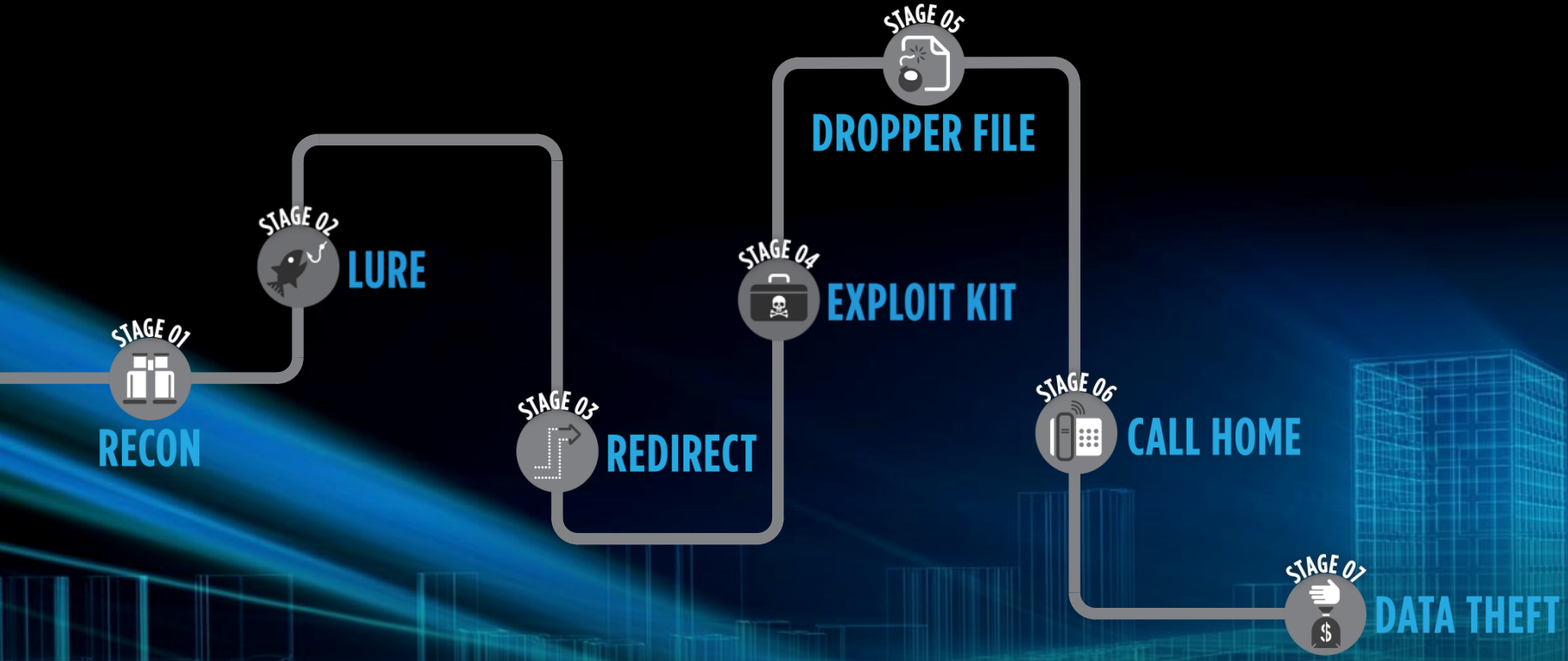
websense
TRITON APX
ADVANCED PROTECTION

Turkcell & PTT fatura zararlısı

Kemal ARTIKARSLAN
kartikarslan@websense.com
MART 2015

Modern Ataklar (APT / Malware) hedefine nasıl ulaşır ?

