturulan sunucu üzerinde kaydedilen erişim logu elde edildikten sonra "C\inetpub\logs\LogFiles\W3SVC1" dizini altında not defteri ile açılabilecek dosyayı analiz ederek bir web Shell dosyasının sunucu üzerinde çalıştırılıp çalıştırılmadığı tespit edilmektedir.

Şekil 6.6.'de erişim loglarının dosya yolu gösterilmiştir.

Şekil 6.6. Log Dosyası Yolu

Oluşan log dosyası zamanına göre, dosya adında zaman bilgisi yer almaktadır. Şekil 6.7.'de log dosyası içeriği gösterilmiştir.



Şekil 6.7. Log Dosyası İçeriği

Bir web kabuğu dosyası sunucu üzerinde çalıştırıldığında sunucu erişim kayıtları içerisinde görüntülenebilmektedir.

6.6. Amcache Kayıtları Analizi

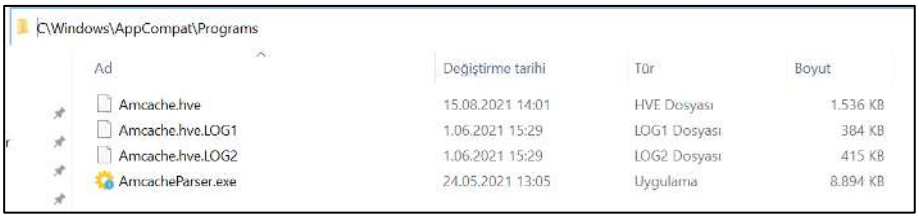
Web kabuğu saldırısı gerçekleştikten sonra kontrol edilmesi gereken bir başka sistem dosyası amcache dosyalarıdır.

Amcache.hve dosyası, çalıştırılabilir uygulamaların bilgilerini depolayan bir kayıt defteri dosyasıdır. Amcache'nin adli analizi hve dosyası, program adı ve sürümü, yürütme dosyası yolu, dosya boyutu, kurulum zaman damgası, ilk çalıştırma zaman damgası, yürütülebilir dosyanın hash bilgisi vb. gibi önemli verileri ortaya çıkarabilir [23]. Ancak, amcache tarafından toplanan bilgiler son derece faydalıdır ve izlerini silen saldırganlar tarafından kolayca gözden kaçırıldığı için bu dosya hakkında farkındalık eksikliği onu çok değerli kılmaktadır [24].

6.6.1. Amcache Kayıtlarının Elde Edilmesi

Amcache dosyası Windows işletim sistemlerinde iki farklı şekilde görüntülenmektedir. Windows 7 ve öncesi sistemlerde recentfile.bcf isimli dosya yer alırken; Windows 8 ve üzeri işletim sistemlerinde amcache.hve dosyası yer almaktadır.

Standart bir Windows sunucu üzerinde amcache.hve dosyası "**\%SystemRoot%\AppCompat\Programs\Amcache.hve"** dizini altında yer almaktadır.
Şekil 6.8.'de amcache dosyasının bulunduğu dizin gösterilmiştir.



Şekil 6.8. Amcache dosyası konumu

Amcacheparser.exe dosyası amcache.hve dosyası ile aynı konumda bulunmalıdır. Dizin içerisinde "**AmcacheParser.exe -f C:\Users\kevser\Desktop\2021-08-15T163326 _WEBSERVER\C\Windows\AppCompat\Programs\Amcache.hve –csv C:\Users\kevser\Desktop\2021-08-15T163326 _WEBSERVER\C\Windows\AppCompat\Programs\cikti.csv"** komutu girilerek amcache.hve dosyası ayrıştırma işlemi gerçekleştirilir.

Bir amcache dosyasının parse komutu işlemi Şekil 6.9.'da gösterilmiştir.

Şekil 6.9. Amcache dosyası ayrıştırma işlem komutu

Oluşan excel dosyası içeriği incelendiğinde makine üzerinde çalıştırılan, yürütülebilir dosyalar görüntülenmektedir. Saldırı sonrası makine üzerinde çalıştırılan ve indirilen dosyaların kayıtları analiz edildiğinde saldırganların kabuk dosyasını yükledikten sonra çalıştırdıkları komut dosyaları kayıtları görülmektedir.

