



Cisco 2019

## Siber Güvenlik Raporu ve Tehdit Analizleri

Volkan MUHTAROĞLU

Consulting Systems Engineer, CyberSecurity

28 Mayıs 2019

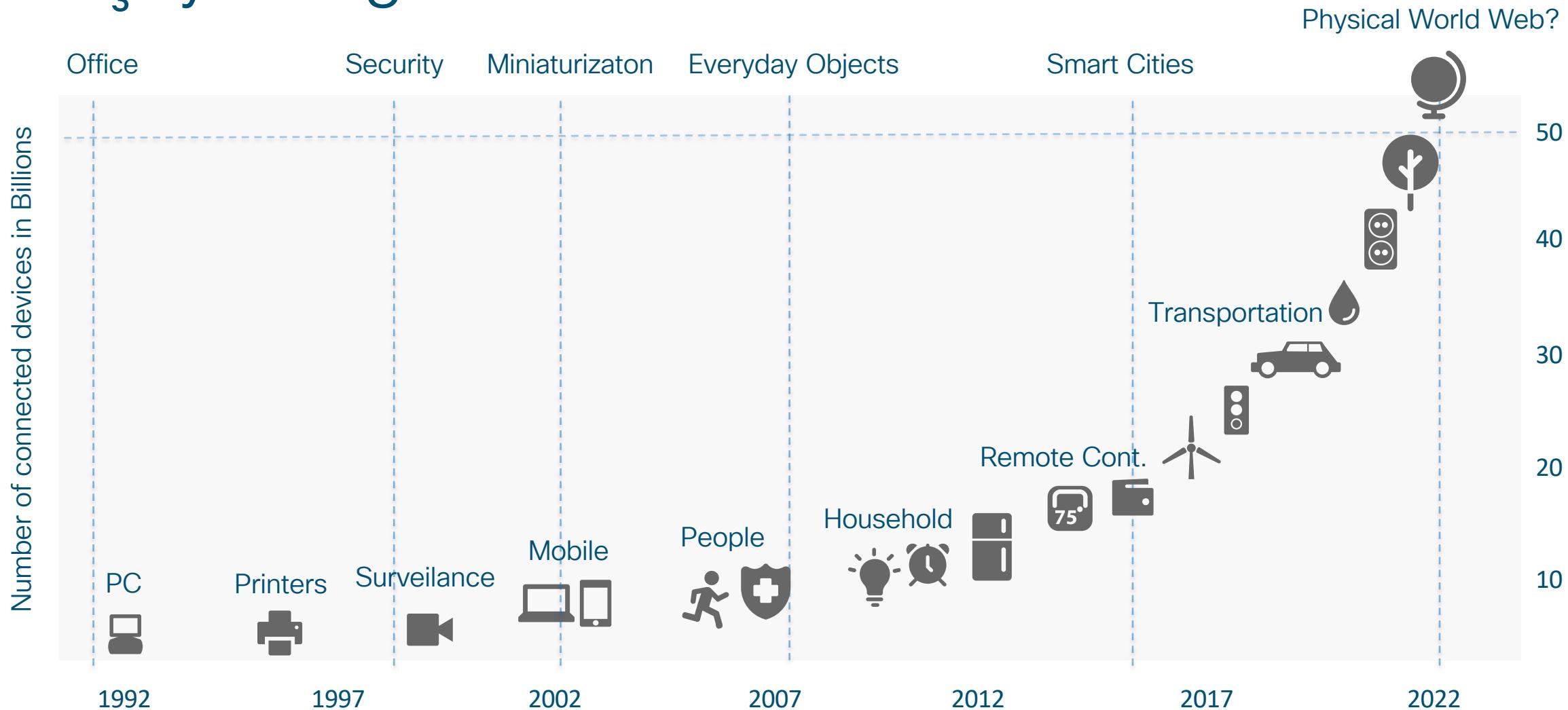


# Hakkımda

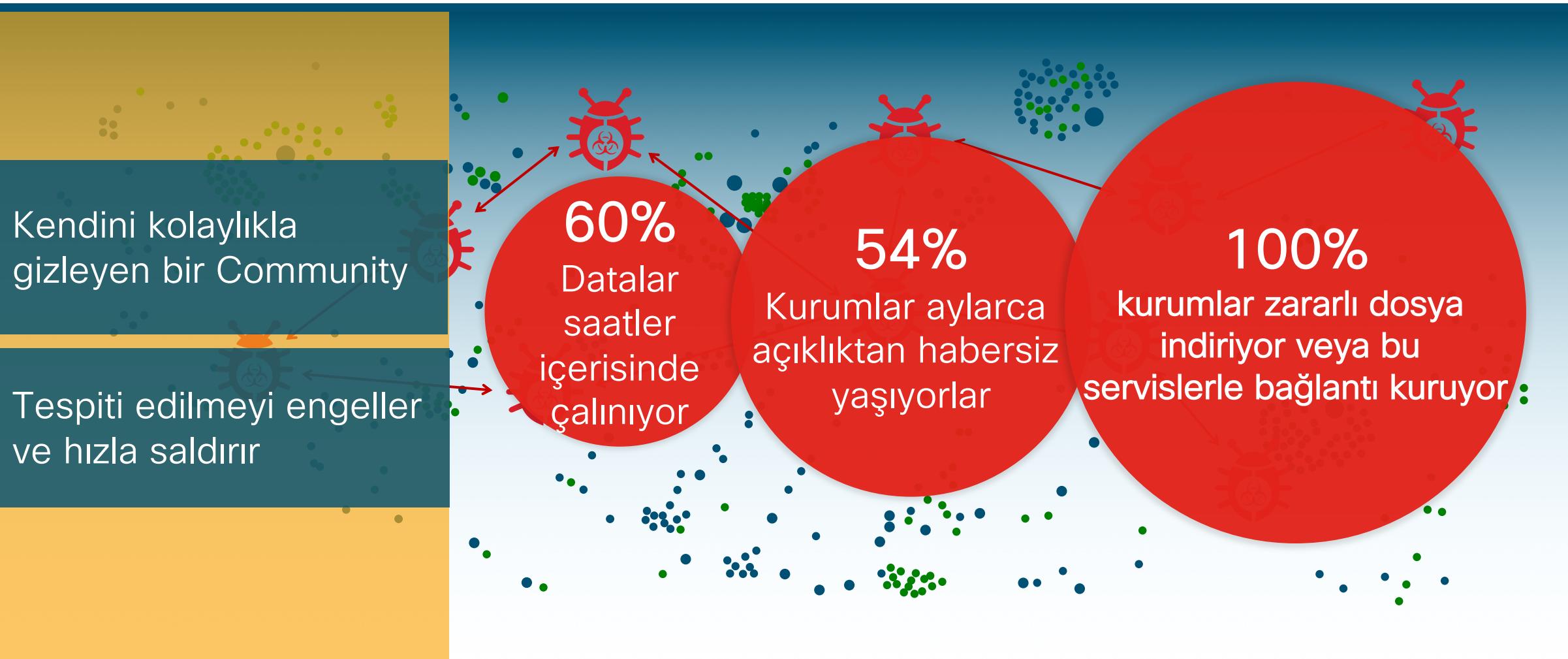
- Consulting Systems Engineer, CyberSecurity
- Güvenlik Sektöründe 13.yıl, 2 farklı üretici deneyimi
- Scuba Diving, Seyahat, Şapka Koleksiyoncusu
- [vmuhtaro@cisco.com](mailto:vmuhtaro@cisco.com)



# Herşeyin Bağlantısı Oldu



# Dinamik Tehdit Haritası



# Cisco 2019 Siber Güvenlik Raporu

- Savunanlar: Kurumları Korumaya Yönerek Yatırım**

- . Otomasyona Güven, Machine Learning, Yapay Zeka (Artifical Intelligence)
- . Kurumları büyük çoğunluğu, kötü aktörlerle karşı davranışsal analitiklerden yararlanıyor

- Saldırırganlar: Olgunlaşan/Büyüyen Ticaret**

- . Kötü amaçlı yazılımların(malware) sahada uygulanması
- . Komuta Kontrol İsteklerinin Gizlenmesi
- . Bulut Kullanımı
- . Network tabanlı ransomware
- . Zaafiyet ve Patch Yönetimi
- . IOT ve DDoS

# Gerçek kaynakların Zararlı(Malicious) Amaçlı Kullanımı



Siber suçlular, gerçek Internet servislerini ve zararlıların oluşturduğu trafiği engellemeyi neredeyse imkansız kılan komuta kontrol kanallarını kullanıyorlar

IP Adresi

A blue cloud-shaped graphic containing the text "IP Adresi".

Altyapı gereksinimi yok

A blue cloud-shaped graphic containing the text "Altyapı gereksinimi yok".

Herkes tarafından güvenilir

A blue cloud-shaped graphic containing the text "Herkes tarafından güvenilir".

Kolay Kurulum

A large blue cloud-shaped graphic containing the text "Kolay Kurulum".

C2 için Şifreli Haberleşme

A blue cloud-shaped graphic containing the text "C2 için Şifreli Haberleşme".