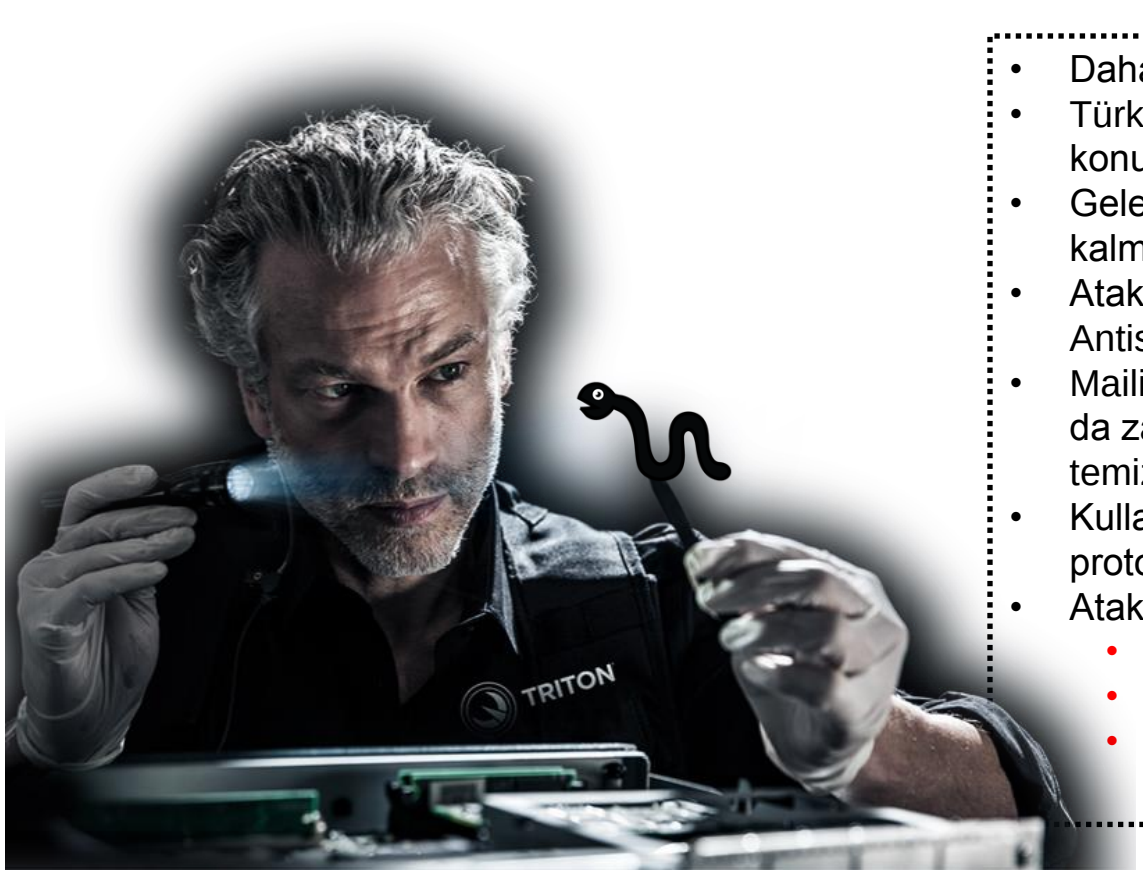


2015 yılında ne bekliyoruz demiştik ?

websense®

1. Help! Call the IT Doctor. My hospital is under attack - again!
2. Your refrigerator is not an IT security threat. Industrial sensors are.
3. Credit card breaches are the least of your worries.
4. You are Only Who Your Phone Says You Are.
5. Open Source or Open Door?
6. Email threats are evolving.
7. Google Docs controls the bot.
8. New cyber war players take a seat at the table.

Atağın DNA’sı ve elde edilen bulgular



- Daha zekice tasarlanmış bir atak çeşididir.
- Türkiye bu tarz ataklarla baş başa kalan 5. ülke konumundadır.
- Geleneksel çözümlerin bir çoğu çaresiz kalmıştır kalmaya devam edecektir.
- Atak mail yoluyla başlamakta ve Antivirüs ve Antispam çözümlerini kolaylıkla atlabilmektedir.
- Mailin içerisinde herhangi bir virüs , spam ya da zararlı obje imzası yerine sadece basit ve temiz gibi görünen linkler bulunmaktadır.
- Kullandıkları linkler sürekli değişmekte ve SSL protokolü kullanılmaktadır.
- Atakların amacı değişiklik göstermektedir.
  - *Proxy bypass aktiviteleri tespit edilmiştir.*
  - *Şifreleme aktiviteleri tesbit edilmiştir.*
  - *Backdoor oluşturarak bilgi çalmaya yönelik aktiviteler tespit edilmiştir.*

STAGE 2 → LURE → Saldırganlar tarafından gönderilen eposta ve içerikleri

STAGE 02 LURE

STAGE 03 REDIRECT

Mail olarak gelen değişken Redirection linkleri;

- *http://turkcell-servis.com*
- *http://turkcell-fatura.org*
- *http://turkcell-fatura.biz*
- *http://turkcell-servis.net*
- *http://ptt-tracking.net*
- *http://ptt-posta.biz*
- *http://ptt-posta.org*
- *http://ptt-cargo.info ve diğerleri...*

Bu bilinçli yapılan bir saldırı. Adresler ve içerik sürekli değişiyor,Email Antispam Gateway, URL filtreleme, Antivirüs , Firewall vb sistemleriniz üzerinde statik kurallar yazarak kendinizi kandırmaya çalışmayın.

LURE

Bu aşamada siber suçlular , Recon aşamasında ele geçirdikleri bilgileri kullanarak insanların ilgisini çekecek zararsız gibi görünen eposta , sosyal medya mesajı , link vb cazip içerikler yaratır. Burada asıl amaç, servis yapılan kişileri cazip bir içerikyardımıyla bazı sayfalara yönlendirmek ve tuzağa düşürmektir. İlgili ataktan anlaşılacağı üzere bu epostalar ; sanki güvenilir bir yerden geliyormuş gibi görünüyor ve içerisinde kullanıcıların ilgisini çeken bazı linkler barındırıyor.

STAGE 3 → REDIRECTION→ Eposta içerisine yerleştirilen masum linkler

STAGE 03 **REDIRECT** → STAGE 04 **EXPLOIT KIT**

Redirection linkleri sonrası exploit kitlerin bulunduğu değişken web sayfaları;

- *https://copy.com/blablabla/PTT_Adres_Form.zip*
- *https://copy.com/blabla/Turkcell_Fatura_789180.zip*