Şekil 6.10.'da parse edilen amcache dosyasından elde edilen çalıştırılan uygulamaların listesi gösterilmiştir.

	A	B	C	D	
	FileKeyLastWriteTimestam	SHA1	FullPath	Name	FileExtension
	15.08.2021 12:34	8c5437cd76a89ec98	c:\windows\system32\cmd.exe	cmd.exe	.exe
	23.06.2021 02:38	6cbce4a295c163791	c:\windows\system32\windowspowershell\v1.0\powershell.exe	powershell.exe	.exe

Şekil 2 Amcache dosyası çıktısı

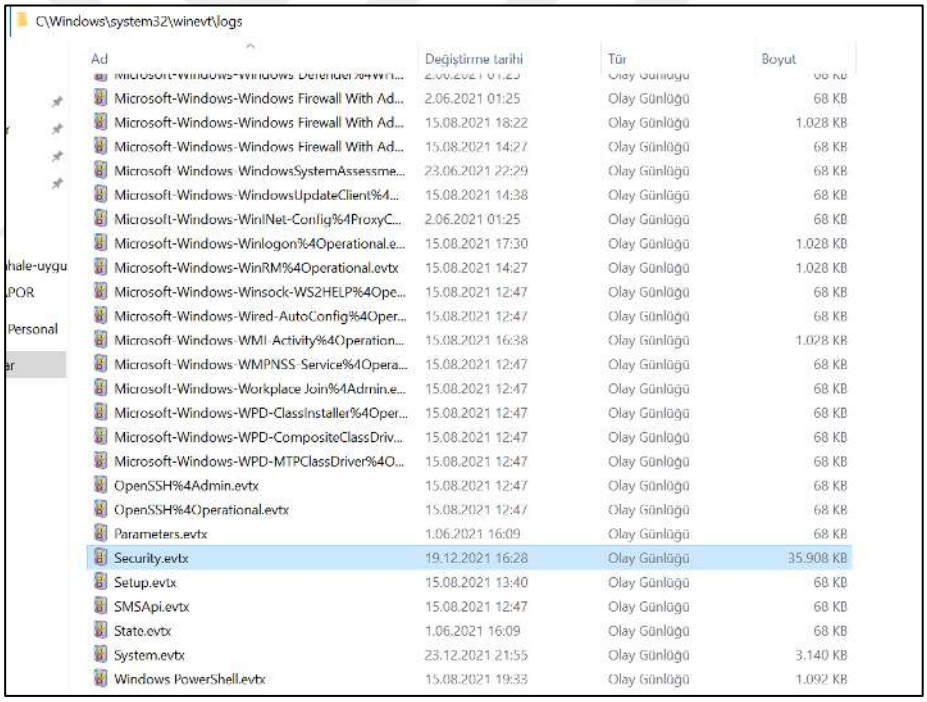
6.7. Güvenlik (Security) Loglarının Analizi

Bir sistem üzerinde güvenlik ihlalinin önlenebilmesi ve sistem güvenliğinin devam edebilmesi için olay günlüklerinin sürekli izlenmesi ve analizi gerekmektedir. Microsoft

Windows işletim sistemleri (OS'ler), sistem sorunlarının teşhis edilmesine ve sistemin optimize edilmesini ve güvenliğinin sağlanmasına yardımcı olabilecek günlüğe kaydetme özelliklerine sahiptir [25].

Kötü amaçlı yazılım bulaşması sırasında yeni bir hizmet veya yeni hesapların oluşturulması da dahil olmak üzere Windows Olay günlüklerinde yakalanabilir. Windows Olay günlükleri, Log Parser 8 ve Event Log Explorer 9 gibi araçlar kullanılarak incelenebilmektedir [26]. Saldırganın sunucu üzerine web kabuğunu yükledikten sonra sunucuda çalıştırılan komutları ve çalıştırılabilir dosyaların analiz edilmesi gerekir. Olay günlüğü üzerinde yer alan 4688 logu bir program çalıştığında, yeni işlem oluşturulduğunda, programın kim olarak çalıştığını ve başlatan süreci işlemektedir. 4688 yeni işlem oluşma logu, Windows işletim sistemlerinde security log dosyası altına kaydedilmektedir. Security.evtx log dosyası "C:\windows\system32\winevt\Logs" dizini altında depolanmaktadır.

