



# Olay Müdahale

Kullanım Kılavuzu



## İçindekiler

1. Olay Müdahale Nedir?	3
1.1 Şüpheli E-postalar	4
1.1.1 Raporlanan	4
1.1.3 Temiz	23
1.1.2 Oltalama	24
1.1.3 Spam	25
1.1.4 Bilinmeyen	26
1.2 Kurallar	27
1.3. Etiketler	28
1.4. Aksiyonlar	30
1.5. Saptama	33
1.6. Panel	34
1.7. Ayarlar	35
1.7.1 Yönetim Paneli	35
1.7.2 SMTP Ayarları	37
1.7.3 E-Posta Şablonları	38
1.7.4 İçerik Güncelleme	39
1.7.5 Syslog Sunucuları	40
1.7.6 Yetkilendirme	41
1.7.7. Virüs Total	43
1.7.8. Plugin Yönetimi	44
1.7.9. Lisans Yönetimi	46
1.7.10. SpamAssassin Yönetimi	47
1.7.11. Veri Saklama Yöntemi	48
1.7.12. İtibar İstatistikleri	49
1.7.13. Roksit DNS API Yönetimi	50
1.7.14. LDAP Ayarları	51
1.7.15. Check Phish	52
1.7.16. WhileList	53
1.7.17. API Konfigürasyon Yönetimi	54
1.7.18. Parola Politikası	55



## 1. Olay Müdahale Nedir?

IT ekibinin, çalışanlar tarafından bildirilen potansiyel olarak zararlı e-postalara öncelik vermesine ve yönetmesine yardımcı olan ek bir üründür. E-posta tehditleri; hızlı bir şekilde tanımlanmakta ve yanıtlanmaktadır.

### 1. Outlook

The screenshot shows the Microsoft Outlook inbox. A blue box highlights the top right corner of the interface, specifically the 'Phishing Report' button. Another blue box highlights the body of an email from 'Google <no-reply@accounts.google.com>' with the subject 'Önemli güvenlik uyarısı'. The email content includes a warning about a login attempt and a link to 'hande.alp@beamteknoloji.com'. Below the email, a message box displays the text 'Oturum açma girişimi engellendi' with a link to the same URL.

Şüpheli e-postaya tıklayın, ekranın sağ üst konumunda Phishing Report Plugin butonu aktif olacaktır. Bu plugin butonu, şüpheli e-posta olarak belirlenen e-postayı analiz edilmesi için olay müdahale uygulamasına iletilecektir.

\*Raporlanan e-posta otomatik olarak çöp kutusuna gönderilecektir.



## 1.1 Şüpheli E-postalar

RS	Gönderici	Konu	Alan Adı	Gönderilme Tarihi	Raporlayan	Raporlanma Tarihi	Etiketler
1	gorhem.saka@beamteknoloji.com	test	beamteknoloji.com	12.08.2020 15:03:23	hal.kas@beamteknoloji.com	12.08.2020 15:03:38	YALI SPAM, SPAM, VT-CLEAN, SA SPAM, VT-CLEAN
1	no-reply@microsoft.com	Bugün: Bayindr Hastanesi Oltala Sunum #	microsoft.com	11.08.2020 13:06:06	beamyigit@outlook.com	12.08.2020 14:01:09	VT-CLEAN
1	edible-history-space@quora.com	Forgotten dessert	quora.com	10.08.2020 22:26:59	hande.alp@beamteknoloji.com	12.08.2020 15:51:04	VT-CLEAN
1	do-not-reply@trello.com	EMRE CAKIR added you to the card. İdap giriş başarısız olursa login e atıyor, İdap login e alırın. on OLTALA YENİ PROJE.	trello.com	11.08.2020 18:03:58	hal.kas@beamteknoloji.com	12.08.2020 13:09:53	VT-CLEAN
1	digest-noreply@quora.com	Which PHP framework is better, Laravel or CodeIgniter?	quora.com	09.08.2020 15:09:28	hande.alp@beamteknoloji.com	12.08.2020 11:54:06	VT-CLEAN
1	beamyigit@outlook.com	Şüpheli E-posta içeriği	outlook.com	12.08.2020 10:56:11	beamyigit@outlook.com	12.08.2020 11:14:21	CP-PHISH, VT-MALICIOUS
1	beamyigit@outlook.com	2. azı	outlook.com	12.08.2020 10:16:57	beamyigit@outlook.com	12.08.2020 10:19:06	CP-PHISH, BLACKLISTED, VT-MALICIOUS
1	beamyigit@outlook.com	2. çoklu	outlook.com	12.08.2020 10:18:27	beamyigit@outlook.com	12.08.2020 10:18:52	CP-PHISH, VT-MALICIOUS
1	beamyigit@outlook.com	sdagdasgdasg	outlook.com	12.08.2020 10:18:55	beamyigit@outlook.com	12.08.2020 10:11:06	CP-PHISH, BLACKLISTED, VT-MALICIOUS
1	beamyigit@outlook.com	sdgasdgdasg	outlook.com	12.08.2020 10:18:28	beamyigit@outlook.com	12.08.2020 10:03:33	CP-PHISH, VT-MALICIOUS
1	beamyigit@outlook.com	asdgdasgasd	outlook.com	12.08.2020 10:00:19	beamyigit@outlook.com	12.08.2020 10:00:33	CP-PHISH, VT-MALICIOUS

1.1.1 **Raporlanan** ekranı, e-posta uygulamasından “Phishing Report” olarak işaretlenmiş e-postaların uygulamada bulunduğu ekranıdır.

**Grupla** seçeneği ile şüpheli e-postalar başlığında bulunan tüm e-postalar; **Gönderici**, **Alan Adı**, **Konu**, **Ekli Dosya** ya da **Tamamı** seçeneği ile gruplayın. Örn:

Grupla :

Gönderici    Alan Adı    Konu    Ekli Dosya    Tamamı

google.com - 4

techrepublic.online.com - 3

gartner.com - 1

euromsg.net - 1

vyond.com - 1

mightydeals.com - 1

webdesignernews.com - 1

Cift tıklayarak e-postanın detaylı analizi yapın.



\*Şüpheli e-posta analizinde, Analiz ve Detaylı Analiz & Aksiyon başlıklarında inceleyin.

The screenshot shows the 'Analiz' tab selected in the top navigation bar. The main content area displays various analysis results and statistics. Key sections include:

- E-posta bilgileri:** Shows sender (Gönderici), recipient (Yanlış adresi), subject (Gönderen Konusu), and analysis status (Analiz Tamamlandı).
- URL:** Shows URL analysis with 1 URL found, 1 client, and 1 file type (txt).
- Raporlama bilgileri:** Shows reporter information (ahmed.sensi@beamteknoloj.com), report date (06.11.2020 23:58:47), and total reporter count (1).
- Oltala Skor:** Score of 15 with a note: "Yeniden yönlendirilen URL içeriyor" (20 Puan).
- Spam Assasian Skor:** Score of -0.5 with a note: "ALL\_TRUSTED / URL\_NOVOWEL".
- Gönderici Analizi:** Compares sender information across various sources like Virus Total, Alien Vault OTX, Blacklist, URLhaus, and CyThreat.
- URL Analizi:** Compares URLs across Virus Total, PhishTank, Check Phish, and URLhaus.
- Ekli dosya analizi:** Compares attachments across Virus Total, Alien Vault OTX, URLhaus, and CyThreat.

**Analiz Ekranı:** e-posta için yapılan analizlerin özet bilgilerinin bulunduğu ekranıdır.

E-posta bilgilerinin içeriğinin bulunduğu ve e-postanın geldiği mail adresi, kime gönderildiği, raporlayan bilgisi, e-posta içeriğinde link ya da eklienti olup olmadığı, e-postanın gönderildiği adresin alan adının oluşturulma, son güncelleme ve köken ve Blacklist kontrolü yapılmaktadır.

E-posta ile ilgili skor analizi yer almaktadır.

**1.Oltala Skor:** E-posta belirtilen kriterlere göre analiz edildikten sonra; bu analiz sonucuna göre bir not belirlenmektedir.

- Yeniden yönlendirilen URL içeriyor (**20 Puan**)
- Bağlantı görünülen adı gerçek bağlantıdan farklı (**15 Puan**)
- Gönderenden farklı alan adında URL içeriyor (**20 Puan**)
- Gönderenden farklı yanıt adresi (**15 Puan**)
- Alan adı yaşı 30 günden az (**30 Puan**)

**2. Spam Assasian Skor:** E-posta içeriği ve header özelinde, Spam Assasian Analiz ve Skorlama yapmaktadır.

**Ayarlar / SpamAssasian** Yönetim Paneli üzerinde belirlediğiniz skor değeri üzerinden otomatik olarak "**SA-SPAM**" etiketlemesi gerçekleşmektektir. Örn: THRESHOLD değeri "1" olarak atanırsa, e-posta analizinde SpamAssasian tarafından 1.0 ve üzeri gelen skorlarda otomatik olarak "**SA-SPAM**" etiketi atanmaktadır.

\*Spam Assasian skor düzenlenmesi ayarlar bölümünden yapılmaktadır. [Ayrıntılar için tıklayın.](#)



Gönderici analizi, varsa ekli dosya ve URL analizinin farklı analiz programlarında tespit edilen sonuçları verilmektedir.

- Tespit edilme işlemi tamamlandı ve bir bulgu var,
- Sunucudan veri gelmedi,
- Tespit edilme işlemi tamamlandı ve herhangi bir bulgu yok,
- Bulunduğu başlıkla ilgili herhangi bir içerik yok,
- Analiz programı ayarlar kısmından kapalı,
- Analiz daha tamamlanmadı,
- Servis ile ilgili hata var



Analiz Detayı analiz &amp; Aksiyon

**Detayı analiz & Aksiyon ekranı;** E-postanın güvenlik sistemleri tarafından detaylı olarak manuel inceleme, analiz ve analiz sonuçlandırma işlemlerinin yanında Plugin ve Saptama işlemlerinin yapıldığı ekrandır.

**1.1.1.1. Temel Analiz:** Raporlanan e-postanın; Ön izleme, Başlıklar, Orijinal Mesaj, Ekli Dosyalar, Eşleşen Kurallar ve Geçmiş başlıklar altında temel analiz sonuçları verilmektedir.

Received

from VIE1EURO02HT186.eop.EURO2.prod.protection.outlook.com (2603:10a6:800:92::20) by VIE194MB0893.EURP194.PROD.OUTLOOK.COM with HTTPS via VI1PRO501CA0010.EURPRD05.PROD.OUTLOOK.COM; Thu, 14 May 2020 11:23:58 +0000

ARC-Seal

i=2; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=pass; b=e5rZqN8l+mIWVCK048THXGMD/Q9Jchj8C900hlM8GbubVq0O03ICE/tI0ozRa2MXxzqZICSSGK...

ARC-Message-Signature

i=2; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com; s=arcselector9901; h=From;Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; bh=CzaCR0MyvFNAB24ZwdNzqtB9ntzSmWSAOxfofbJuRo=; b=Mxu842zPYE9xtET5wIA0zzCF7A16mhoTQFD6YnXzvFdRBUhPMHWIOwsWUk847ypo+EP/oRc9yt...

ARC-Authentication-Results

i=2; mx.microsoft.com l; **spf=pass** (sender ip is **40.92.67.19**) smtp.rcpttomain=outlook.com smtp.mailfrom=outlook.com; **dmarc=pass** (p=none sp=qarantine pct=100) action=none header.from=outlook.com; **dkim=pass** (signature was verified) header.d=outlook.com; arc=pass (O oda=0 Itd=1)

Authentication-Results

**spf=pass** (sender IP is **40.92.67.19**) smtp.mailfrom=outlook.com; outlook.com; **dkim=pass** (signature was verified) header.d=outlook.com; outlook.com; **dmarc=pass** action=none header.from=outlook.com; compauth=pass reason=l00

Received-SPF

Pass (protection.outlook.com: domain of outlook.com designates **40.92.67.19** as permitted sender receiver=protection.outlook.com; client-ip=**40.92.67.19**; helo=EURO2-AM5-obe.outbound.protection.outlook.com)

E-posta içeriğindeki header bilgilerinin analizini kolaylaştırmak amacıyla hazırlanan bölümdür. **IP, spf, dkim, dmarc** bilgilerinin kırmızı renk ile belirtilerek analiz sürecinde kullanıcıya kolaylık sağlamaası için sunulmuştur.



Temel Analiz ▾

On izleme Başlıklar Orijinal Mesaj Eşleşen Kurallar Geçmiş

"Delivered-To": "yigit@beamteknoloji.com",  
"Received": "by 2002a25b74d0:0:0:0 with SMTP id e13csp2696690ybmr; \n Sun, 26 Apr 2020 23:49:42 -0700 (PDT)",  
"X-Received": "by 2002a5b5cf: with SMTP id w1Smr31663968yb2p.2151587970181841; \n Sun, 26 Apr 2020 23:49:41 -0700 (PDT)",  
"ARC-Seal": "i=1; a=rsa-sha256; t=1587970184; cv=none;\n d=google.com; s=arc-20160816;\n b=HAKkbRS8E9wwx7He0qmpwcu0DsgX+IK3cSXQeXIL2OQaj3z6Qf0Nv6G4Hq4k;\n 5VvvuLc4D5eEgb9ynOmQ0jyrCeIkkfQ+QHRWb5tKXV8BPv5bn8enaweoPT97248sNV;\n MpQhInZ+6H54syUDNvUXHxplLq6KlQunQZ926vAbYntxxsD956u7dHSxQxofSe4;\n wYbVsVzMo+JFD3kUyBriwmkzballyyytgd++xtylg/G/hD55QSYTzDw/WpGhx;\n pzyGc/g3oL+5qBiUCHArz7Xrb+9+BInfN0bVpemn3YdGosVNsd2y7XSWTis99W;\n KEaw==",  
"ARC-Message-Signature": "i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;\n h=to:from:subject:message-id-list-unsubscribe:list-id:date;\n mime-version:dkim-signature;\n bh=SH987DoxcMdehBS2aXVaQh9tIK2ccU7fdJqwQ4rw=\n b=MvrtCztnx2LJ/UnBbf6gKzeNuB74418Mnfws6Grn+OZNToBWZCpmqsWbZ;\n M321ID-g4Lvo7MYTE0W5zVnbpPtus2XB0WeJ/ZeeXoDccAABhCqfYMTX2y;\n U3dQXVcAG090JHAU69nR9NNkee2nBmXpEc25anrDEkUOzakW5a/BkXcg1BKLu;\n 2W2SPC2RnPqUh6jAB5UFnTQ02ZH3g6l60fbwzBAtBPyOgU6yuNyCvSnlcItcp;\n IN49OzaZ4vVolv4D05vthBqL23wKRmhp5zO+yhCNy6dcsoJzXG3rlUgaTlNOD;\n L3Ug=",  
"ARC-Authentication-Results": "i=1; mx.google.com;\n dkim=pass header.i=@google.com\n headers=20161025\n header.b=-OIP/a2QP;\n spf=pass (google.com: domain of 3hycmxhqkabw8gg8d62d6jk-fjgj6hdq8gg8d6.4ge@alerts.bounces.google.com)\n dmarc=pass (p=REJECT sp=REJECT\n ds=NONE) header.from=google.com",\n :to:\n :=209.85.220.69;\n abw8gg8d62d6jk-fjgj6hdq8gg8d6.4ge@alerts.bounces.google.com\n sp=REJECT\n ds=NONE\n header.from=google.com",

Ön izleme başlığında görüntülenen e-posta içeriği, RAW formatında orijinal mesaj başlığında yer almaktadır.

Dosya Adı: log.txt  
Dosya Formatı: txt

DOWNLOAD

Temel Analiz ▾

On izleme Başlıklar Orijinal Mesaj Eski Dosyalar Eşleşen Kurallar Geçmiş

E-posta içeriğinde ekli dosya bulunuyorsa; dosya adı ve format bilisi, istenirse indirme işlemi bu başlıkta yapılmaktadır.

Analiz Detaylı analiz & Aksiyon

Temel Analiz ▾

On izleme Başlıklar Orijinal Mesaj Eski Dosyalar Eşleşen Kurallar Geçmiş

Adı: static rule\_1  
Etiketler: YARA\_SPAM\_1

Toplam kayitan 1 - arası gösterilmektedir.