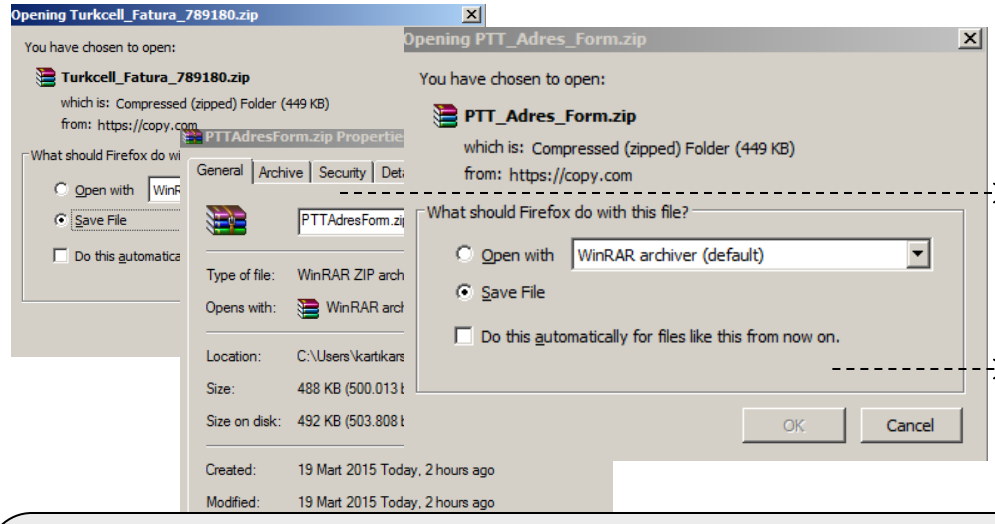
SSL protokolü özellikle tercih edilmiş, adresler ve içerik <u>sürekli değişiyor</u>, URL filtreleme, Antivirüs , Firewall vb sistemleriniz üzerinde statik kurallar yazarak kendinizi kandırmaya çalışmayın. Ayrıca içeriği anlayan bir güvenlik sistemine sahip değilseniz büyük ihtimalle copy.com adresi güvenilir olarak yorumlanacaktır.

REDIRECT

Siber suçlular , Lure aşamasında kullandıkları linkler yardımıyla exploit kit , malware vb şiflenmiş / gizlenmiş zararlı kodları n dağılmasını sağlar. İlgili ataktan anlaşılacağı üzere lure aşamasında kullanılan linklere tıklayan bir kişi , Antivirüs sistemleri tarafından tesbit edilemeyen zararlı bir kodun barındığı güvenilir gibi görünen bir sayfaya yönlendiriliyor ve bu zararlı kod ya da exploit kit kullanıcı bilgisayarına download edilliyor.

STAGE 4→ EXPLOIT KIT → Download edilen ilk dosyalar

STAGE 04 **EXPLOIT KIT** - → STAGE 05 **DROPPER FILE**



AV yazılımları tarafından tesbit edilemeyen sıkıştırılmış dosyalar içerisindeki zararlı uygulamalar çalıştırıldıktan sonra ; dropper file ve C&C aktivitesi için root sertifikalar aşağıdaki adres yardımıyla güncelleniyor

- *http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt*

Saldırganın ele geçirdiği sunucular yardımıyla aşağıdaki dosyalar download edilerek payload işlemi tamamlanıyor.

- *C:\WINDOWS\eqojewaw.exe*
- *C:\WINDOWS\atokuten.exe*
- *C:\WINDOWS\jguqhkix.exe*

EXPLOIT KIT

Siber suçlular , Redirection yardımıyla zararlı bir web sayfasına yönlendirdikleri kişilerin bilgisayarına ; sıfır gün atağına sebep olabilecek ya da arka kapılar oluşturan bazı zararlı kodların alınması için exploit kitler yerleştirmeye çalışır. Bu ataktan anlaşılacağı üzere siber suçluları atağın boyutunu genişletmek için kullanacakları daha zararlı yazılımları bilgisayara download etmek ve otomatik olarak çalışması nı sağlamak için yani dropper file aşaması ve C&C iletişimi için bu adımı kullanıyor.

Download edilen dosyalara karşı AV sistemleri

virustotal

SHA256: ef8ad30fed3ee65fe48c6309d0351e3c35d375718c45a5e932ad1ef933565269

Dosya adı: PTT_Adres_Form.exe

Tespit edilme orani 2/57

virust

SHA256: 221c7b1353b7b5ddca5bcf05bd6c4070f80a81ce28c690e2d9a32d366665eb4a

File name: PTTAdresForm.exe

Detection ratio: 3 / 57

SHA256: ef8ad30fed3ee65fe48c6309d0351e3c35d375718c45a5e932ad1ef933565269

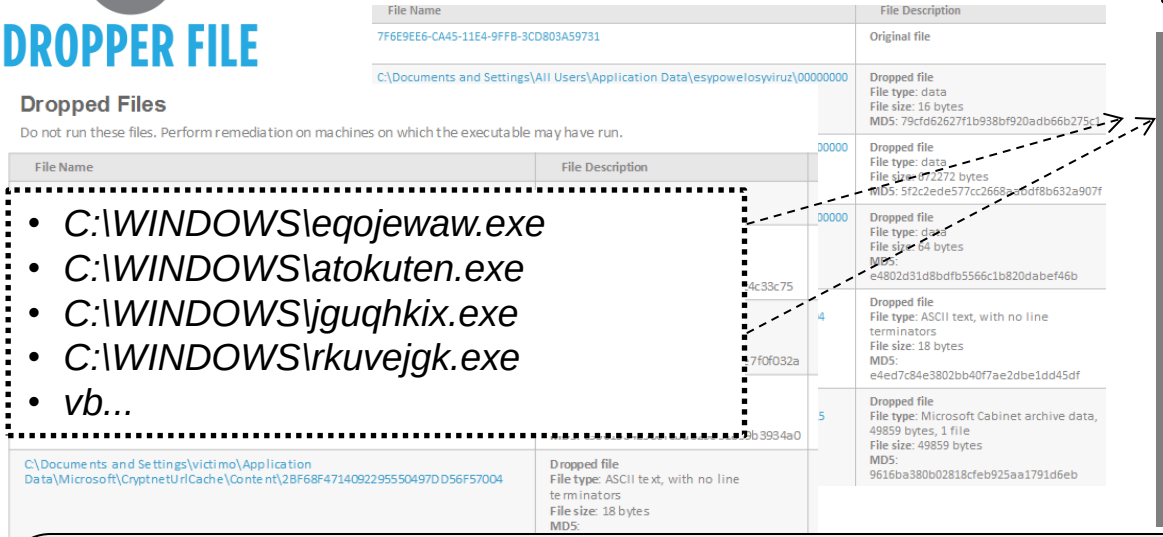
File name: Turkcell_Fatura_789180.exe

Detection ratio: 4/57

Analysis date: 2015-03-12 18:04:24 UTC (2 days, 21 hours ago)