Şekil 6.11.'de Security.evtx dosyasının konumunu göstermektedir.



Şekil 6.11. Security.evtx Dosya Konumu

Dosyanın analizi birden farklı şekilde yapılabilir. Ancak burada incelemesi yapılacak event id değeri belli olduğu için security.evtx dosyası parse edilmeden direk açılır.

Security.evtx log dosyası içeriğinde yer alan olay kimliği bilgileri ve detayları Tablo 6.1., Tablo 6.2., Tablo 6.3. ve Tablo 6.4.'de gösterilmiştir.

Tablo 6.1. Security.evtx Log Dosyası İçeriğinde Yer alan Olay Kimlikleri

Dosya ve Ağ Erişimleri ile Proses Aktivitelerine İlişkin Event ID'ler	
Olay Kimliği	**Açıklama**
1102	Silinen Loglar
4688	Oluşturulan İşlemler/Çalıştırılan Programlar
4656	Erişilen Dosyalar ya da Nesneye Yapılan İstekler
4663	Bir nesneye erişim girişiminde bulunuldu.
4658	Bir dosya veya nesneye erişim kapatıldı.(Dosyadan çıkış sağlandı)
4697	Yeni servis yüklendi.
4782	Bir Hesabın Şifre Karmasına Erişildi.
5140	Ağ Paylaşımı Nesnesine erişildi.

Tablo 6.2. Security.evtx Log Dosyası İçeriğinde Yer alan Olay Kimlikleri

Oturum Açma/Kapama Aktivitelerine İlişkin Event ID'ler	
Olay Kimliği	**Açıklama**
4624	Başarılı hesap açma girişi
4625	Başarısız hesap açma girişimi
4634	Oturumu kapatılan hesaplar
4648	Belirli kimlik bilgileri kullanılarak oturum açılmaya çalışıldı
4672	Yönetici hesabı ile giriş yapıldı
4776	Etki alanı denetleyicisi bir hesabın kimlik bilgilerini doğrulamaya çalıştı.
4778	Oturuma Yeniden Bağlanma (RDP veya FastUser Switch)
4770	Kerberos bileti yenilendi.
4793	Parola Politikası Kontrol API'sı çağrıldı

Tablo 6.3. Security.evtx Log Dosyası İçeriğinde Yer alan Olay Kimlikleri

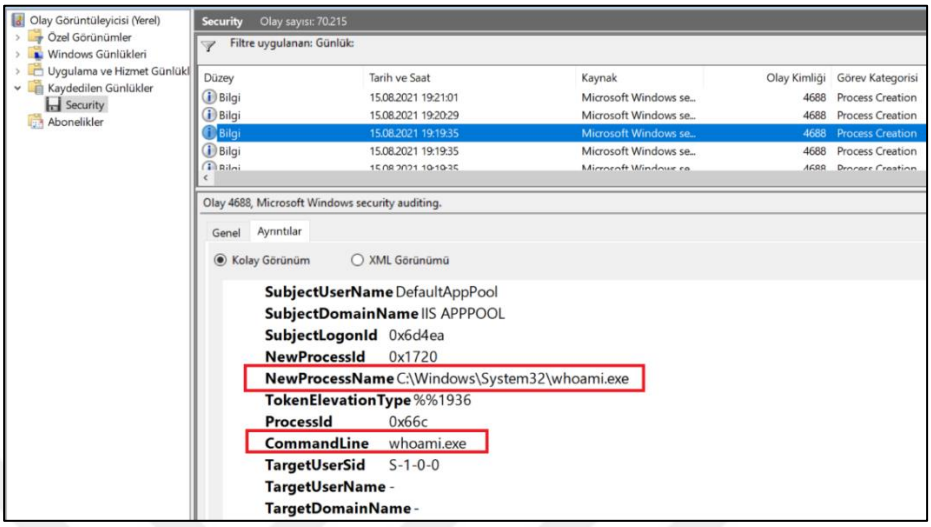
Kullanıcı Hesapları İle İlgili Aktivitelerine İlişkin Event ID'ler	
Olay Kimliği	**Açıklama**
4704	Kullanıcı Hakkı Atandı
4720	Yeni Kullanıcı Hesabı Oluşturuldu
4722	Yeni Kullanıcı Hesabı Etkinleştirildi
4725	Bir kullanıcı hesabı devre dışı bırakıldı
4726	Bir kullanıcı hesabı silindi
4728	Bir üye global gruba eklendi
4731	Güvenliği etkinleştirilmiş bir yerel grup oluşturuldu
4732	Bir üye yerel gruba eklendi
4733	Bir hesap yerel güvenlik grubundan kaldırıldı
4765	SID geçmişi bir hesaba eklendi
4634	Yerel grup silindi
4735	Yerel Grup değiştirildi
4740	Hesap kilitlendi
4748	Yerel grup silindi
4756	Bir üye evrensel gruba eklendi
4766	Bir hesaba SID geçmişi ekleme denemesi başarısız oldu
4767	Bir kullanıcı hesabının kilidi açıldı
4781	Hesap adı değiştirildi