Uygulamada, daha önceden oluşturulan kurallar ve o kurallara atanan etiketler ile herhangi bir eşleşme varsa bu başlık altında yer almaktadır.



## Şüpheli E-posta Sonuç &amp; Aksiyon;

**Etiketler** bölümünden etiket atamaktadır:

- *Önceden oluşturulan etiket,*
- *Yeni oluşturulan etiket.*

**Durumu** bölümünden e-posta durumu belirlenmektedir:

- Analiz edilen şüpheli e-postanın, “Raporlanan” durumundan başka bir duruma (Temiz, Oltalaması, Spam ve Bilinmeyen) atanması yapılmaktadır.  
*\* E-posta için durum seçimi yapılrken; panel ekranında bulunan grafiklere, seçilmiş olan duruma göre sonuçların yansıyacağı **unutulmamalıdır.** E-posta durumuna doğru karar verilmesi, sonuçlar için önemlidir.*

**Sonuç** bölümünden e-posta analizinin tamamlanıp/tamamlanmadığı kararı atanmaktadır.

- Analiz edilen e-postanın; incelenen analiz sonuçlarına göre analiz sürecinin sonuçlanıp sonuçlanmadığı durumunun ataması yapılmaktadır.  
*\* E-posta için sonuç seçimi yapılrken; panel ekranında bulunan grafiklere, seçilmiş olan sonuç bilgisine göre sonuçların yansıyacağı **unutulmamalıdır.** E-posta sonucuna doğru karar verilmesi, sonuçlar için önemlidir.*

**Aksiyon** bölümü:

- Manuel ve otomatik belirlenen aksiyonlar vardır. Otomatik belirlenen aksiyonlar; seçilen özelliklere göre e-posta analizi yapar ve bu özelliklerle eşleşme varsa belirlenen etiketi atar. Aksiyonlar kısmında belirlenen Manuel Tetikle seçenekinde olan bir aksiyon aktifse, burada gözükmür. Yapılan otomatik aksiyonun dışında, burada manuel aksiyon ataması yapılmaktadır.

**Saptama** bölümü:

- Şüpheli e-postanın detaylı analizinin ve aksiyonlarının belirlenebileceği ekrandır.



Plugin ve Exchange detayında; şüpheli e-posta göndereni ve konusu ile, eşleşen bütün Pluginler de işlemler yapılmaktadır.

The screenshot shows the 'Plugin' and 'Karantina' sections of the application. The 'Plugin' section has a blue circle around it, and the 'Karantina' section also has a blue circle around it. A red circle highlights the 'Durumu' (Status) button in the top right corner, which is labeled 'İşlem Tamamlandı' (Operation Completed) with a green checkmark. Below the sections are two smaller windows showing detailed information about specific emails.

### İşlemler:

**Plugin:** E-posta hesabında URL gizle/ göster, bayrak ekle ve e-posta silinmesi işlemleri ve bu işlemlerin takibinin yapılacağı ekrandır.

**Karantina:** Karantinaya alınan e-postalar ve çıkarılan e- postaların karantina işlemleri için karantinaya alma ve çıkış işlemleri takibinin yapılabileceği ekrandır.

**\*Karantina Nedir?** Karantinaya aldığınız bir e-posta, kullanıcı tarafından açılamaz, tıklanamaz ve görünmez. Bir e-posta için karantina işlemi yaptıysanız, şüpheli olan bir e-postayı saklama işlemi yapılmış demektir.

Bir aksiyon gerçekleştirildiğinde, pluginlerle konuşma süreci durumu belirler. İşlem devam ediyorsa, "**İşlem yapılıyor**" şeklinde durum bilgilendirmesi yapılmaktadır.

Hem durumu günceller hem de yeni bulunan ya da yeni yapılan işlemlerin görüntülenmesi için kullanımı **öneMLİDİR**.



**1.1.1.2. Virüs Total Analizi:** E-posta analizinin gönderici, link ve varsa ekleni başlıklarında analizi yapılmaktadır.

Gönderen alan adı sorusuna

Alan Adı: outlook.com  
IP Adresi: 40.92.67.9

Köken: US  
Webutation Güvenlik Skoru: 100  
Oluşturulma Tarihi: 9403 gün önce  
Son Güncelleme: 1400 gün önce

Gönderici   Link   Ekleni  

**WHOIS**  

Kayıt  
Admin City  
Admin Country  
Admin Email  
Admin Organization  
Admin Postal Code  
Admin State/Province  
Creation Date  
Creation Date  
DNSSEC  
Domain Name

**SON DNS KAYITLARI**  

Kayıt Türü	TTL	Deger
NS	0	ns1.msft.net
NS	0	ns4.msft.net
A	0	40.97153146
NS	0	ns21.o365filtering.com
A	0	40.9716150
A	0	40.97128194
NS	0	ns3.msft.net
TXT	0	v=spf1 include:spr-a.outlook.com include:spf-b.outlook.com ip4:157.55.91.28/25 include:spf.protection.outlook.com include:spf-a.hotmail.com include:_spf-ssg.b.microsoft.com include:_spf-ssg.c.microsoft.com -all
TXT	0	google-site-verification=0lLWhIMtxEkwWTFU4ursTr-_OvojaAOlr7PgtSEm

**TOPLULUK PASIF DNS ÇOGALTILMASI**  

SON COZUM  
2019-11-04 18:05:19  
2019-11-04 18:05:19  
2019-11-04 18:05:19  
2019-11-04 18:05:19  
2019-11-04 18:05:19  
2019-11-04 18:05:19  
Toplam 6 kayıtta 1 - 6 arası gösterilmektedir.

**ALT ALANLAR**  

ALT ALAN  
autodiscovery.yandex-team.com.tr  
autoconfig.yandex-team.com.tr

Toplam 2 kayıtta 1 - 2 arası gösterilmektedir.

**TESPIT EDİLEN YÖNLENDİRME ÖRNEKLERİ**  

TARAMA TARIHI	TESPİTLER	SHA256
2019-04-24 01:15:08	67/1	9137d70a36afb15165a5cfba31721e0fdebd5d1949d588940bf7df3100083a6a6
2019-03-30 05:03:44	68/1	769c4b9c855c1050e7070b6e33ed1bc2958cf19e29c0c6f5c092920ba74eb3
2019-02-20 00:39:29	70/2	e72c94af9a9alc719161e4fa79441d3235c1cd68c90dc6267b3ac4bab2690fb6
2018-12-19 07:12:53	70/1	5fad31a392d9f07977fd1144a73fbdb8abaa66c7ff53d928452ca83467fb7
2018-12-07 17:39:49	70/1	fd015d6a40fd6c3a518663e992ad7614123cbde151dcc914903528b4ebd5e22
2018-11-11 23:07:42	67/2	fce02b14c390544377363ab08a0ff0bbcf9b67adf4844a8b8le662de070f68d2
2018-09-24 12:38:42	69/1	0731f96c2b5aed7a54d4b82cfe5a12aeed31aa6592807fc9379512c3701cc8
2018-09-23 06:38:21	70/1	0ccbbe81d43d4b478d1529178984fb885c9cf4524111ebbd9957f939ffdd5
2018-07-22 05:52:49	69/1	b3ba591365db5b54ab9cdee71b80d10a678bc6d28ffd885c197fe66c7d5afe25

Toplam 9 kayıtta 1 - 9 arası gösterilmektedir.



Gönderici Link Ekleni

Alan Adı: [tkdtosanacademy.ir](http://tkdtosanacademy.ir)  
Link: <http://tkdtosanacademy.ir/dir>

Alan Adı: [gemstats1.com](http://www.gemstats1.com)  
Link: <http://www.gemstats1.com>

Analizi Yenile  
Sonuç

Analizi Yenile  
Sonuç

E-posta içerisindeki linklerin analizi yapılarak; herhangi bir bulgu varsa **ünləm simbolü** ile gösterilir ve **“Sonuç”** butonu aktif hale gelerek, detaylı analiz işlemi yapın.

Virus Total Analizi

Alan Adı: [tkdtosanacademy.ir](http://tkdtosanacademy.ir)

Sunucu Adı: [tkdtosanacademy.ir](http://tkdtosanacademy.ir)

Toplam Tarama: 80

Tespit: 15

Gönderici Link Ekleni

URL Alan Adı Sonucu URL Ip Sonucu URL Sonucu

Alan Adı: [tkdtosanacademy.ir](http://tkdtosanacademy.ir)

Sunucu Adı: [tkdtosanacademy.ir](http://tkdtosanacademy.ir)

Toplam Tarama: 80

Tespit: 15

URL Alan Adı Sonucu URL Ip Sonucu URL Sonucu

Alan Adı: [tkdtosanacademy.ir](http://tkdtosanacademy.ir)

Sunucu Adı: [tkdtosanacademy.ir](http://tkdtosanacademy.ir)

Toplam Tarama: 80

Tespit: 15

URL Alan Adı Sonucu URL Ip Sonucu URL Sonucu

## TESPİT

Sağlayıcı Adı	Sonuç
CLEAN MX	phishing site
Comodo Valkyrie Verdict	phishing site
Kaspersky	phishing site
G-Data	phishing site
CyRadar	malicious site
Emsisoft	phishing site
Phishtank	phishing site
Avira	phishing site

URL alan adı sonucu, URL IP sonucu ve URL sonucu olarak 3 başlık altında detaylı analiz sonucu verilmektedir.



Virus Total Analizi

Gönderici Link Ekleni

Dosya Adı : orbital viewer orb.bin

Dosya Formatı : bin

Analizi Yenile Sonuç

E-posta içerisindeki ekleni analizi yapılarak; herhangi bir bulgu varsa **Ünlem simbolü** ile gösterilir ve **“Sonuç”** butonu aktif hale gelerek, detaylı analiz işlemi yapılmaktadır.

File:

Analiz Tarihi: 5/15/20 10:45 AM

Toplam: 57

Tarama

SHA256: ce51a44b0e632bf76989d59cbde1884008f55465f6564716b77489638c700a96

Tespit: 3

Virus Total'de gör

#### TARAMA SONUCU

Sağlayıcı Adı

Bulunan

ZoneAlarm

HEUR:Exploit.Win32.Generic

ClamAV

Win.Trojan.MSShellcode-6360729-0

Kaspersky

HEUR:Exploit.Win32.Generic

E-posta içerisindeki ekleni analizinin detayları bu kısımda yer almaktadır.

\*Eklenin **sadece SHA** bilgisi alınarak analiz gerçekleştirilir.

Analiz işlemi tamamlandıktan sonra uygulanabilecek işlemlerin detayı için [buraya tıklayınız](#).

\*Virüs Total analizi, ayarlardan değişiklik yapmadığınız sürece manuel olarak gerçekleştirilen analizdir. Belirlenen özelliklere göre otomatik analiz yapılması için [Ayarlar/Virüs Total](#) sayfasına gidiniz.



### 1.1.1.3. Tehdit İstihbarat Analiz Merkezi: E-posta analizinin gönderici, link ve varsa eklenen başlıklarında analizi yapılmaktadır.

**Gönderilen e-postanın alan adının; IP adresi, kökeni, Google Güvenli Browsing, oluşturulma ve son güncellenme tarihi olarak analizi yapılmaktadır.**

**WHOIS ve İlgili Domain Adreslerinin Değer başlıkları ile analizi yapılmaktadır.**

**Pasif DNS, İlişkili Linkler, İlişkili Dosyalar sonuçları yer almaktadır.**

**Gönderen alan adı sonu: outlook.com**

**Gönderen IP adresi sonu: 40.92.67.19**

**Köken: US**

**Oluşturma Tarihi: 9/4/2019**

**Son Güncelleme: 14/02/2020**

**Değer:**

Kayıt	clientUpdateProhibited
Status	Wed, 16 Aug 2017 00:00:00 +0000
Expiration Date	Sat, 16 Jul 2016 00:00:00 +0000
Updated Date	nsta.0365filtering.com
Name Servers	unsigned
Dnssec	serverTransferProhibited (https://www.icann.org/epp/serverTransferProhibited)
Status	98/02
Zipcode	serverDeleteProhibited
Status	Thu, 18 Aug 2017 00:00:00 +0000
Creation Date	WhoisMark
Whois Server	Tüm bilgilerinizi gizlemektedir

**İLGİLİ DOMAIN ADRESLERİ:**

Alan Adı	Ozerneden İlgili
office365.com	NSIA.0365FILTERING.COM
office.com	NSIA.0365FILTERING.COM
bigfish.com	NSIA.0365FILTERING.COM
microsoftonline.com	NSIA.0365FILTERING.COM
exchangelabs.com	NSIA.0365FILTERING.COM

**PASİF DNS:**

Adres	İlk Görüme	Son Görüme
NXDOMAIN	4/9/20 5:24 AM	4/9/20 5:24 AM
NXDOMAIN	4/9/20 12:25 AM	4/9/20 12:25 AM
104.47.4.36	4/8/20 11:21 PM	4/8/20 11:21 PM
104.47.5.36	4/8/20 11:21 PM	4/8/20 11:21 PM
104.47.7.138	4/8/20 10:52 AM	4/8/20 10:52 AM
104.47.8.74	4/8/20 10:52 AM	4/8/20 10:52 AM

**İLIŞKILI LINKLER:**

Konu / Alan Yolu	Link	Sunucu Adı	Sunucu Cevabı	IP
2020-04-09 08:36:23	http://mail.bn@nam1ton2108.outbound.protection.outlook.com/	mail.bn@nam1ton2108.outbound.protection.outlook.com	0	
2020-04-09 08:35:56	http://dm6pr09mb5989.namprd09.prod.outlook.com/	dm6pr09mb5989.namprd09.prod.outlook.com	0	
2020-04-09 08:35:55	http://bn8pr18mb2963.namprd18.prod.outlook.com/	bn8pr18mb2963.namprd18.prod.outlook.com	0	
2020-04-09 08:35:55	http://bn8pr18mb2498.namprd18.prod.outlook.com/	bn8pr18mb2498.namprd18.prod.outlook.com	0	
2020-04-09 08:35:48	http://westernseminary-edu.mail.protection.outlook.com/	westernseminary-edu.mail.protection.outlook.com	403	104.47.56.138
2020-04-09 08:35:06	http://admin.protection.outlook.com/datainsights/Image...	admin.protection.outlook.com	200	104.47.43.140
2020-04-09 08:35:06	http://admin.protection.outlook.com/datainsights/Image...	admin.protection.outlook.com	200	104.47.35.21
2020-04-09 08:35:00	http://azurlog-com.mail.protection.outlook.com/	azurlog-com.mail.protection.outlook.com	0	
2020-04-09 08:33:53	http://mail-bgr052103192064.outbound.protection.outlo...	mail-bgr052103192064.outbound.protection.outlook.com	0	
2020-04-09 08:33:53	http://mail-bgr052103194065.outbound.protection.outlo...	mail-bgr052103194065.outbound.protection.outlook.com	0	

**İLIŞKILI DOSYALAR:**

Taraf	Hash
2020-02-03 04:04:36	cd4fc2233drf6691a6eebdb336b203f998bf35ccddc7321223dcee37388255ce
2020-01-31 06:10:09	90e84573lc32e6af53818792ae566bb7a066e3714ab9a9d57a551a6a33ddad9
2020-01-30 05:14:03	769be232f58732a9dbf8d2e7d18683b7739d1a747ecb76d7842d5ab26880d



Tehdit İstihbarat Analiz Merkezi ▾

Gönderici Link Ekleni

Alan Adı: microsoft.com  
Link: <http://schemas.microsoft.com/office/2004/12/omml>

Alan Adı: w3.org  
Link: <http://www.w3.org/TR/REC-html40>

Tüm Url'leri Analiz et

Analiz Sonuç

Analiz Sonuç

E-posta içerisindeki linklerin analizi yapılarak; herhangi bir bulgu varsa **ünlem simbolü** ile gösterilir ve “**Sonuç**” butonu aktif hale gelerek, detaylı analiz işlemi yapılmaktadır.