STAGE 5→ DROPPER FILE → Download edilen diğer zararlı kodlar

DROPPER FILE



- *C:\WINDOWS\eqojewaw.exe*
- *C:\WINDOWS\atokuten.exe*
- *C:\WINDOWS\jguqhkix.exe*
- *C:\WINDOWS\rkuvejgk.exe*
- *vb...*

CALL HOME

Payload işlemleri sonrası sisteme yerleşen kodlar saldırgana ait olan C&C sunucularıyla SSL kanalından haberleşiyor ve kullanıcı botnet ağının bir parçası oluyor.

Rusya 77.246.147.172:443 → spring-knock.ru
Ukrayna 185.86.76.94:443 → yourdatamydata.ru

Botnet ağının parçası olan bir bilgisayar aşağıdaki işlemleri yapabiliri.

- *DoS atak yapabilir*
- *Proxy gibi hizmet verebilir*
- *Spam gönderebilir*
- *Data ve Network trafiğini inspect edebilir*
- *Veri , erişim hesabı , şifre vb sızıtıntılara neden olabilir.*

DROPPER FILE

Siber suçlular , exploit kitler yardımıyla ele geçirdiği bilgisayarlar üzerinde atağın boyutunu genişletmek ve data çalmak özellikle bilgisayarı bir botnet ağının kölesi yapmak için ele geçirilmiş bir başka sunucu üzerindeki hatta antivirüs yazılımları tarafından tespit edilemeyen çalışabilir zararlı dosyayları bilgisayara yerleştirir. Bazı dropper file uygulamaları güvenlik sistemleri tarafından algılanmamak için uykuda bekler ve zamanı geldiğinde aktif olur. Aynı zamanda bu aşama da gerektiğinde ek dropper file aktiviteleri gerçekleştirilir.

STAGE 6 → CALL HOME / BOTNET→ Erişilmeye çalışılan IP Adresleri

STAGE 06 **CALL HOME** → STAGE 07 **DATA THEFT**

Network Access

The analyzed file requested the following IP addresses.

Destination IP Address	Local Port	Process
77.246.147.172:443	1048	C:\WINDOWS\explorer.exe
[illegible]	[illegible]	C:\WINDOWS\explorer.exe
77.246.147.172:443	[illegible]	C:\WINDOWS\explorer.exe
77.246.147.172:443	1051	C:\WINDOWS\explorer.exe

Network Access

The analyzed file requested the f

Destination IP Address	Local	
185.86.76.94:443	1063	
185.86.76.94:443	1064	
185.86.76.94:443	1065	
185.86.76.94:443	1066	C:\WINDOWS\explorer.exe
185.86.76.94:443	1067	C:\WINDOWS\explorer.exe
185.86.76.94:443	1068	C:\WINDOWS\explorer.exe
185.86.76.94:443	1070	C:\WINDOWS\explorer.exe
185.86.76.94:443	1071	C:\WINDOWS\explorer.exe

Rusya 77.246.147.172:443 → spring-knock.ru
Ukrayna 185.86.76.94:443 → yourdatamydata.ru

Botnet ağının parçası olan bir bilgisayar üzerinde hassas veriler sessizce şifrelendikten sonra saldırganın istediği sunuculara upload ediliyor.

Bazen de spam aktivitesi gerçekleştiriyor.

Varsa bilgisayar üzerinde bitcoin vb elektronik cüzdan datalarını almaya çalışıyor.

Web ve email trafiği üzerinde aşağıdaki strinlerle alakalı bir trafik gördüğü anda trafiği inspect ediyor ve saldırgana veri sızdırıyor. USER , PASS , PUT , CONNECT , Authorization , Basic,AUTH,PLAIN,ftp,http,smtp,pop3,pop3_smtp,@

CALL HOME

Dropper file hedef bilgisayar üzerine yerleştikten sonra call home aktivitesi için C&C sunucularıyla haberleşir ve bilgisayar bir bot net ağının kölesi olur. Bu saldırganla hedef bilgisayar arasında doğrudan yapılan ilk iletişimdir ve bu aşamadan sonra bilgisayar artık bizim olmaktan çıkar , veri sızıntıları başlayabilir ve yasal olarak ilgili hedef kişileri zor durumda bırakacak kontrol dışı illegal aktiviteler gerçekleşebilir.