Tablo 6.4. Security.evtx Log Dosyası İçeriğinde Yer alan Olay Kimlikleri

Firewall'da Yapılan Değişikliklere İlişkin Event ID'ler	
Olay Kimliği	**Açıklama**
4946	Güvenlik duvarı kuralı eklendi
4947	Windows güvenlik duvarı listesinde bir değişiklik yapıldı. Bir kural değiştirildi.
4948	Güvenlik duvarı kuralı silindi
4950	Bir Windows güvenlik duvarı ayarı değişti

Web kabuğu saldırısı gerçekleştikten sonra sunucu üzerinde meydana gelen yeni işlem oluşma ve çalıştırılabilir kayıtların analizi için 4688 logu analiz edilir. Saldırganın sunucu

üzerinde çalıştırdığı, sistem bilgisini öğrenmek amacıyla whoami parametresi ve buna benzer kullandığı komut dizeleri tespit edilir. Şekil 6.12.'de örnek bir log içeriği gösterilmiştir.



Şekil 6.12. Security.evtx dosyası 4688 log içeriği

6.8. Kalıcılık Mekanizmalarının Kontrolü

Bir sunucuya kurulduktan sonra, web sheller bir kuruluşta kalıcılığın en etkili yollarından biri olarak hizmet eder. Web shellerin yalnızca kalıcılık mekanizması olarak kullanıldığı durumlar görülmektedir. Web sheller, güvenliği ihlal edilmiş bir ağda bir arka kapının var olduğunu garanti eder, çünkü saldırgan bir sunucuda başlangıç noktası kurduktan sonra kötü niyetli bir iz bırakır. Web sheller tespit edilmezse, saldırganların erişimleri olan ağlardan veri toplamaya ve bu ağlardan para kazanmaya devam etmeleri için bir yol sağlar.

Ele geçirilen sistemi kurtarmak için, saldırganın kalıcılık mekanizmalarını bulup kaldırmadan başarılı ve kalıcı olamaz. Güvenliği ihlal edilmiş sistemi yeniden inşa etmek iyi bir çözüm olsa da mevcut varlıkları geri yüklemek bazen tek uygun seçenek olabilmektedir. Bu nedenle, tüm arka kapıları bulmak ve kaldırmak, ele geçirilen sistemi kurtarmanın kritik bir yönüdür [2].

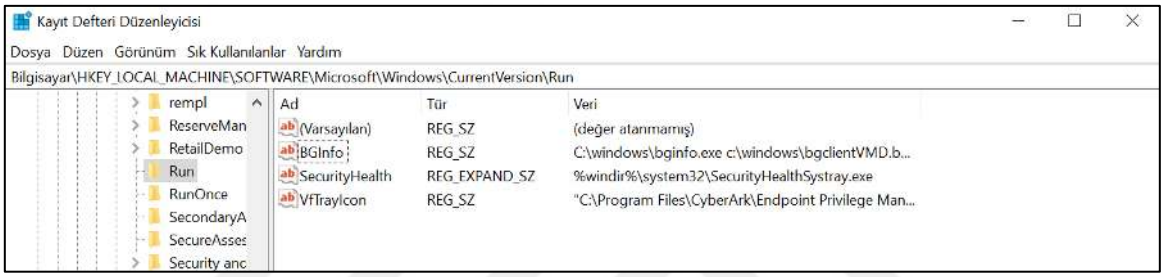
Saldırganlar, sistem üzerine erişim sağladıktan sonra o sistem üzerinde uzun süre kalabilmek isterler. Bunun içinde zamanlanmış görevler oluşturarak sistemde kalıcılık (persistence) sağlayabilirler. Web shell atılan bir sistemde saldırganın sistem her yeniden başladığında tekrardan kalıcılığını sağlayabileceği arka kapılar bırakıp bırakmadığının kontrolü sağlanmalıdır. Kalıcılık mekanizmalarının kontrolü için WMI, Autorun durumlarının kontrolü yapılmalıdır.