URL Analizi <https://www.google.com>

URL Alan Adı Sonucu URL Sunucu Adı Sonucu URL Ip Sonucu URL Sonucu

Alan Adı: [google.com](https://www.google.com) Köken: US

Sunucu Adı: [www.google.com](https://www.google.com)

URL Analizi <https://www.google.com>

URL Alan Adı Sonucu URL Sunucu Adı Sonucu URL Ip Sonucu URL Sonucu

Alan Adı: [google.com](https://www.google.com) Köken: US

Sunucu Adı: [www.google.com](https://www.google.com)

URL Analizi <https://www.google.com>

URL Alan Adı Sonucu URL Sunucu Adı Sonucu URL Ip Sonucu URL Sonucu

Alan Adı: [google.com](https://www.google.com) Köken: US

Sunucu Adı: [www.google.com](https://www.google.com)

URL Analizi <https://www.google.com>

URL Alan Adı Sonucu	URL Sunucu Adı Sonucu	URL Ip Sonucu	URL Sonucu
Alan Adı: <a href="https://www.google.com">google.com</a>		Köken: US	
Sunucu Adı: <a href="https://www.google.com">www.google.com</a>			

## İLİŞKILI LINKLER

Kontrol Edilme Tarihi	Link	Sunucu Adı	Sunucu Cevabı	Ip
2017-07-02 10:10:33	<a href="https://www.google.com">https://www.google.com</a>		200	172.217.3.196

Toplam 1 kayıttan 1 - 1 arası gösterilmektedir.

URL Alan Adı Sonucu, URL Sunucu Adı Sonucu, URL IP sonucu ve URL sonucu olarak 4 başlık altında detaylı analiz sonucu verilmektedir.

Tehdit İstihbarat Analiz Merkezi ▾

Gönderici Link **Eklenti**

Dosya Adı : log

Dosya Formatı : txt

Analiz

Sonuç

E-posta içerisindeki eklenti analizi yapılarak; herhangi bir bulgu varsa **ünlüm simbolü** ile gösterilir ve **"Sonuç"** butonu aktif hale gelerek, detaylı analiz yapılmaktadır.

E-posta içerisindeki eklenti analizinin detayları verilmektedir.

\*Eklentinin **sadece SHA bilgisi alınarak analiz gerçekleştirilmektedir.**

Analiz işlemi tamamlandıktan sonra uygulanabilecek işlemlerin detayı için [buraya tıklayınız.](#)



**1.1.1.4. URLHaus Analizi:** E-posta analizinin gönderici, link ve varsa ekleni başlıklarında analizi yapılmaktadır.

Şüpheli E-Posta Detayı | [Şüpheli E-Postalar](#) / Şüpheli E-Posta Detayı

Analiz Detaylı analiz & Aksiyon

URLHaus Analizi Gönderici Link

Eposta Gönderen Analizi <beamyigit@outlook.com>

Gönderen alan adı sonucu E-posta sunucusu hostname sonucu E-posta sunucusu Ip adresi sonucu

Alan Adı: [outlook.com](#) Köken: US Oluşturulma Tarihi: 9594 gün önce  
IP Adresi: [40.92.51.81](#) Google Güvenli Browsing: İstatistikler bulunamadı Son Güncelleme: 1591 gün önce

Gönderilen e-postanın gönderen analizi; **gönderen alan adı sonucu, E-posta sunucusu hostname sonucu, E-posta sunucusu IP adresi sonucu** olarak 3 başlıkta incelenmektedir.

Analiz Detaylı analiz & Aksiyon

URLHaus Analizi Gönderici Link

Alan Adı: [opora-company.ru](#)  
Link: [http://opora-company.ru/O5Go/](#) ! Tüm Url'leri Analiz et Analizi Yenile Sonuç

Alan Adı: [www.davidephoto.it](#)  
Link: [http://www.davidephoto.it/GsnlO/](#) ! Analizi Yenile Sonuç

Alan Adı: [grup-juniv2.ga](#)  
Link: [http://grup-juniv2.ga/login.php](#) Analizi Yenile Bulgu bulunamadı

Alan Adı: [ikpwd.tk](#)  
Link: [http://ikpwd.tk/EBUKA/live/tre.php](#) Analizi Yenile Bulgu bulunamadı

E-posta içerisinde bulunan linklerinin analizlerinin sonuçlarını inceleyin. Bulgu varsa **ünləm simbolü** ile belirlenmektedir.



“Sonuç” butonuna tıkladığınızda ilgili adresin; host, tehdit, tarih ve durum bilgilerine ulaşabilirsiniz.

URL Haus Analizi

Gönderici Link

Host [www.davidephoto.it](http://www.davidephoto.it) Tehdit [malware\\_download](#) Tarih 2018-03-05 14:26:22 UTC Durumu offline

**BLACKLIST**

liste	Sonuç
SURBL	not listed
SpamHaus	not listed

**PAYLOADS**

Tarih	SHA256	Tip	Virus Total
2018-03-05	5c87e543f487c754a79efaf4e538e24852f2f5ba81b503ca60224c8d29cd30e	exe	16 / 67
2018-03-05	5025365c1f615874a27059230521ecccfc2736f791cc93efe90672f8cd2e85d	exe	16 / 67
2018-03-05	18d57026b3d7e98a44e0d77a01c699f4863e45b365ea91b64f2f435df63ff10	exe	17 / 67
2018-03-05	d8ecfea0f73ad448bdd3998a4209d1154291fbdd90dae5d324b00b5719cfleb5	exe	15 / 67

Toplam 4 kayıtan 1 - 4 arası gösterilmektedir.

Blacklist kaydı olup olmadığı ya da Payloads ile zararlı tespit edilen adresin bilgilerini analiz edebilirsiniz.



**1.1.1.5. CyThreat Analizi:** E-posta analizinin gönderici, link ve varsa ekleni başlıklarında analizi yapılmaktadır.

The screenshot shows the 'CyThreat Analizi' interface with a single item in the list: 'Eposta Gönderen Analizi <beamigit@outlook.com>'. The results are categorized under 'Gönderici' (Sender) and 'Link'. Under 'Gönderici', there is one entry: 'Alan Adı outlook.com' with a 'Risk 0'. Under 'Link', there are three entries: 'E-posta Sunucu Hostname am9pr04mb7697eurprd04.prod.outlook.com', 'E-posta Sunucu IP 40.92.51.81', and another 'Risk 0' entry. A note at the bottom says 'Bulgu bulunamadı' (No report found).

Gönderilen e-postanın gönderen analizi; **gönderen alan adı sonucu**, **E-posta sunucusu hostname sonucu**, **E-posta sunucusu IP adresi sonucu** olarak 3 başlıkta incelenmektedir.

**Risk Skoru** bilgisine de erişebilirsiniz.

The screenshot shows the 'CyThreat Analizi' interface with four items in the list. Each item has a red warning icon and a 'Sonuç' button. The first item is 'Alan Adı: grup-juniv2.ga'. The second is 'Alan Adı: opora-company.ru'. The third is 'Alan Adı: www.davidephoto.it'. The fourth is 'Alan Adı: ikpswrd.tk'. Each item also has a 'Analizi Yenile' button.

E-posta içerisinde bulunan linklerinin analizlerinin sonuçlarını inceleyin. Bulgu varsa **ünləm simbolü** ile belirlenmektedir.



“Sonuç” butonuna tıkladığınızda ilgili adresin **risk skorunu** görebilirsiniz.

The screenshot shows a web interface for domain analysis. At the top left is a button labeled "CyThreat Analizi ~". On the right are buttons for "Gönderici" and "Link". The main content area displays the following information:

**Alan Adı:** grup-juniinv2.ga  
**Risk:** 66  
**Virus Total:** Virus Total'de gör

**Adı:** resolvedUnusually  
**Kural:** Recently Resolved to Unusual IP  
**Kritiklik Etiketi:** Unusual  
**Kanıt:** From DNS resolution data collected by Recorded Future: Recently resolved to 1 Unusual IP Address: 195.20.50.191.  
**Tarih:** 2020-10-12T11:40:28.887Z  
**Kritiklik:** 1

**Adı:** recentMalwareSiteDetected  
**Kural:** Recently Detected Malware Operation  
**Kritiklik Etiketi:** Malicious  
**Kanıt:** 1 sighting on 1 source: Bitdefender. Last observed on Oct 11, 2020.  
**Tarih:** 2020-10-11T00:00:00.000Z  
**Kritiklik:** 3

Alan adı ile ilgili daha önceki istihbarat sonuçlarını görebilirsiniz.



**1.1.1.6. USOM Analizi:** E-posta analizinin gönderici, link ve varsa ekleni başlıklarında analizi yapılmaktadır.

The screenshot shows the 'Gönderici' tab of the USOM Analysis interface. It displays the following information:

Alan Adı	Köken	Oluşturulma Tarihi
outlook.com	US	9584 gün önce
IP Adresi	40.92.51.81	Google Güvenli Browsing İstatistikler bulunamadı
Son Güncelleme 1591 gün önce		

Bulgu bulunamadı

**Gönderen analizi; alan adı, IP adresi, köken, oluşturulma tarihi gibi başlıklarda analizlerini inceleyin.**

The screenshot shows the 'Link' tab of the USOM Analysis interface. It displays four entries, each with a warning symbol (!) indicating potential issues:

Alan Adı	Link	Aksiyon
ikpwd.tk	<a href="http://ikpwd.tk/EBUKA/tvo/fre.php">http://ikpwd.tk/EBUKA/tvo/fre.php</a>	Tüm Alan Adlarını Analiz et Analizi Yenile Sonuç
grup-juniv2.ga	<a href="http://grup-juniv2.ga/login.php">http://grup-juniv2.ga/login.php</a>	Analizi Yenile Bulgu bulunamadı
opora-company.ru	<a href="http://opora-company.ru/OSGo/">http://opora-company.ru/OSGo/</a>	Analizi Yenile Bulgu bulunamadı
www.davidephoto.it	<a href="http://www.davidephoto.it/GsnlQ/">http://www.davidephoto.it/GsnlQ/</a>	Analizi Yenile Bulgu bulunamadı

E-posta içerisinde bulunan linklerinin analizlerinin sonuçlarını inceleyin. Bulgu varsa **ünləm simbolü** ile belirlenmektedir.



**“Sonuç” butonuna tıkladığınızda ilgili adresin **URL alan adı sonucunu ve URL sonucunu inceleyin.****

The screenshot shows a web-based analysis tool. At the top, there's a navigation bar with 'USOM Analizi' and other tabs like 'Gönderici' and 'Link'. Below the navigation, it says 'URL Analizi' followed by the URL 'http://lkpswrd.tk/EBUKA/five/fre.php'. There are two tabs: 'URL Alan Adı Sonucu' (selected) and 'URL Sonucu'. The main content area displays a table with the following data:

Kayıt	Değer
Alan Adı	lkpswrd.tk
Açıklama	Zararlı Yazılım - Komuta Kontrol Merkezi
Kaynak	USOM
Tarih	10.10.2019 - 05:10:21

Alan adı ile ilgili daha önceki istihbarat sonuçlarını görebilirsiniz.



**1.1.3 Temiz ekranı;** e-posta uygulamasından Phishing Report olarak analize gönderilen ve “**Raporlanan**” e-postalarda bulunan e-postaların, diğer başlıklarda bulunan e-postaların ya da belirlenen aksiyonlar sonucunda durumu “**Temiz**” olarak belirlenen e-postaların görüntüülendiği ekranıdır.

Raporlanan		Temiz	Otalama	Spam	Bilinmeyen	Ara...
Grupla:	Gönderici	Alan Adı	Konu	Ek Dosya	Tamamı	
RS	Gönderici	Konu				
1	Microsoft@e-mail.microsoft.com	Dev Essentials - Learn about new features coming to C# 9.0 and more			e-mail.microsoft.com	30.06.2020 00:45:08
1	beamigit@outlook.com	teeemiz			outlook.com	01.07.2020 15:02:44
1	peter.haack@scale-up-360.com	Der digitale Business Continuity Management Summit 2020 für Cybersecurity- und IT-Entscheidungsträger			scale-up-360.com	09.06.2020 08:15:09
1	fabio.sandrin@we-conect.com	Webinar: Bis zu 80% Kosten reduzieren durch Migration von Content-Anwendungen			we-conect.com	10.06.2020 12:45:26

Ayrıca, tekrar “**İncele**” butonuna tıklayarak şüpheli görünen herhangi bir bilgi varsa yapılmış olan “**Temiz**” seçimini değiştirebilirsiniz.

The screenshot shows the 'Temiz' report interface. At the top, there's a navigation bar with tabs: 'Raporlanan', 'Temiz' (which is active and highlighted in blue), 'Otalama', 'Spam', and 'Bilinmeyen'. Below the navigation is a search bar with placeholder text 'Ara...'. Underneath is a table listing reports. The first report in the table has its 'Temiz' status circled in red at the bottom right of its row. A blue arrow points from this circled area down to the 'Analiz ve Detaylı Analiz & Aksiyon' section below.

Analiz ve Detaylı Analiz & Aksiyon işlemlerinin detayı için [tıklayın.](#)



**1.1.2 Oltalama e-posta uygulamasından Phishing Report olarak analize gönderilen ve “Raporlanan” e-postalarda bulunan e-postaların, diğer başlıklarda bulunan e-postaların ya da belirlenen aksiyonlar sonucunda durumu “Oltalama” olarak belirlenen e-postaların görüntüleneceği ekranıdır.**

Raporlanan Temiz **Oltalama** Spam Bilinmeyen Ara...

Grupla Gönderici Alan Adı Konu Eski Dosya Tamamı

	Gönderici	Konu	Alan Adı	Gönderimleme Tarihi	Raporlayan	Raporlanma Tarihi	Etketler
RS	googlealerts-noreply@google.com	Google Uyan - cyber attack	google.com	25.06.2020 09:07:53	yigit@beamteknoloji.com	08.07.2020 11:34:05	SA_SPAM VT_MALICIOUS test2 YARA_SPAM_1
1	googlealerts-noreply@google.com	Google Uyan - siber saldırı	google.com	23.06.2020 18:32:04	yigit@beamteknoloji.com	01.07.2020 15:01:56	SA_SPAM VT_MALICIOUS YARA_SPAM_1
1	beamyigit@outlook.com	asgdgasgasdg Ⓜ	outlook.com	30.06.2020 17:51:25	beamyigit@outlook.com	30.06.2020 17:51:34	PT_PHISHING BLACKLISTED VT_MALICIOUS
1	googlealerts-noreply@google.com	Google Uyan - ransomware	google.com	24.06.2020 10:38:04	yigit@beamteknoloji.com	30.06.2020 17:50:33	SA_SPAM VT_MALICIOUS YARA_SPAM_1
1	googlealerts-noreply@google.com	Google Uyan - phishing	google.com	24.06.2020 10:45:56	yigit@beamteknoloji.com	30.06.2020 17:50:29	SA_SPAM VT_MALICIOUS YARA_SPAM_1

Anahtar Detaylı analiz & Aksiyon

E-posta bilgileri URL Eski dosya Raporlama bilgileri

Gönderici : training@stayafe.sophos.com Yanlış adresi : Sophos Gönderim tarihi : 07.05.2020 01:00:13 URL Evet Etketi : Evet Raporlayan : yigit@beamteknoloji.com  
Alici : CC URL sayısı : 6 Raporlama Tarihi : 07.05.2020 10:55:49  
yigit@beamteknoloji.com Bkz bilgisi yok. Etketi adet : 1 Toplam raporlenen : 1  
Bkz bilgisi yok. Etketi uzantısı : png  
E-posta alıcı adı : stayafe.sophos.com Oluşturulma Tarihi : 502 gün önce Son Güncelleme : 10:05 gün önce  
Kolek : GB Backlist Analizi :

Oltalama Sayı : 35 Spam Assistant Sayı : 2 HME\_NO\_TEXT / NO\_DE\_AVIS // PP\_HME\_FAKE\_ASCII\_TEXT / T\_DKHM\_INVALID

Gönderici Analizi URL Analizi Eski dosya analizi

Gönderici E-posta Hostname : 10.0.2.1995 Gönderici E-posta Domains : Virus Total : 0 Alert Vault OTX : Virus Total : 0 Alert Vault OTX : Virus Total : 0 Alert Vault OTX : Virus Total : 0  
Virus Total : 0 Alert Vault OTX : 0 Blacklist : 0 Blacklist : 0 Blacklist : 0 Blacklist : 0  
Alert Vault OTX : 0 Blacklist : 0 Blacklist : 0 Blacklist : 0 Blacklist : 0  
Virus Total : 0 Alert Vault OTX : 0 Blacklist : 0 Blacklist : 0 Blacklist : 0 Blacklist : 0

Ayrıca, tekrar “**Incele**” butonuna tıklayarak şüpheli görünen herhangi bir bilgi varsa yapılmış olan “Oltalama” seçimini değiştirin.