STAGE 7 → DATA THEFT→ Manipülasyon ve veri sızıntıları

Category	Last Attempt	CC	Direction	Incidents
Information Technology: Proxy Avoidance	2015-03-12 15:38:00	Multiple	outbound	20013
Security: Malicious Web Sites	2015-03-12 12:18:00	RU	outbound	128
Extended Protection: Dynamic DNS	2015-03-11 08:04:00	RU	Multiple	71
Multiple	2015-03-12 15:26:00	Multiple	Multiple	49
Security: Phishing and Other Frauds	2015-03-12 15:22:00	IT	outbound	30
Security: Malicious Web Sites	2015-03-12 10:35:00	RU	outbound	30
Security: Malicious Web Sites	2015-03-12 14:55:00	Multiple	outbound	21
Security: Phishing and Other Frauds	2015-03-12 09:07:00	IT	outbound	20
Security: Bot Networks	2015-03-12 14:11:00	UC0	outbound	18
Security: Bot Networks	2015-03-12 11:44:00	LV	outbound	18
Security: Phishing and Other Frauds	2015-03-12 11:09:00	IT	outbound	15

Category	Last Attempt	CC	Direction	Incidents
Security: Bot Networks	2015-03-12 14:11:00	UC0	outbound	18
Security: Bot Networks	2015-03-12 13:34:00	UC0	outbound	2
Security: Bot Networks	2015-03-12 11:44:00	LV	outbound	18
Security: Bot Networks	2015-03-12 09:07:00	UC0	outbound	4
Security: Custom-Encrypted Uploads	2015-03-10 17:16:00	TR	outbound	3
Security: Bot Networks	2015-03-01 22:52:00	Multiple	outbound	1670
Security: Bot Networks	2015-02-25 10:01:00	UC0	outbound	2
Security: Bot Networks	2015-02-24 05:28:00	Multiple	outbound	6

DATA THEFT

Modern siber ataklar için bu aşama oyunun son perdesidir ve her türlü hassas veri saldırganların eline geçer . Siber suçlular için paraya dönüşecek her şey değerlidir ve yeri geldiğinde bu verileri de kullanarak başka saldırılar gerçekleştirmeye devam ederler.

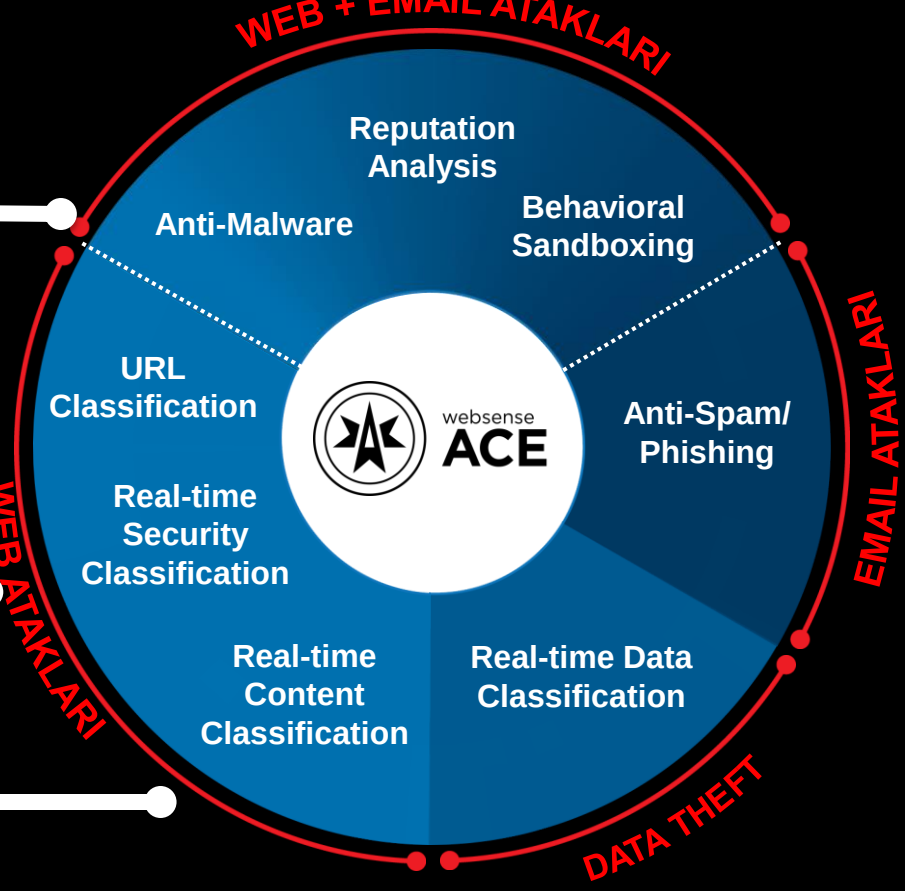
Websense APX ile nasıl korunabilirsiniz ?

APX; APT ve benzeri gelişmiş atakların ilk aşaması olan email içerisindeki linkleri analiz eder gerekirse engeller ve APT yaşam döngüsünün işlemesini engeller.

APX gerekli gördüğü takdirde URL sanboxing sayesinde kullanıcıyı her cihaz üzerinde her yerde korur

APX; ACE ile binlerce farklı algoritma kullanarak sayfaları içeriğine göre kategorize eder ve zararlı dosya alımını engeller.

APX; password , şifreli dosya ve her türlü hassa verinin siber suçluların eline geçmesini engeller.



Bu ataktan Websense ile nasıl korunabilirsiniz ?

- LURE → Atak ilk olarak email ile başladığı için daha ilk seviyede temiz gibi görünen zararlı link barındıran email AP- Email / Hibrid güvenlik teknolojileri ile durdurabiliriz.

- REDIRECT → Lure aşamasının başarılı olması durumunda Email içerisinde gelen linklere ofis içinde ya da ofis dışında tıklanılmasına karşılık AP-Web / Hibrid güvenlik teknolojileri ile durdurabiliriz.