Bu başlıklar altında kalıcılık mekanizmalarının analizi anlatılacaktır.

6.8.1. Autorun Kontrolü

Autorun, bilgisayar açıldığında otomatik olarak çalışan uygulamalardır. Otomatik başlatma durumları hakkında en kapsamlı kayıtların yer aldığı bu yardımcı program, sistem açılışı veya oturum açma sırasında hangi programların çalışacak şekilde yapılandırıldığını göstermektedir. Autorun ile sistem üzerine eklenmiş üçüncü taraf otomatik başlayan programlar tespit edilebilir.

Sistem üzerinde herhangi bir araç yardımı olmadan manuel olarak, eklenen kayıtlar **"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"** dizininden kontrol edilebilir. Saldırgan sistem üzerinde kalıcılık sağlamak için sistemin her açılışında otomatik olarak başlatacağı uygulamaların belirlendiği kayıt bölümünde değişiklikler yapabilir. Autorun kayıtlarının yer aldığı dizin Şekil 6.13.'de gösterilmiştir.



Şekil 3 Autorun Dosya Yolu

6.8.2. WMI Kontrolü

WMI (Windows Management Instrumentation); Windows işletim sistemlerinde hemen hemen her nesnenin kontrol edilebilmesini sağlayan, işletim sistemindeki operasyonları ve yönetim işlevlerini gerçekleştirebilen bir teknolojidir. Tüm bu işleri bünyesindeki 900'e yakın sınıf sayesinde gerçekleştirebilir. Bu sınıfların her birinde çeşitli amaçlara yönelik olarak hazırlanmış fonksiyonlar bulunmaktadır.

Windows üzerinde program geliştiren (script) kişiler tarafından WMI sınıfları sıklıkla kullanılır. WMI kullanan uygulamalar C, C++, C#, VB gibi programlama dilleri ya da Windows derleyicisine sahip betik dilleri (scripting languages) ile geliştirilebilir [27]. WMI, bilgisayardaki uygulamaların sistem hakkında bilgi edinmesini kontrol eden bir işlemdir.

WMI ile;

- Olay görüntüleyicisindeki (event viewer) kayıtları sorgulama,
- Bilgisayardaki bir processi başlatma,
- Bilgisayarı yeniden başlatabilme gibi işlemler uzaktan yapılabilmektedir.

Bilgisayarınızdaki diğer uygulamaların sisteminiz hakkında bilgi edinmesini kontrol eden bir işlemdir. WMI sistem yöneticilerinin, görevleri yerinden veya uzaktan gerçekleştirmesini

sağlar. Bir saldırgan WMI'ı kalıcılık, yanal hareket, kod yürütme ve komuta ve kontrol gibi çeşitli faaliyetleri gerçekleştirmek için kullanabilir.

WMI Debug Log ile herhangi bir uygulamanın, sunucu veya istemci sistem üzerinden hangi wmi sorgusunu çalıştırdığı ve bu sorgu hata ile sonuçlandı ise alınan hatanın ayrıntısı görüntülenebilmektedir. Bu özellik aktifleştirilerek WMI kayıtları üzerinde kontrol gerçekleştirilebilinir.