Analiz ve Detaylı Analiz & Aksiyon işlemlerinin detayı için [tıklayın.](#)



**1.1.3 Spam** ekranı, e-posta uygulamasından Phishing Report olarak analize gönderilen ve “**Raporlanan**” e-postalarda bulunan e-postaların, diğer başlıklarda bulunan e-postaların ya da belirlenen aksiyonlar sonucunda durumu “**Spam**” olarak belirlenen e-postaların görüntüleneceği ekrandır.

The screenshot shows the 'Spam' analysis interface. At the top, there's a navigation bar with tabs: Raporlanan, Temiz, Olitalama, **Spam**, Bilinmeyen, and a search bar. Below the navigation is a filter section with 'Grupla:' dropdowns for 'Gönderici', 'Alan Adı', 'Konu', 'Eski Dosya', and 'Tamamı'. The main area displays a table of reported emails:

Sıra	Gönderici	Konu	Alan Adı	Gönderimleme Tarihi	Raporlayan	Raporlanma Tarihi	Etilkiler
1	newsletter@raconteur.net	Is this the end of office life?	raconteur.net	25.06.2020 08:08:37	yigit@beamteknoloji.com	08.07.2020 15:16:40	SA-SPAM VT-CLEAN YARA_SPAM_1
1	peerinsights@ReviewIT.gartner.com	Yiğit, Gartner Needs Your Help!	ReviewIT.gartner.com	23.06.2020 18:04:03	yigit@beamteknoloji.com	01.07.2020 15:02:04	SA-SPAM VT-CLEAN test2 YARA_SPAM_1
1	taco@trello.com	How to use Trello as a calendar	trello.com	23.06.2020 18:22:29	yigit@beamteknoloji.com	01.07.2020 15:02:00	SA-SPAM VT-CLEAN YARA_SPAM_1
1	dboller@squiglit.com	Your Free Squiglit Account	squiglit.com	24.06.2020 00:38:06	yigit@beamteknoloji.com	01.07.2020 15:01:52	SA-SPAM VT-CLEAN YARA_SPAM_1
1	training@staysafe.sophos.com	Reminder: your required security awareness training is incomplete	staysafe.sophos.com	24.06.2020 02:10:26	yigit@beamteknoloji.com	01.07.2020 15:01:48	SA-SPAM VT-CLEAN YARA_SPAM_1
1	media@code-cafe.blog	RE: 5 Steps to Integrate SAST into the DevSecOps Pipeline   Webinar	code-cafe.blog	12.06.2020 12:01:25	yigit@beamteknoloji.com	30.06.2020 17:51:27	SA-SPAM VT-CLEAN test2 YARA_SPAM_1

Below the table is a detailed analysis section titled 'Analiz Detayı & Aksiyon' (Analysis Detail & Action). It includes sections for 'E-posta bilgileri' (Email Info), 'Ortalama Skor' (Average Score), and 'Spam Assistant Skor' (Spam Assistant Score). The 'E-posta bilgileri' section shows details like 'Gönderici: staysafe.sophos.com', 'Yanlış adres: Sophos', 'Gönderim tarihi: 01.07.2020 08:00:13', etc. The 'Ortalama Skor' section shows a score of 35 with a note about URL analysis. The 'Spam Assistant Skor' section shows a score of 2 with a note about MIME\_NO\_TEXT\_NO\_RELAYS errors. The bottom part of the analysis section contains 'Gönderici Analizi' (Sender Analysis) and 'URL Analizi' (URL Analysis) tables.

Ayrıca, tekrar “**İncele**” butonuna tıklayarak şüpheli görünen herhangi bir bilgi varsa yapılmış olan “**Spam**” seçiminin değiştirin.

Analiz ve Detaylı Analiz & Aksiyon işlemlerinin detayı için [tıklayın.](#)



**1.1.4 Bilinmeyen** ekranı, e-posta uygulamasından Phishing Report olarak analize gönderilen ve “**Raporlanan**” e-postalarda bulunan e-postaların, diğer başlıklarda bulunan e-postaların ya da belirlenen aksiyonlar sonucunda durumu “**Bilinmeyen**” olarak belirlenen e-postaların görüntüleneceği ekrandır.

Analiz Detayı analiz & Aksiyon

Grupla :	Gönderici	Konu	Alan Adı	Gönderimle Tarihi	Raporlayan	Raporlanma Tarihi	Etiketler
RS	no-reply@dropbox.com	Your transfer from hande deniz alp expires in 1 day	dropbox.com	25.07.2020 15:19:07	hande.alp@beamteknoloji.com	12.08.2020 13:51:27	VT-CLEAN
1	beamyigit@outlook.com	tests2 Ⓜ	outlook.com	29.06.2020 12:56:38	beamyigit@outlook.com	29.06.2020 12:56:56	VT-MALICIOUS, PT-PHISHING, BLACKLISTED
1	beamyigit@outlook.com	test ekili 2 Ⓜ	outlook.com	14.05.2020 16:29:37	beamyigit@outlook.com	14.05.2020 16:29:25	YARA_SPAM_1
1	sender@gmail.com	Test E-Mail 3	gmail.com	04.09.2020 10:50:17	receiver@gmail.com	04.14.2020 10:50:17	

**E-posta bilgisi**

Gönderici : training@laysafe.sophos.com	Yanıt adresi : Sophos	Gönderim tarihi : 07.05.2020 01:08:33	URL : Evet	Etkili : Evet	Raporlayan : yigit@beamteknoloji.com	
Ara : yigit@beamteknoloji.com	CC : Brbg bulanmejor	Anahtar : İsimzanesi	URL sayısı : 6	Etkili adedi : 1	Etkili uzantıları : png	Raporlanma Tarihi : 07.05.2020 15:51:19
E-posta alan adı : staysafe.sophos.com			Olusturulma Tarihi : 9/22 gün önce	Son Güncelleme : 12/05 gün önce	Köken : GB	Toplam raporları : 1
Blacklist Analizi : <input checked="" type="checkbox"/>						

**Otala Skor**

35	• Yanlışlıkla phish'eşten URL'ler var • Başlangıçtaki e-posta adı geçici looksalitik funkcı • Gönderenin tarihinde atanmış URL içermeyen • Gönderenin tarihinde yanlış adresi • Alan adı parçalarının adı
----	---

**Spam Assassin Skor**

2	MIME_NO_TEXT / NO_RELAYS / PP_MIME_FAKE_ASCH_TEXT / T_OOM_INVALID
---	---

**Gönderici Analizi**

Gönderici E-posta Hostname : 17.02.7795	Gönderici E-posta Domain : Virus Total : Alert Vault OTX : Blacklist :	Gönderici E-posta Sunucusu IP : Virus Total : Alert Vault OTX : Blacklist :
Virus Total : 0/0	Virus Total : 0/0	Virus Total : 0/0
Alert Vault OTX : 0/0	Alert Vault OTX : 0/0	Alert Vault OTX : 0/0
Blacklist : 0/0	Blacklist : 0/0	Blacklist : 0/0

**URL Analizi**

URL : Virus Total : Proshrank : 0/0	URL Domain : Virus Total : Alert Vault OTX : Blacklist : 0/0	URL Sunucusu IP : Virus Total : Alert Vault OTX : Blacklist : 0/0	Etkili dosya analizi : Virus Total : Alert Vault OTX : 0/0
Proshrank : 0/0	Virus Total : 0/0	Alert Vault OTX : 0/0	Virus Total : 0/0
Blacklist : 0/0	Blacklist : 0/0	Blacklist : 0/0	Alert Vault OTX : 0/0

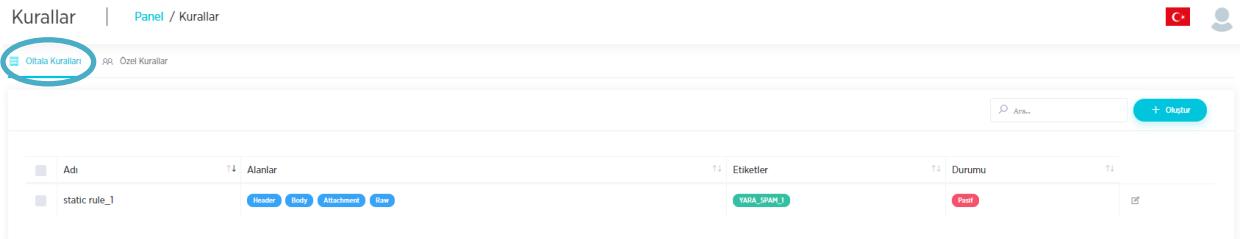
Ayrıca, tekrar “**İncele**” butonuna tıklayarak şüpheli görünen herhangi bir bilgi varsa yapılmış olan “**Bilinmeyen**” seçiminin değiştirin.

Analiz ve Detaylı Analiz & Aksiyon işlemlerinin detayı için [tıklayın](#).



## 1.2 Kurallar

E-postanın incelenmesi olana alanlarını belirleyip (başlık, içerik, ekleni), etiket ekleyerek koşula atanabilmektedir. **Yara kurallarını kullanarak mailleri etiketlemek (Taging) için kullanılır.**



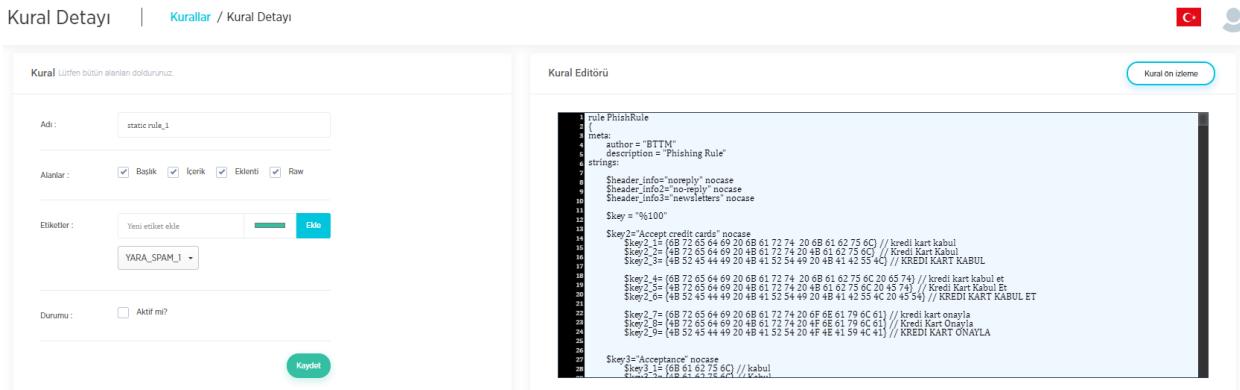
Kurallar | Panel / Kurallar

Oltala Kuralları | Özel Kurallar

Adı: static rule\_1 | Alanlar: Header, Body, Attachment, Raw | Etiketler: YARA\_SPAM\_1 | Durumu: Prof | Arama: + Okluar

Kurallar; Oltala ve Özel kurallar olarak ayrılmıştır.

- Oltala Kuralları:** Platformumuza özgü hazırlanmış olan kural ve sonucunda atanacak olan etiketi ve kural detayı görüntülenebilir ya da pasif/ aktif durumu kontrol edilebilmektedir.
- Özel Kurallar:** Oluşturulmak istenen, kullanıcıların kendisinin belirlediği özelliğe kuralların oluşturulabileceği ekranıdır.



Kural Detayı | Kurallar / Kural Detaylı

Kural | Kuralın bütün alanları doldurunuz.

Adı: static rule\_1

Alanlar:  Basılık  İcerik  Ekleni  Raw

Etiketler: Yeni etiket ekle |  | YARA\_SPAM\_1

Durumu:  Aktif mi?

Kural Editörü

```
rule PhishRule
{
    meta:
        author = "BTTM"
        description = "Phishing Rule"
        strings:
            Sheader_info="bounce"
            Sheader_info2="no-reply"
            Sheader_info3="newsletters" nocase
            Skey = "%{100}"
            Skey2="Accept credit card" nocase
            Skey2_1=(6B 72 65 64 69 20 6B 61 72 74 20 6B 61 62 75 6C) // kredi kart kabul
            Skey2_2=(4B 72 65 64 69 20 4B 61 72 74 20 4B 61 62 75 6C) // KREDİ KART KABUL
            Skey2_3=(4B 72 65 64 69 20 4B 61 72 74 20 4B 61 62 75 6C) // KREDİ KART KABUL
            Skey2_4=(6B 72 65 64 69 20 6B 61 72 74 20 6B 61 62 75 6C) // kredi kart kabul et
            Skey2_5=(4B 72 65 64 69 20 4B 61 72 74 20 4B 61 62 75 6C) // KREDİ KART KABUL ET
            Skey2_6=(4B 52 45 44 49 20 4B 61 52 54 49 20 4B 61 62 75 6C) // KREDİ KART KABUL ET
            Skey2_7=(6B 72 65 64 69 20 6B 61 72 74 20 6F 6E 61 79 6C 61) // kredi kart onayla
            Skey2_8=(4B 72 65 64 69 20 4B 61 72 74 20 4F 6E 61 79 6C 61) // KREDİ KART ONAYLA
            Skey2_9=(4B 52 45 44 49 20 4B 61 52 54 20 4F 4E 41 59 4C 41) // KREDİ KART ONAYLA
            Skey3="Acceptance" nocase
            Skey3_1=(6B 61 62 75 6C) // kabul
            Skey3_2=(4B 61 62 75 6C) // kabul
}
```

E-postanın incelenmesi istenilen alanlar, birden fazla seçim yapılarak kural oluşturulabilmektedir. Kural editörü yardımıyla, incelenmesi istenilen değeri "string" kısmına yazılarak, ön izleme kısmından bu duruma uyan e-postalar görüntülenebilmektedir.

**Bir kuralın kaydedilmesi veya güncellenmesi durumunda 'İlgili kurala uyan bütün e-postalar için' kural içerisinde 'girilmesi zorunlu' olan etiket alanında seçilen bütün etiketler e-postalara atanmaktadır.**



### 1.3. Etiketler

Etiket; e-postalara, kural ya da aksiyon işlemleri tanımlanarak e-posta analizi sürecinde kolaylık sağlamağaçdır.

Etiketler	Panel / Etiketler	C	Ayarlar
			Arka...
Adı	Sıralı E-Postalar	Kurallar	Aksiyonlar
VT-PENDING	0		Spam
VT-CLEAN	44		Clean / Spam
VT-MALICIOUS	44		Malicious / Spam
PT-PHISHING	3		Malicious / Spam
SA-SPAM	33		Spam
YARA_SPAM_1	66	Detaylı	Spam
BLACKLISTED	32		Malicious / Spam
test	7		Malicious / Spam
MNLI_FEED	2		Main Action

Otomatik olarak yapılan tarama işlemi sonucunda, tarama işlemine ait olan sonuçları etiketlere atanmaktadır. Kullanıcıya analiz aşamasında kolaylık sağlama amacıyla belirlenen etiketler aşağıda verilmiştir.

**VT-MALICIOUS**

Virüs Total- E posta içerisinde, ekli dosya olup olmadığına taramasını yapar. Ekli dosya var ise, analiz edilen ya da yeni bildirilecek olan e-posta “VT-Malicious” etiketini alır.

*Etiketi ve bağlı olduğu aksiyon ve kuralları, butonu ile detaylı inceleyin.*

**VT-CLEAN**

Virüs Total- E posta içerisinde, herhangi bir zararlı içerik yoksa analiz edilen e-posta “VT-Clean” etiketini alır.

*Etiketi ve bağlı olduğu aksiyon ve kurallarını, butonu ile detaylı inceleyin.*

**BLACKLISTED**

Belirlediğiniz aksiyonlar ya da kurallar sonrasında, e-postanın belirlenen koşulları sağladığında analiz edilen ya da yeni bildirilecek olan e-posta “Blacklisted” etiketini alır.

*Etiketi ve bağlı olduğu aksiyon ve kurallarını, butonu ile detaylı inceleyin.*

**YARA\_SPAM\_1**

YARA kurallarının belirlenmiş olduğu ve bu kurallara sahip olan e-postaların alacağı etikettir.