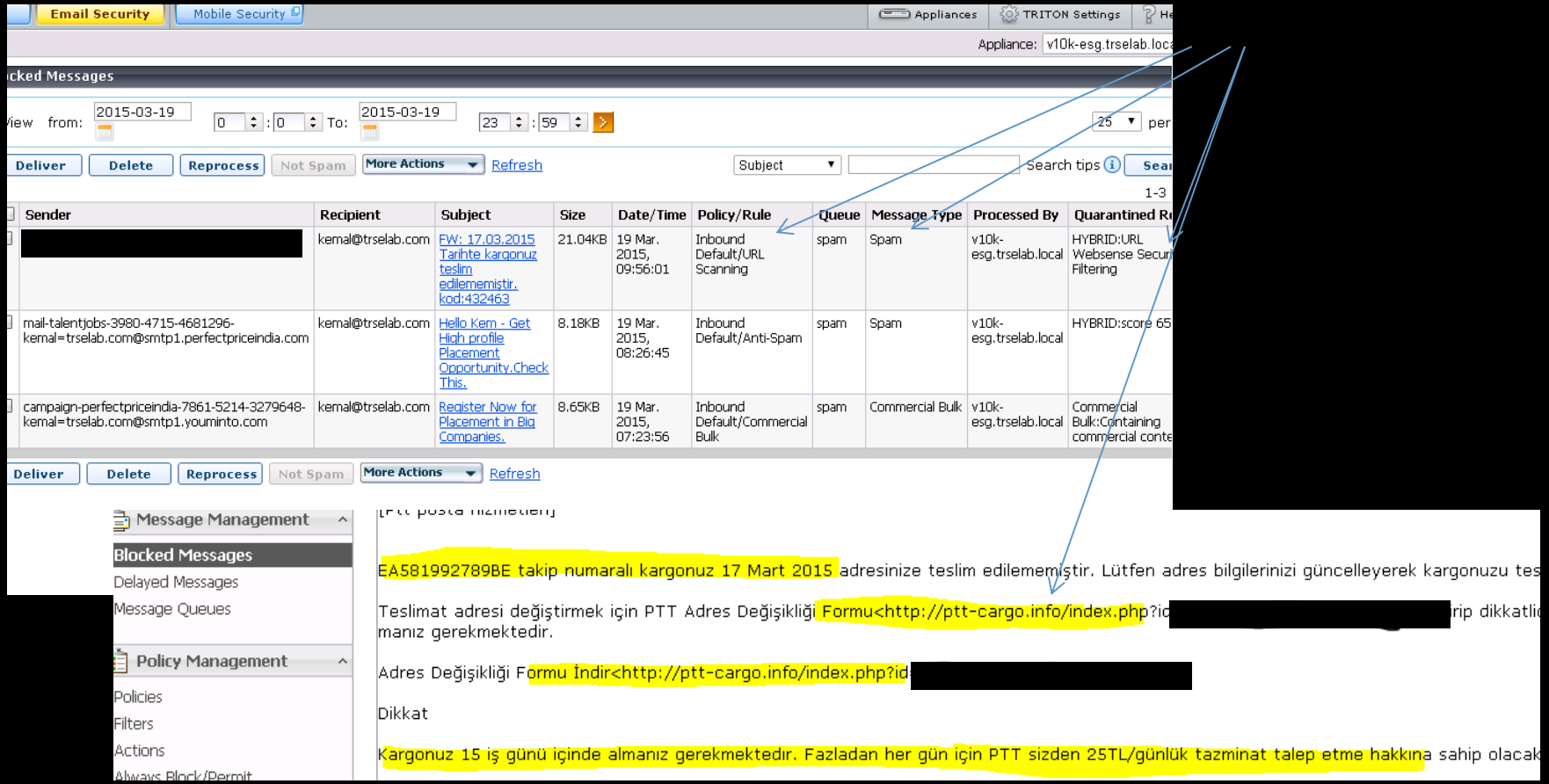
- EXPLOIT → Redirect aşamasının başarılı olması durumunda download edilen zararlı dosyalar ve exploit kitlerini AP-Web / Hibrid güvenlik teknolojileri ile durdurulabilir.

- DROPPER FILE → Exploit aşamasının başarılı olması durumunda Call Home yapabilmek için download edilecek zararlı dosyaları AP-Web / Hibrid / Sandboxing teknololeri ile durdurabiliriz.