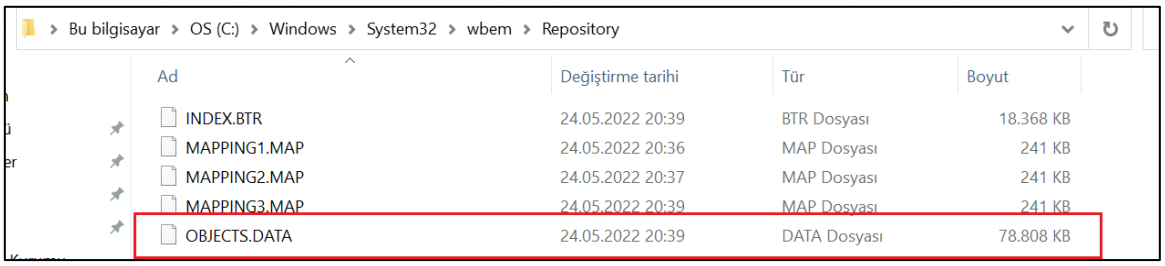
Kaydedilen log dosyası "C:\Windows\System32\wbem\Logs" dizini altından kontrol edilebilinir.

Windows sistemler üzerinde WMI tarafından yönetilen nesnelerin kontrolü için kaydedilen "objects.data" dosyası yer almaktadır. Kalıcılık mekanizmaları içerisinde OBJECTS.DATA dosyasının analizi anlatılacaktır.

6.8.2.1. OBJECTS.DATA Kayıtlarının Analiz Edilmesi

Windows sistemler üzerinde WMI tarafından yönetilen nesnelerin kontrolü için kaydedilen "objects.data" dosyası yer almaktadır. Bir web shell saldırısı sonrası sistem üzerinde çalıştırılan kayıtların kontrolü için "C:\Windows\System32\wbem\Repository" dizini altında OBJECTS.DATA dosyası yer almaktadır.

Objects.data dosyasının konumu Şekil 6.14.'de gösterilmiştir.



Şekil 6.14. Objects.data Dosya Konumu

OBJECTS.DATA dosyası açık kaynak olarak yayınlanan WMI_Forensics isimli araç yardımı ile parse edilebilmektedir.

Cmd.exe ile CCM_RUA_Finder.py -i path\to\OBJECTS.DATA -o path\to\output.xls komutu çalıştırılarak, çıkan .xls dosyası incelenir. Çalıştırılan komut çıktısı Şekil 6.15.'de gösterilmiştir.

```
C:\Users\[redacted]\Desktop\TOOLS\WMI_Forensics-master>CCM_RUA_Finder.py -i C:\Users\[redacted]\Desktop\TOOLS\WMI_Forensics-mast
er\OBJECTS.DATA -o C:\Users\[redacted]\Desktop\TOOLS\WMI_Forensics-master\cikti.xls
```

Şekil 6.15. Objects.data dosyası parse işlem komutu

7. SONUÇLAR

İnternete açık sunucularda görünürlük kazanmak, web kabukları tehdidini tespit etmek ve ele almak için çok önemlidir. Günümüzde artan siber saldırılarda saldırganın büyük kamu ve kuruluşlarına yaptığı tehdit faktörleri artmaktadır. Bu tez çalışmasında bir saldırı yöntemi olan web shell'in bir sistem üzerine yüklenmesi, yüklenen sistem üzerinde sağlayabildiği avantaj ve ayrıcalıklar, sistem üzerine yüklenildikten sonra tespit etmek için yapılan analiz çalışmaları aktarılmıştır. Bu çalışma ile saldırganın sistem üzerinde yayılmasını ve daha büyük hasar kaybını önlemek için hızlı sürede aksiyon alma ve tespit etme adımlarına değinilmiştir.

Bu adımlar da;

- Shell dosyası tespit edildikten sonra elde edilen komut dosyasının atılan sisteme özel olarak mı yazıldığı ya da yaygın kullanılan bir zararlı yazılım olup olmadığının kontrolü için farklı kaynaklardan sorgulamaları yapılmıştır.
- Saldırgan bir sistem üzerine web shell komut dosyasını attıktan sonra, oluşturma zamanı ve aynı zaman aralığında farklı zararlı yazılımların yüklenip yüklenmediğinin kontrolü yapılmıştır.
- Web Shell atılan sistemde, saldırganın erişim kazanıp kazanmadığının kontrolü için sunucu erişim loglarının analizi sağlanmıştır.
- Analiz sırasında amcache çalıştırılabilir sistem kayıtları kontrol edilerek saldırganın sistem üzerinde erişim elde ettikten sonra çalıştırdığı uygulamalar görüntülenmiştir.
- Amcache kayıtlarının yanısıra security loglarıda kontrol edilerek uygulama içerisinde çalıştırılan komutlar görülmüştür.
- Saldırganın makine üzerine erişim sağladıktan sonra uzun süre kalabilmesi için sistem üzerinde bazı değişiklikler yapması gerekmektedir. Bunun için Windows sistemler üzerinde kalıcılık mekanizması oluşturup oluşturmadığının analizleri sağlanmıştır.