*Etiketi ve bağlı olduğu aksiyon ve kurallarını, butonu ile detaylı inceleyin.*

**VT-PENDING**

Yeni bildirilen bir e-posta, analiz sürecinde ve analizinin tamamlanması bekleniyorsa “VT-Pending” etiketini alır.

*Etiketi ve bağlı olduğu aksiyon ve kurallarını, butonu ile detaylı inceleyin.*

Etiket Detayı | [Etiketler](#) / Etiket Detayı

## phishing



Şüpheli E-Postalar



Aksiyonlar

Tag İsmi: phishing  
Son Güncelleme: 09.01.2020 13:15:14

Güncelle

**Etiket Detayı/ Şüpheli E-postalar başlığında, etiketin atanmış olduğu e-postalar görüntülenmektedir.**

Etiket Detayı | [Etiketler](#) / Etiket Detayı

## phishing



Şüpheli E-Postalar



Aksiyonlar

SUBJECT IS ALL CAPITALS 21ff0990-6f1a-489b-a072-b4012282d398

Gönderici: spamTest@olta.la

Raporlayanlar: beamygtt@yahoo.com

Etiketler: [phishing](#) [done](#)

Detay

edfa556a-f051-40c0-bb42-d2010ed42fd7

Gönderici: test@olta.la

Raporlayanlar: beamygtt@yahoo.com

Etiketler: [phishing](#) [done](#)

Detay

f35e140a-5478-49f8-9aed-2c6c262f8ebd

Gönderici: test@olta.la

Raporlayanlar: beamygtt@yahoo.com

Etiketler: [phishing](#) [done](#)

Detay

Etiket Detayı | [Etiketler](#) / Etiket Detayı

## phishing



Şüpheli E-Postalar



Aksiyonlar

test  
Alanlar: [body](#) [header](#)Etiketler: [phishing](#) [done](#)

Detay

test2  
Alanlar: [header](#)Etiketler: [phishing](#)

Detay

**Etiket Detayı/ Kurallar başlığında, etiketin kullanıldığı kurallar incelenebilir ve **detay** kısmından ilgili kurallar görüntülenebilmektedir.**



## 1.4. Aksiyonlar

Raporlanmış olan e-postaları, etiket niteliklerine veya kullanıcının manuel olarak tetiklemesine bağlı olarak aksiyonları alırmaktır. Oluşturulan aksiyonların sıralaması değiştirilerek, öncelikli olarak çalışması istenilen aksiyon belirlenmektedir.

Aksiyonlar | [Panel](#) / Aksiyonlar

Aksiyon Listesi

Adı	Açıklama	Tetikleyiciler	Durumu	Son Güncelleme
testt	testt	Etiket Belirlendi	<span>Aktif</span>	09.01.2020 17:30:54



### 1. Genel Bilgiler:

Aksiyon adının, açıklamasının ve aktif/ pasif durumunun seçildiği kısımdır.  
**Aktif olmayan hiçbir aksiyon işleme alınmaz.**

Aksiyon Detayı | [Aksiyonlar](#) / Aksiyon Detayı

Aksiyon Oluştur / Güncelle



Kaydet

Genel Bilgiler	
Aksiyon Adı	Açıklama
Son Güncelleme	Aktif mi? <input checked="" type="checkbox"/>
<a href="#">Tetikleyiciler</a> +	
<a href="#">Aksiyonlar</a> +	



## 2. Tetikleyiciler: Aksiyonun hangi mesajlar üzerinde aktif olacağını göstermektedir.

Aksiyon Detayı | [Aksiyonlar](#) / [Aksiyon Detayı](#)

Aksiyon Oluştur / Güncelle

Kapat

**Tetikleyiciler**

Her Mesaj:   Hepsi  Herhangi  Sadece  
Belirlenen etiketlere sahip olan e-postaları bul.

Etiket Olmayanlar:   Hepsi  Herhangi  Sadece  
Belirlenen etiketlere sahip olmayan şüpheli e-postaları bul.

Etiket Belirle:   Hepsi  Herhangi  Sadece  
Belirlenen etiketlere sahip olan şüpheli e-postaları bul.

Manuel Tetikle:

**Her mesaj: Bütün e-postalar için** aksiyonlar içerisinde belirtilen işlemleri yapacaktır.

**Etiketi Olmayanlar:** Aksiyon **sadece etiketi olmayan e-postalar için** aksiyonlar içerisinde belirtilen işlemleri yapacaktır.

**Etiket Belirle:** Kullanıcıya mantıksal seçim sunarak, **kullanıcının etiket bazlı elemesine uyan e-postalar için** aksiyonlar içerisinde belirtilen işlemleri yapacaktır.

➤ Sahip olan kısmı:

- **Hepsi:** Seçilen etiketlerin tamamına sahip olan, **bunların haricinde de etikete sahip olan ya da olmayan** e-postaları secer.
- **Herhangi:** Seçilen etiketlerden herhangi birine sahip, **bunların haricinde de etikete sahip olan ya da olmayan** e-postaları secer.
- **Sadece:** Sadece gönderilen etikete sahip olan e-postaları secer.

➤ Sahip olmayan kısmı:

- **Hepsi:** Seçilen etiketlerin hiçbirine sahip olmayan, **bunların haricinde de etikete sahip olan ya da olmayan** e-postaları secer.
- **Herhangi:** Seçilen etiketlerden herhangi birine sahip olmayan, **bunların haricinde de etikete sahip olan ya da olmayan** e-postaları secer.
- **Sadece:** Sadece gönderilen etikete sahip olmayan e-postaları secer.

**Manuel Tetikle:** Kullanıcının sadece manuel tetiklenmesi ile oluşacak aksiyonlardır.



### 3. Aksiyonlar

Aksiyon Detayı | [Aksiyonlar / Aksiyon Detayı](#)



Genel Bilgiler +

Tetikleyiciler +

**Aksiyonlar** -

Durum Ata

Etket Ata

E-posta Gönder

Sylog Gönder

E-postanı Sil

Hemen Uygula

Durdur

**Durum ata:** Belirlenen tetikleyicilere sahip e-postaların; durumunun **Temiz**, **Spam**, **Şüpheli** ya da **Bilinmeyen** belirlendiği seçeneklerdir.

**Etket ata:** Belirlenen tetikleyicilere sahip e-postaların; oluşturulmuş olan ya da yeni belirlenen etikete atanmasıdır.

**E-posta Gönder:** Belirlenen tetikleyicilere sahip e-postanın şüpheli olduğunu belirten maili; raporlayan kişiyi dahil ederek ya da yeni alıcı belirleyerek, orijinal e-postanın gönderme tipine göre şablon seçerek e-postanın gitmesi istenilen kişi/kışiler belirlenmektedir.

Raporlayan Dahil Et  Alıcı Belirle

Original e-postanın ekli dosya olarak gönder  Original e-postanın sonuna ekleyerek gönder

E-posta şablonu seç

Otomatik raporlama bildirimi  
Şüpheli URL.  
Deneme  
Sorunsuz e-post  
Raporlama Sablonu  
Raporlama Bildirim Sablonu

**Sylog Gönder:** Belirlenen tetikleyicilere sahip e-postanın, json formatında bilgilerini sylog'a gönderilmesidir.

**E-postaları sil:** Belirlenen tetikleyiciler ile eşleşen şüpheli e-postaların olay müdahale platformundan silinmesidir.

**Plugin İşlemleri:** Belirlenen işlemlere göre; e-postayı **silme**, **bayrak ekleme**, **url gizle/göster**, **karantinaya al /çıkar** işlemleri atanmaktadır.

Sil  Bayrak  Uri gizle

Uri göster  Karantinaya al  Karantinadan çıkar

**Hemen uygula:** Tetikleyiciler tarafından belirlenen tüm e-postalara uygulanacaktır.

**Durdur:** Bu aksiyonun işlemi bittiğinde, başka aksiyonu işleme almaması anlamına gelir.



## 1.5. Saptama

Saptama ekranında belirlenen kriter ya da kriterleri karşılayan e-postaların bulun ve analiz edin.

The screenshot shows a list of search results for various email addresses. The 'Saptama' button on the left sidebar is circled in blue. The 'Yeni Saptama' button at the top right is also circled in blue.

Adı	Ölçütüran	Son Aksiyon	Durumu	Bitti Tarihi	İşlem Görmüş E-posta Kutusu Sayısı	Aksiyon
dasdasdasd	team@olta.la Okutunma: 15.08.2020 09:50:47 Son Güncelleme: Thu Aug 13 09:37:11 EEST 2020	Sil	Searching		2	
asdglasgasdas	team@olta.la Okutunma: 15.08.2020 09:28:16 Son Güncelleme: Thu Aug 13 09:37:11 EEST 2020	Bul	Searching		1	
test	team@olta.la Okutunma: 12.08.2020 17:27:13 Son Güncelleme: Wed Aug 12 17:33:02 EEST 2020	Bul	Searching		3	
yigit gönderen	team@olta.la Okutunma: 12.08.2020 16:07:29 Son Güncelleme: Wed Aug 12 16:36:03 EEST 2020	Bul	Searching		0	
asdglasgasdasdasdas	team@olta.la Okutunma: 11.08.2020 16:02:54 Son Güncelleme: Wed Aug 12 16:38:26 EEST 2020	Bul	Searching		4	
dasgasgdgasgasgas	team@olta.la Okutunma: 12.08.2020 16:02:29 Son Güncelleme: Wed Aug 12 16:37:49 EEST 2020	Bul	Searching		4	
asdglasgasdasdas	team@olta.la Okutunma: 12.08.2020 16:02:25 Son Güncelleme: Wed Aug 12 16:37:32 EEST 2020	Bul	Searching		4	
dasgasgdgas	team@olta.la Okutunma: 12.08.2020 16:02:29 Son Güncelleme: Wed Aug 12 16:37:49 EEST 2020	Bul	Searching		4	
fasgasgasd	team@olta.la Okutunma: 12.08.2020 15:57:15 Son Güncelleme: Wed Aug 12 15:58:54 EEST 2020	Bul	Searching		3	
toplu mime type	team@olta.la Okutunma: 12.08.2020 15:57:15 Son Güncelleme: Wed Aug 12 15:58:54 EEST 2020	Bul	Searching		3	
docx	team@olta.la Okutunma: 12.08.2020 15:53:31	Bul	Searching		4	

Yeni Saptama oluşturmak için “Yeni Saptama” butonuna tıklayın.

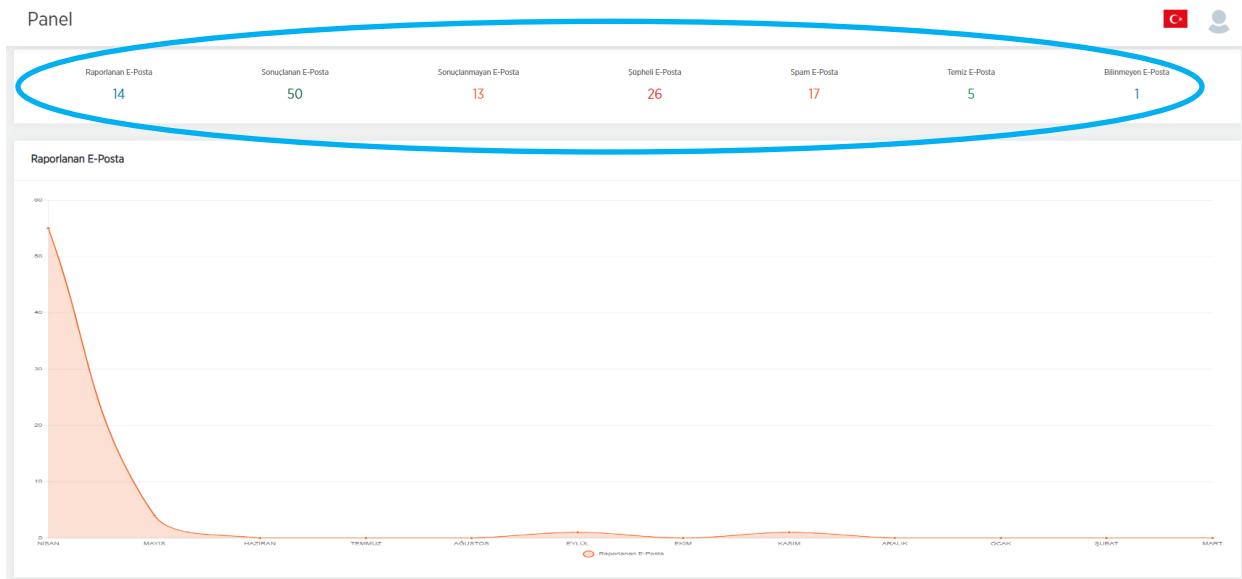
The screenshot shows the 'Saptama Aracı' (Search Tool) configuration page. The 'Gönderi Konusu' field is circled in blue. The 'Tümle' (Preview) and 'Kaydet' (Save) buttons at the bottom right are also visible.

Gönderi Konusu, Gönderici, Ekli Dosya İsmi, Ekli Dosya Mime Type, Ekli Dosya Hash ve Tarih Aralığı belirleyerek bu kriterleri karşılayan e-postaları bulun ve hepsine aynı işlemleri aynı anda yapın.

**Not:** Örn: Gönderici Konusu yazmışsanız, “Enter” tuşuna basarak kaydetme işlemini yapmalısınız.

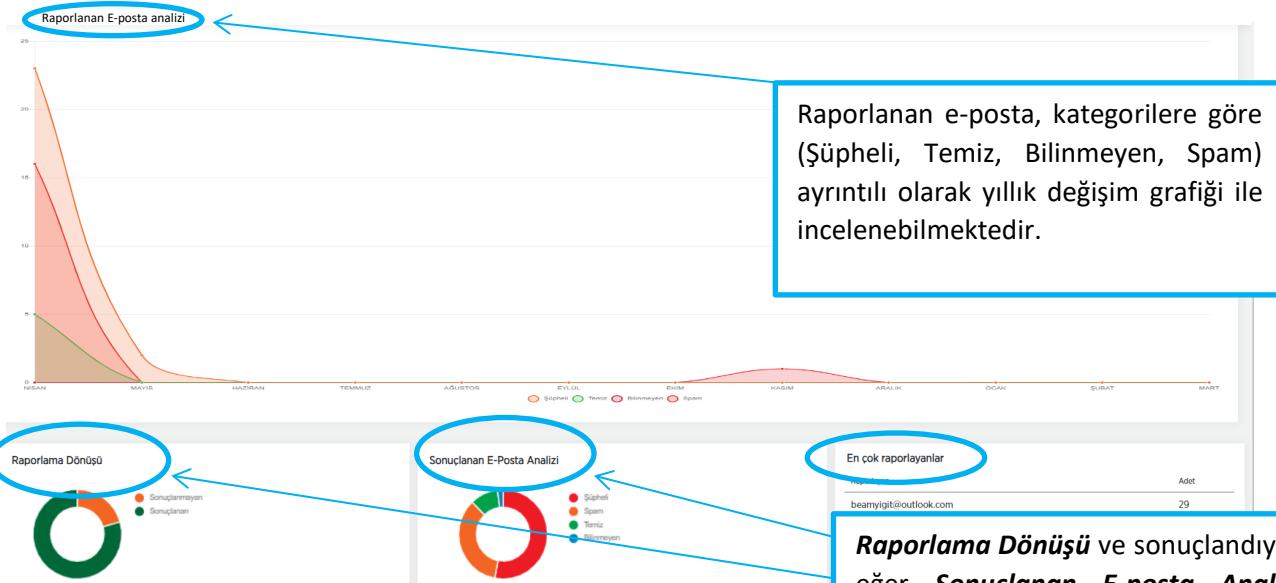


## 1.6. Panel



E-postalar; atanmış olan durumlara göre ilgili başlıklar altında sayıları incelenebilmektedir.

Ayrıca, **Raporlanan E-Posta** grafiği ile bir yıllık hareketleri takip edilebilmektedir.



Raporlanan e-posta, kategorilere göre (Şüpheli, Temiz, Bilinmeyen, Spam) ayrıntılı olarak yıllık değişim grafiği ile incelenebilmektedir.