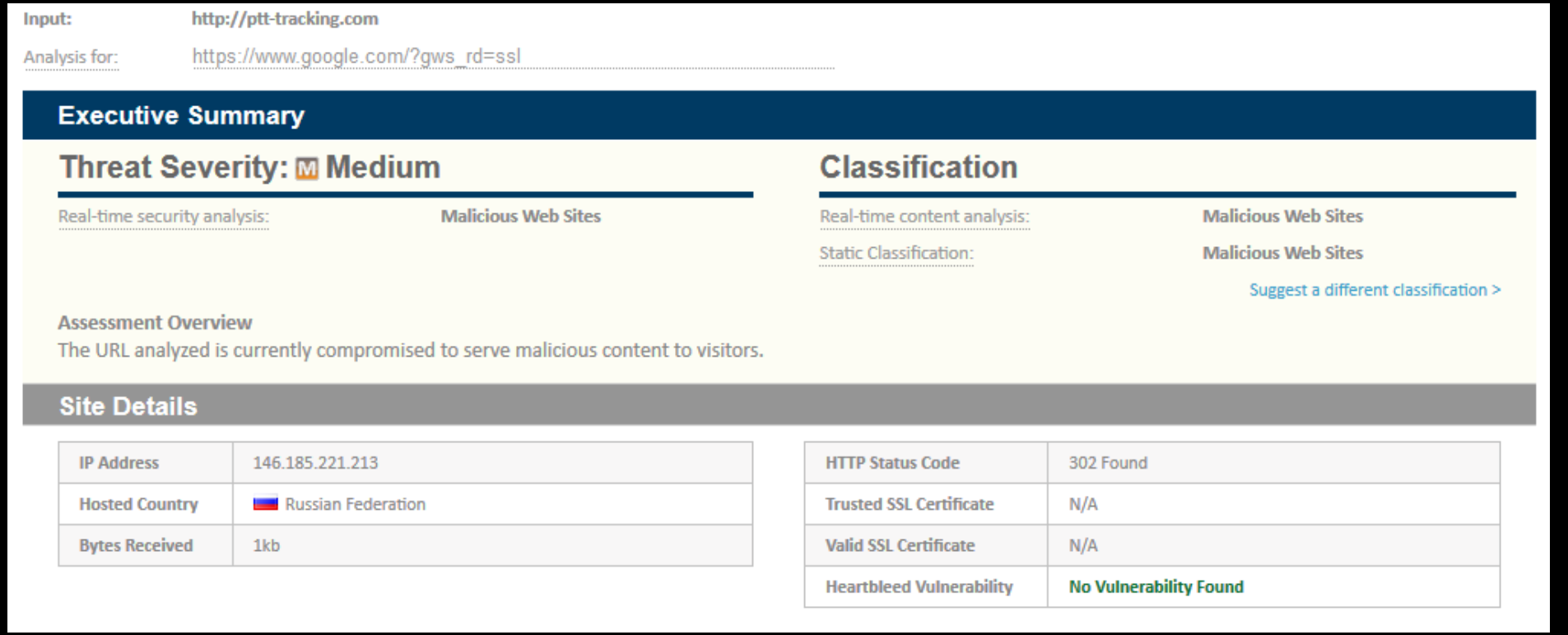
- CALL HOME → Dropper File aşamasının başarılı olması durumunda Call Home , Botnet , C&C aktivitelerini AP-Web / Hibrid teknolojileri ile durdurabiliriz.

- DATA THEFT → Diğer aşamaların başarılı olması durumunda saldırganların almak istediği kritik veri sızıntı aktivitelerini AP-Web / Hibrid / Ap-Data / AP-Endpoint ile durdurabiliriz.

Gönderilen e-mail içerikleri



Mail içerisinde gönderilen linkler



Input: http://ptt-tracking.com

Analysis for: https://www.google.com/?gws_rd=ssl

Executive Summary

Threat Severity: M Medium

Real-time security analysis: **Malicious Web Sites**

Classification

Real-time content analysis: **Malicious Web Sites**

Static Classification: **Malicious Web Sites**

Suggest a different classification >

Assessment Overview

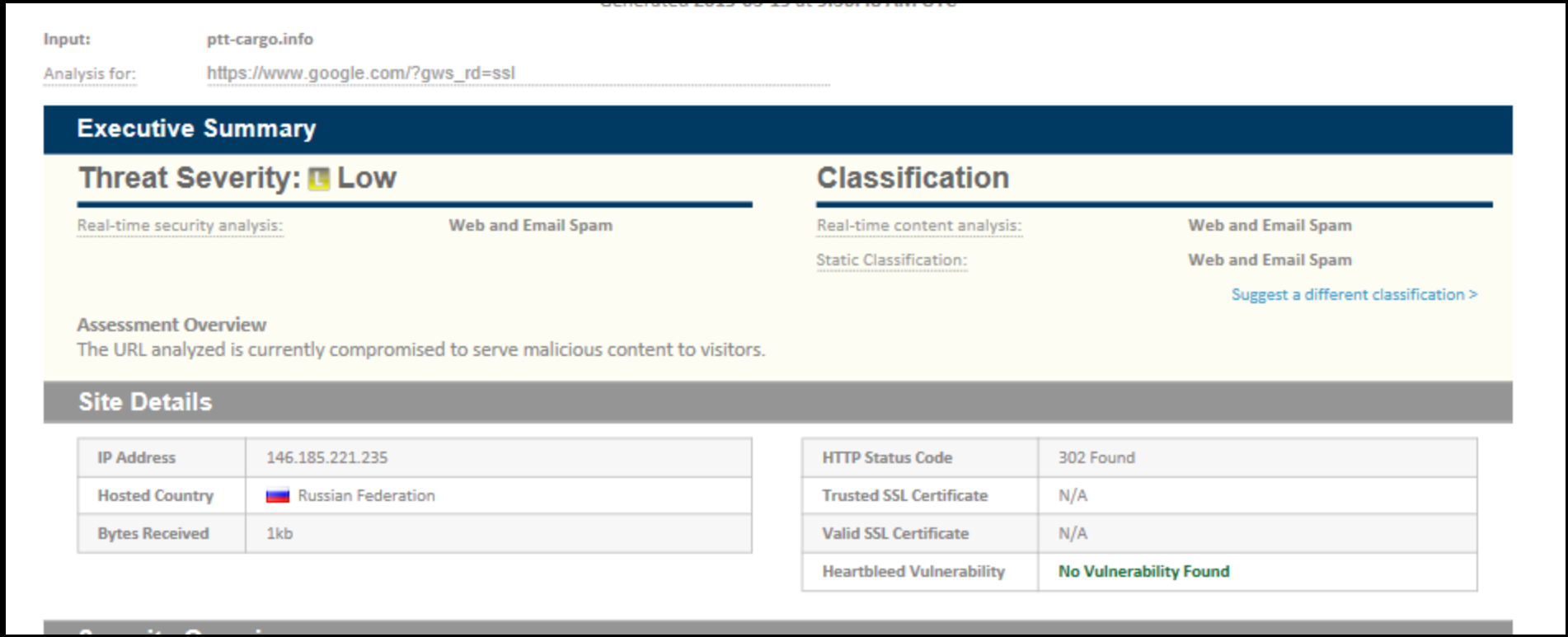
The URL analyzed is currently compromised to serve malicious content to visitors.