Literatürde yer alan veriler genellikle bir saldırının keşif aşamalarını kapsamakta ve bir saldırı özelinde yapılacak adımları içermemektedir. Bu tez çalışmasında bir saldırı özelinde sistem üzerinde incelenmesi gereken önemli noktalar toplu olarak vurgulanmıştır.

ÖNERİLER

Saldırgan bir Web shell'i halihazırda güvenliği ihlal edilmiş bir web uygulamasına kalıcılık erişimi sağlamak ve sürdürmek için yükler. Bir web kabuğunun kendisi uzaktaki bir güvenlik açığına saldıramaz veya bunlardan yararlanamaz, bu nedenle her zaman bir saldırının ikinci adımıdır.

IIS ve işletim sistemleri üzerindeki güvenlik yamaları, SQL kaynaklı veritabanı saldırılarına yönelik tedbirler ve diğer güvenlik önlemlerinin kombinasyonu, web sitesini daha güvenli hale getirecektir.

Saldırılara karşı riskleri daha aza indirmek için web uygulamaları güncel tutulmalıdır. Herhangi bir zafiyet açıklığına karşılık güvenlik açığı taramaları yapılarak sistemlerdeki güvenlik açıkları araştırılmalıdır. Web sunucuları izlenmeli ve web sunucusu tarafından sunucu üzerine yeni bir komut dosyası bırakıldığında alarmları etkinleştirilmelidir. Web shell saldırılarından korunmak için dosya bütünlüğü izleme çözümleri, web'den erişilebilen dizinlerdeki dosya değişikliklerini engellemek için tasarlanmıştır. Bir değişiklik algılandığında, güvenlik personelini uyarır.

Web uygulamaları için izinler tanımlarken, en az ayrıcalık kavramını kullanmak önemlidir.

En az ayrıcalık ilkesi, tehdit aktörlerinin savunmasız uygulamalara bir web kabuğu yüklemesini önlemeye yardımcı olabilir. Web uygulamalarının doğrudan web'den erişilebilen bir dizine yazmasına veya web'den erişilebilen kodu değiştirmesine izin vermeyerek bunu ayarlayabilirsiniz. Bu şekilde sunucu üzerine saldırganın erişmesini engeller.

İzinsiz giriş önleme sistemi (IPS), ağ trafiği akışını izleyerek tehditlere karşı korumak için tasarlanmış bir ağ güvenliği teknolojisidir. Web uygulaması güvenlik duvarları (WAF), web servislerine giden ve gelen HTTP trafiğini filtreleyerek, izleyerek ve engelleyerek tehditlere karşı koruma sağlar. IPS ve WAF çözümlerinin her biri trafik akışını izleyebilir ve bilinen kötü amaçlı yüklemeleri engelleyebilir.

Belirli uç nokta algılama ve yanıt (EDR) çözümleri, web kabuğu saldırılarına karşı korumaya yardımcı olmaktadırlar. Bu çözümler, makine aktivitelerini izler ve anormallikleri işler. EDR çözümleri web shelleri tespit etmede çok önemli rol oynamaktadır.

Oluşabilecek tehditleri ve 0-day açıklıklarını erken aşamada algılayan, güvenlik çözüm ürünleri kullanılmalıdır.

Güvenlik yamaları güncel tutularak APT saldırganlarının yararlanabileceği güvenlik açıkları kontrol altında tutulabilir.

Kuruluşun en değerli varlıklarını belirleyin: Bu şekilde kuruluş içerisindeki, en çekici hedefler korunabilir.

KAYNAKLAR

[1] URL-1, https://www.sans.org/cyber-security-courses/windows-forensic-analysis/, Erişim 19 Haziran 2022.

[2] URL-2, https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/, Erişim 19 Haziran 2022.