**Raporlama Dönüşü** ve sonuçlandıysa eğer **Sonuçlanan E-Posta Analizi** grafiği ile detaylı sonuçlar görüntülenmektedir.

Ayrıca **En Çok Raporlayanlar** kısmından raporlayan kişinin bilgilerini ve raporlama sayısı incelenebilmektedir.



## 1.7. Ayarlar

### 1.7.1 Yönetim Paneli

Ayarlar | [Panel](#) / Ayarlar[C-](#) [C+](#)

<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanılacak SMTP sunucusu için gerekli, ayarlar düzenlenir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
<b>İçerik Güncelleme</b> Senaryolar ve körpüne içeriğin bulunması üzerinden güncelleme sağlar.	<b>SysLog Sunucuları</b> SysLog sunucularının eklenme, güncelleme ve silme işlemleri.	<b>Yetkilendirme</b> Uygulama rollerinin yetkilendirilmesini güncelleme yapmaktadır.
<b>Virus Total</b> Virus Total için API anahtar değerler tanımına işlemleri burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcı üzerinde kurulu olan PhishingReport Plugin'lerini kontrol etmeye sağlar.	<b>Lisans Yönetimi</b> Uygulama lisans ayarlarının yönetimi yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimini yapabilirsiniz.	<b>Veri Koruma Yönetimi</b> Buradan uygulama verilerinin kalıcılığını yönetimi yapabilirsiniz.	<b>İtibar İstatistikleri</b> Burada raporlama yapan kullanıcılar istatistiklerini görebilir veya sıfırlayabilirsiniz.
<b>Roksit DNS API Yönetimi</b> Roksit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile giriş için LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish için API anahtar değerler tanımına işlemleri burdan yapılmaktadır.
<b>Whitelist</b> Whitelist yönetimi.	<b>API Konfigurasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcının parolarının güvenlik politikası bu ekranдан düzenlenmektedir.

Kullanıcı Yönetimi | [Panel](#) / [Ayarlar](#) / Kullanıcı Yönetimi[C-](#) [C+](#)

Kullanıcılar							2FA Yönetimi
#	Adı Soyadı	EMAIL	Hesap Türü	Durumu	İşlemler	+ Ekle	
1		admin@response.io	Yönetici Rolü	✓			
2		user@response.io	Firma Kullanıcısı	✓			
3		admin@response	Yönetici Rolü	✓			
4		user@response	Firma Kullanıcısı	✓			

Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.



## Kullanıcı Yönetimi

Panel / Ayarlar / Kullanıcı Yönetimi

Kullanıcılar

2FA Yönetimi

Çift Adımlı Doğrulamayı aktifleştir



Çift adımlı doğrulama etkinleştirilerek, QR kod doğrulaması ile güvenlik arttırmaktadır.

## Kullanıcı Yönetimi

Panel / Ayarlar / Kullanıcı Yönetimi



Kullanıcılar

2FA Yönetimi

#	Adı Soyadı	EMAIL	Hesap Türü	Durumu	İşlemler
1		admin@response.io	Yönetici Rolü	✓	
2		user@response.io	Firma Kullanıcı	✓	
3		admin@response	Yönetici Rolü	✓	
4		user@response	Firma Kullanıcı	✓	



“Ekle” butonuna ile uygulamayı kullanması için yeni kişiler ekleyin.

## Kullanıcı Ekle

Panel / Ayarlar / Kullanıcı Yönetimi

Kullanıcı Adı \*

Kullanıcı adı e-posta şeklinde verilir. Verilen adresde parola olumsuz e-postası gönderilecektir.

Adı \*

Soyadı \*

Cep Telefonu \*

Sabit Telefon \*

Hesap Türü \*

Sayfalar arası kolay geçiş için buradaki butonlar kullanılmaktadır.

Kaydet



## 1.7.2 SMTP Ayarları

Ayarlar | Panel / Ayarlar

TR



Yönetim Paneli <small>Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.</small>	SMTP Ayarları <small>Kampanyalarda kullanılabilecek SMTP sunucusu için genel, ayarlar düzenleyin.</small>	E-posta Şablonları <small>Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.</small>
İçerik Güncelleme <small>Sınırlılar ve kütüphane içeriklerinin bulut üzerinde güncelleme yapılmasını sağlar.</small>	SysLog Sunucuları <small>SysLog sunucularının eklemeye, güncelleme ve silme işlemlerini.</small>	Yetkilendirme <small>Uygulama rollerinin yetkilendirilmesini güncelleme yapılmaktadır.</small>
Virus Total <small>Virus Total için API anahtarları değer tarama işlemleri burdan yapılmaktadır.</small>	Plugin Yönetimi <small>Kullanıcılar üzerinde kurulan PhishingReport Plugin'ını kontrol etmeye sağlar.</small>	Lisans Yönetimi <small>Uygulama lisans ayarının yönetimi yapılmaktadır.</small>
SpamAssassin Yönetimi <small>Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılmaktadır.</small>	Veri Koruma Yönetimi <small>Buradan uygulama verilerinin kalıcılığını yönetimi yapılmaktadır.</small>	İtibar İstatistikleri <small>Burada raporlama yapan kullanıcılar istatistiklerine göre bilgi veya sıralayabilmektedir.</small>
Rokit DNS API Yönetimi <small>Rokit DNS Uri ve API yönetimi.</small>	LDAP Ayarları <small>LDAP ile giriş için LDAP ayarları düzenlenmektedir.</small>	Check Phish <small>Check Phish için API anahtarları değer tarama işlemleri burdan yapılmaktadır.</small>
Whitelist <small>Whitelist yönetimi.</small>	API Konfigürasyon Yönetimi <small>API yönetimi burdan yapılmaktadır.</small>	Parola Politikası <small>Uygulama kullanıcılarının parolarının güvenlik politikası bu ekranın düzenlenmektedir.</small>

\*SMTP, e-posta göndermeye yardımcı olan **internet standartıdır**. Sunucular için gerekli ayarlamaları buradan yapılmaktadır.

### SMTP Sunucusu Erişim Bilgileri

Sunucu \*

Port \*

SSL Kullan \*

**Kaydet**



### 1.7.3 E-Posta Şablonları

Ayarlar | [Panel](#) / Ayarlar[Türkçe](#)

Yönetim Paneli	SMTP Ayarları	E-posta Şablonları
Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	Kampanyalarda kullanılacak SMTP sunucusu için gerekli ayarlar düzenlenir.	Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
İçerik Güncelleme	SysLog Sunucuları	Yetkilendirme
Senaryolar ve kütüphane içeriklerinin bütünlüğinden güncelleme sağlar.	SysLog sunucularının eklenme/güncelleme ve silme işlemleri.	Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
Virus Total	Plugin Yönetimi	Lisans Yönetimi
Virus Total için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.	Kullanıcılar üzerinde kurulu olan PhishingReport Plugin'ını kontrol etmeye sağlar.	Uygulama lisans ayarlarının yönetimi yapılmaktadır.
SpamAssassin Yönetimi	Veri Koruma Yönetimi	İtibar İstatistikleri
Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılmaktadır.	Burada uygulama verilerinin kaçışının yönetimi yapılmaktadır.	Check Phish
Roksit DNS API Yönetimi	LDAP Ayarları	Parola Politikası
Roksit DNS Uri ve API yönetimi.	LDAP ile girdi için LDAP ayarları düzenlenmektedir.	Uygulama kullanıcının parolalarının güvenlik politikası bu ekranдан düzenlenmektedir.
Whitelist	API Konfigurasyon Yönetimi	
Whitelist yönetimi	API yönetimi burdan yapılmaktadır.	

Sistem E-postaları | [Panel](#) / [Ayarlar](#) / Sistem E-postaları[Türkçe](#)

#	Sistem E-posta	Tanımlandi mı?
1	Raporlama Şablonu	<a href="#">Güncelle</a> <a href="#">On izleme</a>
2	Raporlama Bildirim Şablonu	<a href="#">Güncelle</a> <a href="#">On izleme</a>
3	Parola Unutma Şablonu	<a href="#">Güncelle</a> <a href="#">On izleme</a>
4	Hesap Aktivasyon Şablonu	<a href="#">Güncelle</a> <a href="#">On izleme</a>
5	Hesap İşlemleri Bildirim Şablonu	<a href="#">Güncelle</a> <a href="#">On izleme</a>
6	Hata Şablonu	<a href="#">Tanımla</a>

Toplam 6 kayttan 1 - 6 arası gösterilmektedir.

Sistem E-Posta şablonlarının görüntülendiği ekranıdır. Ön izleme ya da Güncelle seçenekleri ile içerik görüntüleyin ya da güncelleyin.



## 1.7.4 İçerik Güncelleme

Ayarlar | [Panel](#) / Ayarlar

[TR](#)

<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanılabilecek SMTP sunucusu için gerekli, ayarlar düzenlenir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
<b>İçerik Güncelleme</b> Senaryolar ve kılavuzlar içeriklerinin buzdan düzenlenmesini sağlar.	<b>SysLog Sunucuları</b> SysLog sunucularının eklenme, güncelleme ve silme işlemleri.	<b>Yetkilendirme</b> Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
<b>Virus Total</b> Virus Total için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcılar özende kurulmuş PresingReport Plug-inlerini kontrol etmeye sahiptir.	<b>Lisans Yönetimi</b> Uygulama lisanslarının yönetimi yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılabilirsiniz.	<b>Veri Koruma Yönetimi</b> Buradan uygulama verilerinin kalıcılığının yönetimi yapılabilirsiniz.	<b>İtibar İstatistikleri</b> Burada raporlama yapılan kullanıcıların istatistiklerini görebilir veya sıralayabiliyorsunuz.
<b>Roksit DNS API Yönetimi</b> Roksit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile giriş için LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.
<b>Whitelist</b> Whitelist yönetimi.	<b>API Konfigurasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcılarının parolarının güvenlik politikası bu ekranдан düzenlenmektedir.

### İçerik Güncelleme

| [Panel](#) / [Ayarlar](#) / İçerik Güncelleme

Sistem E-postalarını Güncelle

Güncelle

Sistem E-postalarının güncellenmesi bu ekranın yapılmaktadır.



## 1.7.5 Syslog Sunucuları

Ayarlar | [Panel](#) / Ayarlar[TR](#)

<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanılabilecek SMTP sunucusu için genel, ayarlar düzenlentir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
<b>İçerik Güncelleme</b> Senaryolar ve İotophane içeriklerinin bulut üzerinde güncellemesini sağlar.	<b>SysLog Sunucuları</b> <b>SysLog sunucularının ekleme, güncelleme ve silme işlemleri</b>	<b>Yetkilendirme</b> Uygulama rollerinin yetkilendirilmesinin güncellemesi yapılmaktadır.
<b>Virus Total</b> Virus Total için API anahtar değer tarama işlemleri burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcılar üzerinde kurulu olan PhishingReport Plugin'ını kontrol etmeye sahiptir.	<b>Lisans Yönetimi</b> Uygulama lisans ayarlarının yönetimi yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılabilirsiniz.	<b>Veri Koruma Yönetimi</b> Buradan uygulama verilerinin kalışığının yönetimi yapılabilirsiniz.	<b>İtibar İstatistikleri</b> Burada raporlama yapan kullanıcılar istatistiklerine gözlebilir veya sıralayabilirsiniz.
<b>Roksit DNS API Yönetimi</b> Roksit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile giriş için LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish için API anahtar değer tarama işlemleri burdan yapılmaktadır.
<b>Whitelist</b> Whitelist yönetimi	<b>API Konfigurasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcılarının parolarının güvenli politikası bu ekranдан düzenlenmektedir.

SysLog sunucularının ekleme, güncelleme ve silme işlemleri yapılmaktadır.

Syslog Sunucuları | [Panel](#) / [Ayarlar](#) / Syslog Sunucuları[TR](#)

<input type="checkbox"/>	#	Adı	Tı	Host	Tı	Port	Tı	Protokol	Tı	Format	Tı
<input type="checkbox"/>	1	Sys1 UDP		192.168.2.21		5257		UDP		JSON	<a href="#">Test</a> <a href="#">Edit</a>



## 1.7.6 Yetkilendirme

Ayarlar | [Panel](#) / Ayarlar

Yönetim Paneli	SMTP Ayarları	E-posta Şablonları
Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	Kampanyalarda kullanılacak SMTP sunucusu için gerekli, ayarlar düzenlenir.	Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
İçerik Güncelleme	SysLog Sunucuları	Yetkilendirme
Senaryolar ve kategoriye içeriğin bulut üzerinden güncellemesini sağlar.	SysLog sunucularının ekme, güncelleme ve silme işlemleri	Uygulama rollerinin yetkilendirme权限被更新了。
Virus Total	Plugin Yönetimi	Lisans Yönetimi
Virus Total için API anahtar değer tanımlama işlemleri burdan yapılmaktadır.	Kullanıcılar üzerinde kurulu olan PhishingReport Plug-inlerini kontrol etmeyi sağlar.	Uygulama lisanslarının yönetimi yapılmaktadır.
SpamAssassin Yönetimi	Veri Koruma Yönetimi	İtibar İstatistikleri
Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılabilirsiniz.	Burada uygulama verilerinin kalıcılığının yönetimi yapılabılırınız.	Burada raporlama yapan kullanıcılar istatistiklerini görebilir veya sıyrılabılırınız.
Roksit DNS API Yönetimi	LDAP Ayarları	Check Phish
Roksit DNS Uri ve API yönetimi.	LDAP ile giriş için LDAP ayarları düzenlenmektedir.	Check Phish için API anahtar değer tanımlama işlemi burdan yapılmaktadır.
Whitelist	API Konfigurasyon Yönetimi	Parola Politikası
Whitelist yönetimi	API yönetimi burdan yapılmaktadır.	Uygulama kullanıcının parolalarının güvenlik politikası bu ekranın düzenlenmektedir.

Yetkilendirme sadece on-premise çözüm olarak kullanıma açktır. Rollerin görüntüleme, ekleme, silme, başlatma vb yetkileri bu ekran üzerinden tanımlanmaktadır.

<b>Yönetici Rolü</b>	<b>Düzenle</b>
<b>Distributor Rolü</b>	<b>Düzenle</b>
<b>Firma Yöneticisi</b>	<b>Düzenle</b>
<b>Firma Kullanıcısı</b>	<b>Düzenle</b>
<b>Firma Denetçisi</b>	<b>Düzenle</b>
<b>Demo Kullanıcı</b>	<b>Düzenle</b>

“Düzenle” butonu tıklanarak kullanıcı yetkileri düzenlenmektedir.



## Rol Güncelle

| Panel / Ayarlar / Yetkilendirme / Firma Denetçisi

## Firma Denetçisi

- Senaryolar
- Kullanıcılar
- Kampanyalar
- Kotophane
- Şöpheli E-postalar
- Detaylı Sorulama
- Firmalar
- Simülasyon
- Ayarlar

## Yetkiler

- Ekran
- Senaryo Ekleme/Düzenleme
- Senaryo silme

Kullanıcının erişim sağlanması istenilmeyen ya da erişim sağlanması istenilen bölümler için ilgili kutucuk seçilir ya da seçim kaldırılır.

**Yetkilendirme, sizin belirlediğiniz kullanıcıya göre değişiklik gösterecektir. Bu şekilde bir fark olması simülasyonun asıl amacını koruyacaktır.**



## 1.7.7. Virüs Total

Ayarlar | [Panel](#) / Ayarlar

Yönetim Paneli	SMTP Ayarları	E-posta Şablonları
Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	Kampanyalarda kullanıacak SMTP sunucusu için gerekli, ayarlar düzenlenir.	Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmemektedir.
İçerik Güncelleme	SysLog Sunucuları	Yetkilendirme
Ses yolları ve kotonphane içeriklerinin bulut üzerinde güncellenmesini sağlar.	SysLog sunucularının ekme, güncelleme ve silme işlemleri	Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
<b>Virus Total</b>	Plugin Yönetimi	Lisans Yönetimi
Virus Total için API anahtar değer tanımlama işlemleri burdan yapılmaktadır.	Kullanıcılar üzerinde kurulu olan PhishingReport Plugin'ını kontrol etmeye sağlar.	Uygulama lisansının yönetimi yapılmaktadır.
SpamAssassin Yönetimi	Veri Koruma Yönetimi	İtibar İstatistikleri
Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılabilirsiniz.	Buradan uygulama verilerinin kılcalığının yönetimi yapılabilirsiniz.	Burada raporlama yapılan kullanıcıların istatistiklerini görebilir veya sıfırlayabilirsiniz.
Roksit DNS API Yönetimi	LDAP Ayarları	Check Phish
Roksit DNS Uri ve API yönetimi.	LDAP ile giriş için LDAP ayarları düzenlenmemektedir.	Check Phish için API anahtar değer tanımlama işlemleri burdan yapılmalıdır.
Whitelist	API Konfigürasyon Yönetimi	Parola Politikası
Whitelist yönetimi	Aşağıda yer almaktadır.	Uygulama kullanıcılarının parolarının güvenli politikası bu ekranın düzenlenmemektedir.