Site Details

IP Address	146.185.221.213
Hosted Country	Russian Federation
Bytes Received	1kb

HTTP Status Code	302 Found
Trusted SSL Certificate	N/A
Valid SSL Certificate	N/A
Heartbleed Vulnerability	No Vulnerability Found

Mail içerisinde gönderilen linkler



Input: ptt-cargo.info

Analysis for: https://www.google.com/?gws_rd=ssl

Executive Summary

Threat Severity: Low

Real-time security analysis: Web and Email Spam

Classification

Real-time content analysis: Web and Email Spam

Static Classification: Web and Email Spam

Suggest a different classification >

Assessment Overview

The URL analyzed is currently compromised to serve malicious content to visitors.

Site Details

IP Address	146.185.221.235
Hosted Country	Russian Federation
Bytes Received	1kb

HTTP Status Code	302 Found
Trusted SSL Certificate	N/A
Valid SSL Certificate	N/A
Heartbleed Vulnerability	No Vulnerability Found

Zararlı dosyaların download edileceği adresler

Input: https://copy.com/6cVbNIAY4a6iAvDf/Turkcell_Fatura_789180.zip

Analysis for: https://www.copy.com/error?id=1021&ref=/6cVbNIAY4a6iAvDf/Tur...

Executive Summary

Threat Severity: M Medium

Real-time security analysis: **Malicious Web Sites**

Classification

Real-time content analysis: **Malicious Web Sites**

Static Classification: **Malicious Web Sites**

Suggest a different classification >

Assessment Overview

Real-time analysis of the content downloaded from URL indicates that the website is compromised to serve malicious content to visitors. We recommend that you do not visit this URL in a web browser until the malicious content has been removed.

Site Details

IP Address	64.235.151.46
Hosted Country	United States
Bytes Received	2kb

HTTP Status Code	302 Found
Trusted SSL Certificate	Yes
Valid SSL Certificate	Yes
Heartbleed Vulnerability	No Vulnerability Found

Zararlı dosyaların download edileceği adresler

Input: https://copy.com/z33MEDKGlJnRuqs2/PTT_Adres_Form.zip

Analysis for: https://copy.com/z33MEDKGlJnRuqs2/PTT_Adres_Form.zip

Executive Summary

Threat Severity: Low

Real-time security analysis:	Potentially Unwanted Software
Anti-malware detection:	Potentially Unwanted Software

Classification

Real-time content analysis:	Personal Network Storage and Backup
Static Classification:	Personal Network Storage and Backup

Suggest a different classification >

Assessment Overview

Real-time analysis of the content downloaded from URL indicates that the website is compromised to serve malicious content to visitors. We recommend that you do not visit this URL in a web browser until the malicious content has been removed.

Site Details

IP Address	64.235.151.41
Hosted Country	United States
Bytes Received	448kb

HTTP Status Code	200 OK
Trusted SSL Certificate	Yes
Valid SSL Certificate	Yes
Heartbleed Vulnerability	No Vulnerability Found

Download edilen zararlı dosyaların Websense Sandbox raporu

Turkcell - Fatura
http://csi.websense.com/ThreatScope/FileAnalysis?requestId=80ca1898-0c47-4dfc-bfcf-a45b005a82f4

PTT – Adres değişikliği
http://csi.websense.com/ThreatScope/FileAnalysis?requestId=32eb0805-7411-4049-a181-a45900fce235

PTT - Kargo
http://csi.websense.com/ThreatScope/FileAnalysis?requestId=8f31d284-5c97-4725-9e00-a460002f9a40

Erişilmeye çalışılan Botnet sunucusu

Input: 185.86.76.94:443

Analysis for: 185.86.76.94:443

Executive Summary

Threat Severity: H High

Real-time security analysis: **Bot Networks**

Classification

Real-time content analysis: **Bot Networks**

Static Classification: **Bot Networks**

Suggest a different classification >

Assessment Overview

Real-time analysis of the content downloaded from URL indicates that the website is compromised to serve malicious content to visitors. We recommend that you do not visit this URL in a web browser until the malicious content has been removed.

Site Details

IP Address	185.86.76.94
Hosted Country	Ukraine
Bytes Received	1kb

HTTP Status Code	504 Gateway Timeout
Trusted SSL Certificate	N/A
Valid SSL Certificate	N/A
Heartbleed Vulnerability	No Vulnerability Found

Önerilerimiz

- ***SSL inspection aktif edilmelidir.***
- ***Hibrid email ve hibrid web güvenliği aktif olarak kullanılmalıdır.***
- ***Veri sızıntılarına karşılık DLP politikaları hayata geçirilmelidir.***
- ***Güvenlik istisnasız herkes için uygulanmalıdır ve güvenlik anlamında risk taşıyan kategoriler engellenmelidir.***
- ***Akıllı ve dinamik kategorizasyon yeteneğine sahip çözümler kullanılmalıdır.***
- ***Kurum güvenlik bilinci yukarı çekilmelidir.***
- ***Bize ulaşabilirsiniz.***

TEŞEKKÜRLER