[3] Xu Mingkun, Chen Xi Hu Yan., Wentz, Design of Software to Search ASP Web Shell, 2012. https://ur.booksc.me/book/20211929/4fdd60.

[4] URL-3, https://www.cisa.gov/uscert/ncas/alerts/TA15-314A, Erişim 19 Haziran 2022.

[5] URL-4, https://null-byte.wonderhowto.com/how-to/use-sql-injection-run-os-commands-get-shell-0191405/, Erişim 19 Haziran 2022.

[6] URL-5, https://yakupseker.medium.com/sqlmap-nedir-nas%C4%B1l-kullan%C4%B1l%C4%B1r-e1b4a961aae2, Erişim 19 Haziran 2022.

[7] URL-6, https://nuriyavuz2-71.medium.com/local-file-inclusion-ve-remote-file-inclusion-f6d0ef2486a4, Erişim 19 Haziran 2022.

[8] URL-7, https://www.siberguvenlik.web.tr/index.php/2021/02/10/aptadvanced-persistent-threat-nedir/, Erişim 19 Haziran 2022

[9] URL-8, https://www.netes.com.tr/blog/buyuyen-tehdit-apt-gruplari, Erişim 19 Haziran 2022

[10] URL-9, https://ramazankoyuturk.medium.com/apt-advanced-persistent-threats-gruplar%C4%B1-nedir-a752c75d4d0a, Erişim 19 Haziran 2022

[11] URL-10, https://www.beyaz.net/tr/guvenlik/makaleler/zeroday_nedir.html, Erişim 19 Haziran 2022

[12] URL-11, https://www.darkreading.com/attacks-breaches/inside-the-web-shell-used-in-the-microsoft-exchange-server-attacks/d/d-id/1340498, Erişim 19 Haziran 2022

[13] URL-12, https://www.acunetix.com/blog/articles/introduction-web-shells-part-1, Erişim 19 Haziran 2022

[14] URL-13, https://en.wikipedia.org/wiki/China_Chopper, Erişim 19 Haziran 2022

[15] URL-14, https://www.trinitycyber.com/hubfs/CTA%20PDFs%20(threat%20briefs,%20data%20sheet,%20case%20study)/3_TC_ThreatBrief_TwoFace_v2.pdf, Erişim 19 Haziran 2022

[16] URL-15, https://unit42.paloaltonetworks.com/unit42-twoface-webshell-persistent-access-point-lateral-movement/, Erişim 19 Haziran 2022

[17] URL-16, https://tr.wikipedia.org/wiki/Internet_Information_Services, Erişim 19 Haziran 2022

[18] URL-17, https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF, Erişim 19 Haziran 2022

[19] URL-18, https://github.com/nsacyber/Mitigating-Web-Shells/blob/master/README.md#detecting-blocking-web-shells, Erişim 19 Haziran 2022

[20] URL-19, https://www.bgasecurity.com/2019/05/siber-tehdit-istihbarati-nedir-bolum-1, Erişim 19 Haziran 2022

[21] Uçar, A., Wındows İşletım Sıstemı Kalıntılarının Analızını Gerçekleştıren Sıber Olay Müdahale Aracının Gelıştırılmesı Ve Olay Zaman Çızelgesının Çıkarılması, 2021. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

[22] URL-20, https://forensicswiki.xyz/wiki/index.php?title=$MFT, Erişim 19 Haziran 2022[23] URL-21, https://andreafortuna.org/2017/10/16/amcache-and-shimcache-in-forensic-analysis/, Erişim 19 Haziran 2022

[24] URL-22, https://www.ssi.gouv.fr/uploads/2019/01/anssi-coriin_2019-analysis_amcache.pdf, Erişim 19 Haziran 2022

[25] Giuseppini, G. ve Burnett, M., Microsoft Log Parser Toolkit,Syngress Press, (2005).

[26] Malin, C., Casey, E., Aquilina, J. , Malware Forensics Field Guide for Windows Systems, Syngress Press, (2021).

[27] URL-23, https://www.mshowto.org/wmi-nedir-sorgu-ve-test-araclari-nelerdir.html, Erişim 19 Haziran 2022

ÖZGEÇMİŞ

Kevser Mehveş DAĞCI

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]