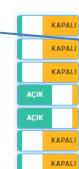
Virus Total | [Panel](#) / [Ayarlar](#) / Virus Total

Virus Total API Anahtarı \*

dd5e0200077ex2751cd450694c199c0365680b7789df1d9e06dc6418285ah

TARAMA AÇMA&KAPAMA<  
Alan Adlarını Tara  
İpleri Tara  
Mail Sunucusu Hostname Tara  
Eski Dosyaları Tara  
Bağlantı Adreslerini Tara  
Bağlantı Adreslerinin Alan Adlarını Tara  
Bağlantı Adreslerinin İplerini Tara

TAG ÖZELLEŞTIRMESİ  
Bağlantı adresi tarama sonucu  
En az  
Eski dosya tarama sonucu  
En az  
Etiketini ekle



**Virus Total API anahtarını girdikten sonra,  
Tarama yapmak istediğiniz kısımları seçin.**

**Belirleyeceğiniz tarama kriterine göre, bu kriterde sahip olan e-posta sayısını belirleyerek ilgili etiketi almasını sağlayın.**

Örn: Bağlantı adresi tarama sonucunu "Açık" ve en az "4" belirlediyseniz; tarama sonucunda 4 bağlantı adresi zararlı tespit edildiyse belirlediğiniz etiketi alır. Sonuç 1,2 ya da 3 ise bu etiketi almaz.



## 1.7.8. Plugin Yönetimi

Ayarlar | [Panel](#) / Ayarlar

<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanılacak SMTP sunucusu için gerekli, ayarlar düzenlenir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta şablonları buradan düzenlenebilir.
<b>İçerik Güncelleme</b> Senaryolar ve kılışphane içeriklerinin bulut üzerinden güncellemesini sağlar.	<b>SysLog Sunucuları</b> SysLog sunucularının ekleme/güncelleme ve silme işlemleri.	<b>Yetkilendirme</b> Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
<b>Virus Total</b> Virus Total için API anahtar değer tarama işlemi burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcılar üzerinde kurulu olan PhishingReport Pluginlerini kontrol etmeyi sağlar.	<b>Lisans Yönetimi</b> Uygulama lisanslarının yönetimi yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılabilirsiniz.	<b>Veri Koruma Yönetimi</b> Buradan uygulama verilerinin kalıcılığının yönetimi yapılabılırınız.	<b>İtibar İstatistikleri</b> Burada raporlama yapan kullanıcıların istatistiklerini görübileceğiniz veya sıfırlayabilirsiniz.
<b>Roksit DNS API Yönetimi</b> Roksit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile giriş için LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish için API anahtar değer tarama işlemi burdan yapılmaktadır.
<b>Whitelist</b> Whitelist yönetimi.	<b>API Konfigurasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcılarının parolarının güvenlik politikası bu ekranın düzenlenmektedir.

Plugin Yönetimi | [Panel](#) / [Ayarlar](#) / Plugin Yönetimi

Pluginler	Plugin İçeriği	Plugin Hataları																								
<table border="1"><thead><tr><th>#</th><th>E-posta Kutusu</th><th>Ip</th><th>Son Güncelleme</th></tr></thead><tbody><tr><td>1</td><td>beamigit@outlook.com</td><td>192.168.0.16</td><td>08.05.2020 11:17:32</td></tr><tr><td>2</td><td>yigit@beamteknoloji.com</td><td>192.168.0.16</td><td>08.05.2020 11:17:32</td></tr><tr><td>3</td><td>cancer_gerze@hotmail.com</td><td>192.168.2.103</td><td>08.05.2020 01:18:17</td></tr><tr><td>4</td><td>canertuncer57@outlook.com</td><td>192.168.2.103</td><td>08.05.2020 01:18:18</td></tr><tr><td>5</td><td>canertuncer57@outlook.com</td><td>192.168.2.103</td><td>08.05.2020 01:18:18</td></tr></tbody></table>	#	E-posta Kutusu	Ip	Son Güncelleme	1	beamigit@outlook.com	192.168.0.16	08.05.2020 11:17:32	2	yigit@beamteknoloji.com	192.168.0.16	08.05.2020 11:17:32	3	cancer_gerze@hotmail.com	192.168.2.103	08.05.2020 01:18:17	4	canertuncer57@outlook.com	192.168.2.103	08.05.2020 01:18:18	5	canertuncer57@outlook.com	192.168.2.103	08.05.2020 01:18:18		
#	E-posta Kutusu	Ip	Son Güncelleme																							
1	beamigit@outlook.com	192.168.0.16	08.05.2020 11:17:32																							
2	yigit@beamteknoloji.com	192.168.0.16	08.05.2020 11:17:32																							
3	cancer_gerze@hotmail.com	192.168.2.103	08.05.2020 01:18:17																							
4	canertuncer57@outlook.com	192.168.2.103	08.05.2020 01:18:18																							
5	canertuncer57@outlook.com	192.168.2.103	08.05.2020 01:18:18																							

Kullanıcılar üzerinde kurulu olan Phishing Report Pluginlerini kontrol etmeyi sağlar. Ayrıca Plugin içeriği ve hataları da incelenebilmektedir.



Plugin içeriği, kullanıcıya raporladığında raporlama ile ilgili ya da herhangi bir sorun olduğunda sorunu bildirmek için gidecek olan mesajların bulunduğu ekrandır.

**Olta.la** uygulamamızdan yapılan bir simülasyonun e-postası raporlandığında, kullanıcıya gidecek olan mesajdır. İstediğiniz gibi özelleştirin.

Kullanıcı bir e-posta raporladığında gidecek olan mesajdır. İstediğiniz gibi özelleştirin.



#	Plugin Hata Mesajı	Plugin Uyanı Konusu	Plugin Uyanı Mesajı	Son Güncelleme
1	Öğe tasnimis ya da silinmis.	Mesaj İçeriği Hatası	Mesaj içeriğine erişken hata oluştu.	09.06.2020 17:42:32
2	Öğe tasnimis ya da silinmis.	Silinmis Öğeler Dosya Yolu	Silinmiş öğeler dosya yoluna erişilken hata oluştu	09.06.2020 17:42:33
3	Öğe tasnimis ya da silinmis.	E-posta Raporlama İsteği Genel hata	Sunucuya istek gönderilemedi	09.06.2020 17:42:34
4	Unexpected character encountered while parsing value: <. Path "", line 0, position 0.	Sunucu Cevabı Hatası   hande.alp@beamteknoloji.com.j	Sunucudan cevap alınamadı.	24.06.2020 16:52:03

Pluginler ile ilgili hataların, konu ve mesaj olarak bilgisinin bulunduğu ekrandır.



## 1.7.9. Lisans Yönetimi

Ayarlar | [Panel / Ayarlar](#)[TR](#)

<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanılacak SMTP sunucusu için gerekli, ayarlar düzenlenir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
<b>İçerik Güncelleme</b> Senaryolar ve kütüphane içeriklerinin bulut üzerinde güncellemesini sağlar.	<b>SysLog Sunucuları</b> SysLog sunucularının ekme, güncelleme ve silme işlemleri.	<b>Yetkilendirme</b> Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
<b>Virus Total</b> Virus Total için API anahtar değerin tanımlama işlemleri burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcılar üzerinde kurulu olan PhishingReport Plugini'ni kontrol etmeye sahiptir.	<b>Lisans Yönetimi</b> Uygulama lisans ayarlarının yönetimi yapılmaktadır. 
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimini yapabilirsiniz.	<b>Veri Koruma Yönetimi</b> Burada uygulama verilerinin kılavuzun yönetimi yapılmaktadır.	<b>İtibar İstatistikleri</b> Burada raporlama yapan kullanıcılar istatistiklerini görebilir veya sıralayabilmektedir.
<b>Roksit DNS API Yönetimi</b> Roksit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile giriş için LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish için API anahtar değerin tanımlama işlemleri burdan yapılmaktadır.
<b>Whitelist</b> Whitelist yönetimi.	<b>API Konfigurasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcılarının parolalarının güvenlik politikası bu ekranın düzenlenmektedir.

Lisans Yönetimi | [Panel / Ayarlar / Lisans Yönetimi](#)

Tip: \*

Başlangıç Tarihi: \*

Bitiş Tarihi: \*

Uygulama lisans ayarlarının yönetiminin yapıldığı ekranıdır.

1/2



## 1.7.10. SpamAssassin Yönetimi

Ayarlar | Panel / Ayarlar

[C](#) [Kullanıcı](#)

Yönetim Paneli Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	SMTP Ayarları Kampanyalarda kullanılabilecek SMTP sunucusu için gerekli, ayarlar düzenlenir.	E-posta Şablonları Sistem tarafından gönderilen e-posta şablonları buradan düzenlenebilir.
İçerik Güncelleme Sınırlar ve kılınçlara içeriğin en son güncelleme sağlar.	SysLog Sunucuları SysLog sunucularının eklenme/güncelleme ve silme işlemleri.	Yetkilendirme Uygulama rollerinin yetkilendirilmesini güncellemesi yapılmaktadır.
Virus Total Virus Total için API anahtar değerin tarama işlemleri burdan yapılmaktadır.	Plugin Yönetimi Kullanıcılar üzerinde kurulu olan PhishingReport Pluginlarını kontrol etmeye sağlanır.	Lisans Yönetimi Uygulama lisanslarının yönetimi yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılabilir.	Veri Koruma Yönetimi Buradan uygulama verilerinin kalıcılığını yönetimi yapılmaktadır.	İtibar İstatistikleri Burada raporlama yapılan kullanıcıların istatistiklerini görebilir veya sıfırlayabilirsiniz.
Rokit DNS API Yönetimi Rokit DNS Uri ve API yönetimi.	LDAP Ayarları LDAP ile giriş için LDAP ayarları düzenlenmektedir.	Check Phish Check Phish için API anahtar değerin tarama işlemleri burdan yapılmaktadır.
Whitelist Whitelist yönetimi.	API Konfigurasyon Yönetimi API yönetimi burdan yapılmaktadır.	Parola Politikası Uygulama kullanıcının parolalarının güvenlik politikası bu ekranın düzenlenmesi gerekmektedir.

Spam Assassin Yönetimi | Panel / Ayarlar / Spam Assassin Yönetimi

[C](#) [Kullanıcı](#)

The screenshot shows the 'Spam Assassin Yönetimi' (Spam Assassin Settings) page. In the top left, there's a 'Threshold' input field containing the value '2'. To its right is a 'Etiketler' (Labels) section with a 'Yeni etiket ekle' (Add new label) button and a 'Kaydet' (Save) button. A dropdown menu is open over the 'Etiketler' section, showing various label names: SA-SPAM, VT-PENDING, VT-CLEAN, VT-MALICIOUS, PT-PHISHING, YARA\_SPAM\_1, BLACKLISTED, test, and MNIL\_FEED. The 'SA-SPAM' option is currently selected. A blue arrow points from the 'Threshold' input field towards the 'Etiketler' section, indicating the relationship between the two.

Threshold sayısı; puan sınırı olarak düzenlenip, belirlenecek olan ya da yeni oluşturulacak etiketin, bu sınırı aşıldığında etiketin atanması anlamına gelmektedir.



## 1.7.11. Veri Saklama Yöntemi

Ayarlar | [Panel / Ayarlar](#)[C](#)

<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanılacak SMTP sunucusu için gerekli, ayarlar düzenlenir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
<b>İçerik Güncelleme</b> Seçenekler ve katalogda içeriklerin bütçeden güncellenmesini sağlar.	<b>SysLog Sunucuları</b> SysLog sunucularının ekleme, güncelleme ve silme işlemleri.	<b>Yetkilendirme</b> Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
<b>Virus Total</b> Virus Total için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcılar üzerinde kurulu olan PhisingReport Plugin'larını kontrol etmeye sağlar.	<b>Lisans Yönetimi</b> Uygulama lisans ayarlarının yönetimi yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradı uygulamanın SpamAssassin ayarlarının yönetimi yapılabilirsiniz.	<b>Veri Koruma Yönetimi</b> Buradı uygulama verilerine katkıdağın yönetimi yapılabilirsiniz. 	<b>İtibar İstatistikleri</b> Burada raporlama yapan kullanıcılar istatistiklerini görebilir veya sıralayabilirsiniz.
<b>Roksit DNS API Yönetimi</b> Roksit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile giriş için LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.
<b>Whitelist</b> Whitelist yönetimi	<b>API Konfigurasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcılarının parolarının güvenlik politikası bu ekranдан düzenlenmektedir.

Veri Saklama Yönetimi | [Panel / Ayarlar / Veri Saklama Yönetimi](#)[C](#)

<b>Plugin Verileri</b>	
Durumu	<input checked="" type="checkbox"/>
Sıkıştırma	<input checked="" type="checkbox"/>
Plani zamanda başlat	<input checked="" type="checkbox"/>
Hemen başlat	<input type="checkbox"/>
Sıkılık arası	<input type="text"/>
Gen	<a href="#">▼</a>
<b>Geçmiş Veriler</b>	
Durumu	<input checked="" type="checkbox"/>
Sıkıştırma	<input checked="" type="checkbox"/>
Plani zamanda başlat	<input checked="" type="checkbox"/>
Hemen başlat	<input type="checkbox"/>
Sıkılık arası	<input type="text"/>
Gen	<a href="#">▼</a>

Kullanıcının belirleyeceği zaman aralığında, plugin ya da geçmiş veriler ile ilgili (raporlanan e-postalar ya da plugin işlemleri gibi) saklama işlemlerinin sağlanabileceği ekranıdır.



## 1.7.12. İtibar İstatistikleri

Ayarlar | Panel / Ayarlar



Yönetim Paneli Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	SMTP Ayarları Kampanyalarda kullanıacak SMTP sunucusu için gerekli, ayarlar düzenlenir.	E-posta Şablonları Sistem tarafından gönderilen e-posta şablonları buradan düzenlenebilir.
İçerik Güncelleme Senaryolar ve kütüphane içeriğinin butucu üzerinden güncelleme sağlar.	SysLog Sunucuları SysLog sunucularının ekleme, güncelleme ve silme işlemleri.	Yetkilendirme Uygulama rollerinin yetkilendirilmesini güncelleme yapmaktadır.
Virus Total Virus Total için API anahtar değerini taramma işlemleri burdan yapılmaktadır.	Plugin Yönetimi Kullanıcılar üzerinde kurulu olan PhisingReport Plugini'ni kontrol etmeye sağlar.	Lisans Yönetimi Uygulama lisans ayarlarının yönetimi yapılmaktadır.
SpamAssassin Yönetimi Buradan uygulamanın SpamAssassin ayarlarını yönetimi yapabilirsiniz.	Veri Koruma Yönetimi Buradan uygulama verilerinin kaçışının yönetimi yapılabılır.	İtibar İstatistikleri Burada raporlama yapılan kullanıcılar statisitiklerine göre bilgi veya sıfırlayabilirisiniz.
Roksit DNS API Yönetimi Roksit DNS Uri ve API yönetimi.	LDAP Ayarları LDAP ile giriş için LDAP ayarları düzenlenmektedir.	Check Phish Check Phish için API anahtar değerini taramma işlemleri burdan yapılmaktadır.
Whitelist Whitelist yönetimi	API Konfigurasyon Yönetimi API yönetimi burdan yapılmaktadır.	Parola Politikası Uygulama kullanıcılarının parolarının güvenlik politikası bu ekranдан düzenlenmektedir.

Şüpheli E-postaları raporlayan ve analiz kısmında otomatik ya da manuel olarak **"Sonuç"** bölümünü **"Sonuçlandı"** olarak belirleyen kullanıcıların raporlama istatistiklerini inceleyebilir ya da sıfırlama işleme yapabilirsiniz.

#	E-posta Adresi	Spam Sayısı	Toplam Raporlama	Skor
1	beamigit@outlook.com	8	24	★★★★★
2	yigit@beamteknoloji.com	29	46	★★★★★
3	cancer.tuncer@beamteknoloji.com	2	5	★★★★★
4	cancer_gerze@hotmail.com	0	1	★★★★★
5	yaparkadir@outlook.com.tr	0	1	★★★★★
	hande.alp@beamteknoloji.com	0	1	★★★★★

**Taramaya Etkisi** butonu ile tarama ve raporlama sonucunda skorlama yapılmasını ya da yapılmaması aksiyonunun belirleyin.

**Skor Temizle** işlemi yapmak için, kullanıcının bulunduğu kutucuğu seçerek skor bilgilerini silin.



### 1.7.13. Roksit DNS API Yönetimi

Ayarlar | Panel / Ayarlar

Yönetim Panelli  
Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.

SMTP Ayarları  
Kampanyalarda kullanılabilecek SMTP sunucusu için gerekli, ayarlar düzenlenir.

E-posta Sablonları  
Sistem tarafından gönderilen e-posta sablonları buradan düzenlenmektedir.

İçerik Güncelleme  
Sesçiyolar ve kategoriye içeriklerin bulunduğu türden güncelleme sağlar.

SysLog Sunucuları  
SysLog sunucularının eklenmesi, güncelleme ve silme işlemleri.

Yetkilendirme  
Uygulama rolesinin yetkilendirilmesini güncelleme yapmaktadır.

Virus Total  
Virus Total için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.

Plugin Yönetimi  
Kullanıcılar üzerinde kurulu olan PhishingReport Plugin'ını kontrol etmemeyi sağlar.

Lisans Yönetimi  
Uygulama lisans ayarlarını yönetmektedir.

SpamAssassin Yönetimi  
Buradan uygulananen SpamAssassin ayarlarını yönetmeni yapabilirsiniz.

Veri Koruma Yönetimi  
Buradan uygulama verilerinin kalıcılığını yönetmeni yapabilirsiniz.

Roksit DNS API Yönetimi  
Roksit DNS Url ve Api yönetimi.

Roksit DNS Url ve API Yönetimi ayarlarını yapın.

Roksit Yönetimi | Panel / Ayarlar / Roksit Yönetimi

Roksit URL  
Lütfen Roksit Url adresini giriniz.

Roksit ApiKey  
Lütfen Roksit ApiKey değerini giriniz.

Test Kaydet

Roksit URL adresi ve Roksit ApiKey bilgilerini girin, analizini başlatın.



## 1.7.14. LDAP Ayarları

Ayarlar | [Panel](#) / Ayarlar

Yönetim Paneli	SMTP Ayarları	E-posta Şablonları
Uygulama kullanıcı hesaplarının önemini için kullanılmaktadır.	Kampanyalarda kullanılabilecek SMTP sunucusu için gerekli ayarlar düzenlenir.	Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmemektedir.
İçerik Güncelleme	SysLog Sunucuları	Yetkilendirme
Senaryolar ve kötüphane içeriğinin bolut özenden güncellemesini sağlar.	SysLog sunucularının eklenme/güncelleme ve silme işlemleri	Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
Virus Total	Plugin Yönetimi	Lisans Yönetimi
Virus Total için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.	Kullanıcılar üzerinde kurulu olan PhishingReport Plugin'ını kontrol etmeye sahiptir.	Uygulama lisanslarının yönetimi yapılmaktadır.
SpamAssassin Yönetimi	Veri Koruma Yönetimi	İtibar İstatistikleri
Burdan uygulamanın SpamAssassin ayarlarının yönetimi yapılmaktadır.	Buradan uygulama verilerinin kaçırdığının yönetimi yapılmaktadır.	Burada raporlama yapan kullanıcılar statistiklerini görebilir veya sıfırlayabilirsiniz.
Roksit DNS API Yönetimi	LDAP Ayarları	Check Phish
Roksit DNS Uri ve API yönetimi.	LDAP ile giriş için LDAP ayarları düzenlenmektedir.	Check Phish için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.
Whitelist	API Konfigurasyon Yönetimi	Parola Politikası
Whitelist yönetimi	API yönetimi burda yapılmaktadır.	Uygulama kullanıcılarının parolarının güvenlik politikası bu ekranın düzenlenmektedir.

LDAP ile giriş yapmak için kullanın.

LDAP Ayarı Ekle | [Panel](#) / [LDAP Konfigurasyon Listesi](#) / LDAP Ayarı Ekle

LDAP Sunucusu Erişim Bilgileri

URL \*  
eg. https://ad-host:636, http://ad-host:389

UserOn \*  
CN=Administrator,DC=ulta,DC=ta

Parola \*

Test et

Sorgulama

Konfigürasyon Adı \*

LDAP konfigürasyonları özelleştirmek için konfigürasyon adı girilmelidir.

BaseOn \*

LDAP sorulduğunda yapılmışlıkla döndürülür.

User Object Category \*

Person

LDAP tabanında bulunan kullanıcıların sorulduğumda kullanılabilek için kullanılabilek nesne kategorisi girilmelidir.

Özellikler

Kullanıcı Adı Özelliği  
name

LDAP veritabanından kullanıcı adına referans için gerekli attribute türü girilmelidir.

Kullanıcı Soyadı Özelliği \*

ssn

LDAP konfigürasyonu için gerekli olan ayarları gerçekleştirin.

Uygulamaya giriş yaparken “**LDAP ile Giriş**” seçeneği ile Active Directory bilgilerinizle kolayca giriş yapın.



## 1.7.15. Check Phish

Ayarlar | [Panel](#) / Ayarlar[TR](#)

<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanılacak SMTP sunucusu için gerekli, ayarlar düzenlenir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta sablonları buradan düzenlenemektedir.
<b>İçerik Güncelleme</b> Senaryolar ve kılçephane içeriklerinin bulut üzerinden güncellemesini sağlar.	<b>SysLog Sunucuları</b> SysLog sunucularının ekmele,güncelleme ve silme işlemleri.	<b>Yetkilendirme</b> Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
<b>Virus Total</b> Virus Total için API anahtar değer tanımlama işlemleri burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcılar özürde kurulu olan PhishingReport Plugin'ını kontrol etmeyi sağlar.	<b>Lisans Yönetimi</b> Uygulama lisans ayarlarının yönetimi yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimini yapabilirsiniz.	<b>Veri Koruma Yönetimi</b> Buradan uygulama verilerinin kılcalanın yönetimini yapabilirsiniz.	<b>İtibar İstatistikleri</b> Burada raporlama yapan kullanıcılar statistiklerini görebilir veya sıfırlayabilirsiniz.
<b>Roksit DNS API Yönetimi</b> Roksit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile gerekli LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish için API anahtar değer tanımlama işlemleri burdan yapılmaktadır. 
<b>Whitelist</b> Whitelist yönetimi	<b>API Konfigurasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcılarının parotanının güvenlik politikası bu ekranın düzenlenemektedir.

Check Phish | [Panel](#) / Ayarlar / Check Phish[TR](#)

Check Phish API Anahtarı \*

zeod69m280z84lrethbawnsai19ifviodsumvslbyskfae64gpuvr8eviupha

Check Phish için API anahtar değeri tanımlama işlemi yapın.



## 1.7.16. WhileList

Ayarlar | [Panel](#) / Ayarlar[TR](#)

<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanılacak SMTP sunucusu için gereki, ayarlar düzenlenir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
<b>İçerik Güncelleme</b> Senaryolar ve kütüphane içeriklerinin bulut üzerinden güncellemesini sağlar	<b>SysLog Sunucuları</b> SysLog sunucularının ekleme,güncelleme ve silme işlemi	<b>Yetkilendirme</b> Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
<b>Virus Total</b> Virus Total İzin API anahtar değer taramama işlemleri burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcılar üzerinde kurulu olan PhishingReport Pluginlarını kontrol etmeyi sağlar.	<b>Lisans Yönetimi</b> Uygulama lisanslarının yönetimi yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılmaktadır.	<b>Veri Koruma Yönetimi</b> Buradan uygulama verilerinin kılavuzun yönetimi yapılmaktadır.	<b>İtibar İstatistikleri</b> Burada raporlama yapan kullanıcılar istatistiklerini görebilebilir veya sıfırlayabilirsiniz.
<b>Rokit DNS API Yönetimi</b> Rokit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile giriş için LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish İzin API anahtar değer taramama işlemleri burdan yapılmaktadır.
<b>Whitelist</b> <small>Whitelist yönetimi</small>	<b>API Konfigurasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcılarının parolalarının güvenlik politikası bu ekranдан düzenlenmektedir.

Whitelist Yönetimi | [Panel](#) / [Ayarlar](#) / Whitelist Yönetimi[TR](#) [+ Ekle](#)

#	Alan Adı	DKIM	SPF	DMARC	İşlemler
1	turkiyefinans.com.tr	✓	✓	✓	
2	google.com	✓	✓	✓	
3	beamteknoloji.com	✓	✓	✗	

Toplam 3 kayttan 1 - 3 arası gösterilmektedir.

Alan adlarının DKIM, SPF ve DMARC kayıtlarının durumunu belirleyerek;  
tanımladığınız alan adlarını whitelist e tanımlayabilirsiniz.



### 1.7.17. API Konfigürasyon Yönetimi

Ayarlar | [Panel](#) / Ayarlar[Cz](#)

<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetimi için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanıacak SMTP sunucusu için gerekli, ayarlar düzenlenir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
<b>İçerik Güncelleme</b> Senaryolar ve Kotiphane içeriklerinin bulut üzerinde güncellenmesini sağlar	<b>SysLog Sunucuları</b> SysLog sunucularının eklenme, güncelleme ve silme işlemleri	<b>Yetkilendirme</b> Uygulama rollerinin yetkilendirilmesinin güncellenmesi yapılmaktadır.
<b>Virus Total</b> Virus Total içeriği API anahtar değer tarama işlemleri burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcılar özneinde kurulu olan PhishingReport Plugin'ını kontrol etmeli sağırlar.	<b>Lisans Yönetimi</b> Uygulama lisans ayarlarını yönetme yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılabilirsiniz.	<b>Veri Koruma Yönetimi</b> Buradan uygulama verilerinin kılavuzlu yönetimi yapılabilirsiniz.	<b>İtibar İstatistikleri</b> Burada raporlama yapılan kullanıcılar istatistiklerini görüntüleyebilir veya sıfırlayabilirsiniz.
<b>Roksit DNS API Yönetimi</b> Roksit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile giriş için LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish içeriği API anahtar değer tarama işlemleri burdan yapılmaktadır.
<b>Whitelist</b> Whitelist yönetimi	<b>API Konfigürasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcılarının parolalarının güvenlik politikası bu ekranın düzenlenmektedir.

### Api Konfigurasyon Yönetimi

| [Panel](#) / [Ayarlar](#) / Api Konfigurasyon Yönetimi[Kaydet](#)

White List	<input type="checkbox"/>
Virus Total	<input checked="" type="checkbox"/>
CyThreat	<input checked="" type="checkbox"/>
Phish Tank	<input checked="" type="checkbox"/>
URL Haus	<input checked="" type="checkbox"/>
Check Phish	<input checked="" type="checkbox"/>
BlackList	<input checked="" type="checkbox"/>
OTX	<input checked="" type="checkbox"/>
Spamassassin	<input checked="" type="checkbox"/>
USOM	<input checked="" type="checkbox"/>



API konfigürasyon yönetiminde bulunan uygulamaların, şüpheli e-posta analizinde devrede olması için “açık” ya da analizin yapılması istemediğiniz bir uygulama varsa “kapalı” olarak durumunu belirleyin.



## 1.7.18. Parola Politikası

Ayarlar | Panel / Ayarlar



<b>Yönetim Paneli</b> Uygulama kullanıcı hesaplarının yönetim için kullanılmaktadır.	<b>SMTP Ayarları</b> Kampanyalarda kullanılabilecek SMTP sunucusu için gerekli, ayarlar düzenlenir.	<b>E-posta Şablonları</b> Sistem tarafından gönderilen e-posta şablonları buradan düzenlenmektedir.
<b>İçerik Güncelleme</b> Senaryolar ve kategoriye taraflanan bulut üzerinden güncellemesini sağlar.	<b>SysLog Sunucuları</b> SysLog sunucularının eklemeye, güncelleme ve silme işlemleri.	<b>Yetkilendirme</b> Uygulama roollen yetkilendirilmesine gereklenmesi yapılmaktadır.
<b>Virus Total</b> Virus Total için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.	<b>Plugin Yönetimi</b> Kullanıcılar üzerinde kurulu olan PhisingReport Plugin'ını kontrol etmeye sağlar.	<b>Lisans Yönetimi</b> Uygulama lisanslarının yönetimi yapılmaktadır.
<b>SpamAssassin Yönetimi</b> Buradan uygulamanın SpamAssassin ayarlarının yönetimi yapılmaktadır.	<b>Veri Koruma Yönetimi</b> Buradan uygulama verilerinin kalıcılığını yönetimi yapılmaktadır.	<b>İtibar İstatistikleri</b> Burada raporlama yapan kullanıcıların istatistiklerini görebilir veya sıfırlayabilirsiniz.
<b>Roksit DNS API Yönetimi</b> Roksit DNS Uri ve API yönetimi.	<b>LDAP Ayarları</b> LDAP ile giriş için LDAP ayarları düzenlenmektedir.	<b>Check Phish</b> Check Phish için API anahtar değerini tanımlama işlemleri burdan yapılmaktadır.
<b>Whitelist</b> Whitelist yönetimi.	<b>API Konfigurasyon Yönetimi</b> API yönetimi burdan yapılmaktadır.	<b>Parola Politikası</b> Uygulama kullanıcılarının parolalarının güvenlik politikası bu ekranın düzenlenmesiyle.

Parola Politikası Ekle | Panel / Ayarlar / Parola Politikası / Parola Politikası Ekle



<b>Adı</b> <input type="text"/>	<b>Roller</b> <input type="text"/> Ara... <input type="text"/> Ara... Seçilebilir Roller Demo Kullanıcı (ROLE_DEMO) Firma Yöneticisi (ROLE_MANAGER) Yönetici Rolü (ROLE_ADMIN) Firma Denetçisi (ROLE_AUDITOR) Firma Kullanıcısı (ROLE_USER) Seçilmiş Roller
<b>Açıklama</b> <input type="text"/>	<b>Hesaplar</b> <input type="text"/> Ara... <input type="text"/> Ara... Seçilebilir Hesaplar admin@response user@response team@olta.la user responsiblesans@getnada.com Seçilmiş Hesaplar
<b>Karakter Kümlesi</b> <input type="checkbox"/> Boyuk Harf <input type="checkbox"/> Küçük Harf <input type="checkbox"/> Sayısal Karakter <input type="checkbox"/> İşaret	
<b>Minimum Parola Uzunluğu</b> <input type="text"/> -1 Parola uzunluğu minimum seçili uzunlık kadar olacaktır. -1 değeri bu özellilik deven dura break.	
<b>Parola Ömrü</b> <input type="text"/> -1 Parola belirtilen sayıda gün sonunda yenilenmeye zorlanacaktır. -1 değeri bu özellilik deven dura break.	
<b>Gecmiş Parolalar</b> <input type="text"/> -1 Belirtilen sayıda geçmiş parola bilgisi kullanılamayacaktır. -1 değeri bu özellilik deven dura break.	
<b>Sıradaki Değişiklik</b> <input type="text"/> -1 Belirtilen sayıda gecikme parola bilgisi değiştirelmeyecektir. -1 değeri bu özellilik deven dura break.	
<b>Politikayı Çaprazlı</b> <input type="checkbox"/> Politikayı çaprazlaştırmak için seçili hale getirin.	<b>Varsayılan mı?</b> <input type="checkbox"/> Herhangi bir politika ortaklığı varsa onun politikası uygulanır.

Uygulama kullanıcılarının parolalarının güvenlik politikası bu ekranın düzenlenmektedir.

Belirlediğiniz kurallara göre bir parola politikası oluşturun.

**Rollere ya da hesaplara göre bu politikayı kişilere uygulayın.**