Etki Alanı ve Sertifika tabanlı İstihbarat

A blue cloud-shaped graphic containing the text "Etki Alanı ve Sertifika tabanlı İstihbarat".

Adaptasyon

A blue cloud-shaped graphic containing the text "Adaptasyon".

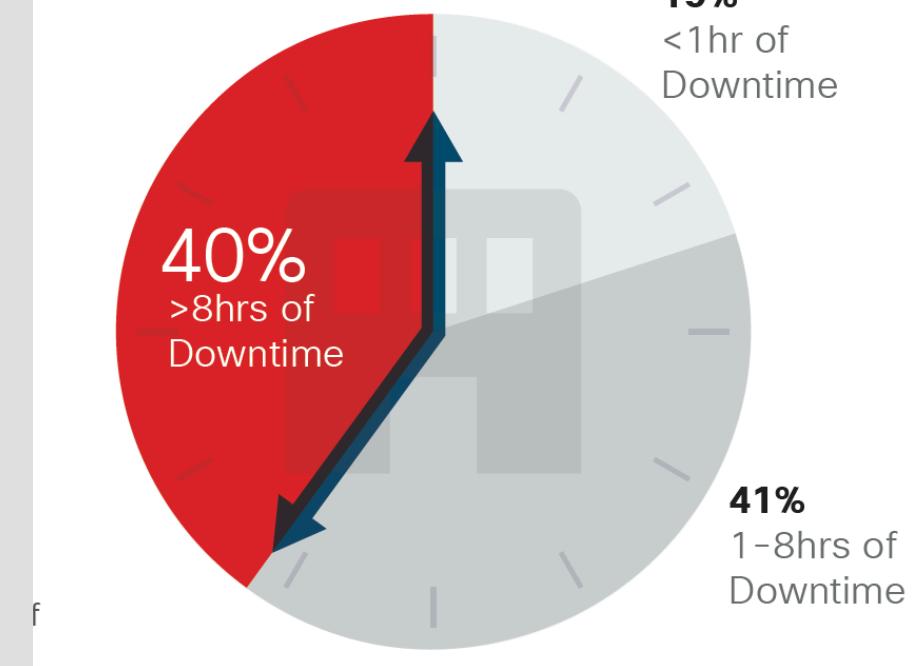
Source: Anomali



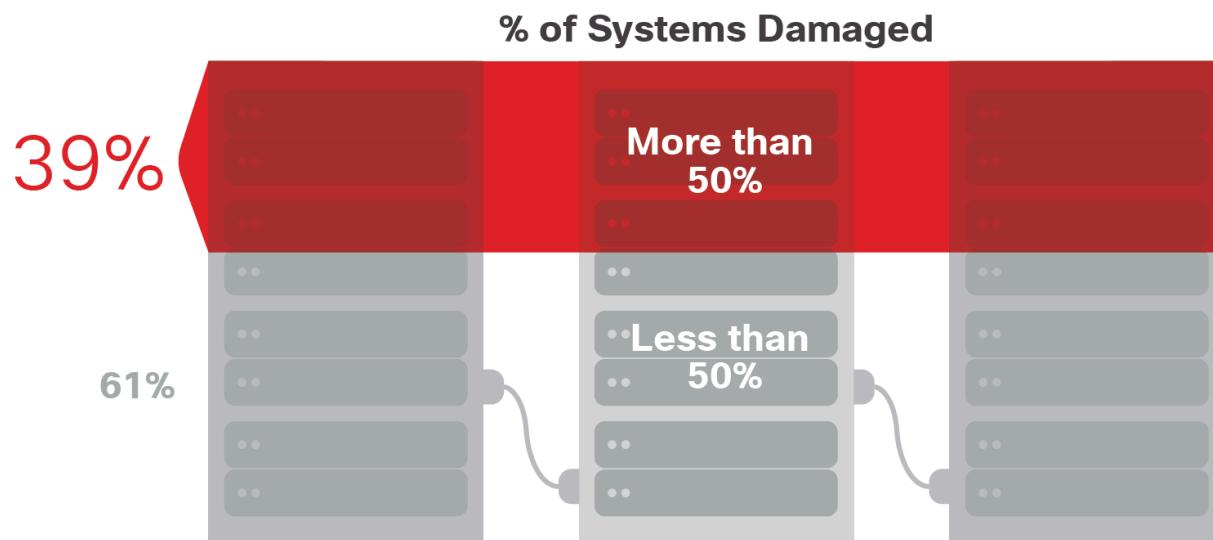


**53% of midmarket companies have experienced a breach**

**Figure 1** System downtime following a severe breach



**Figure 2** Percentage of systems affected by a severe breach



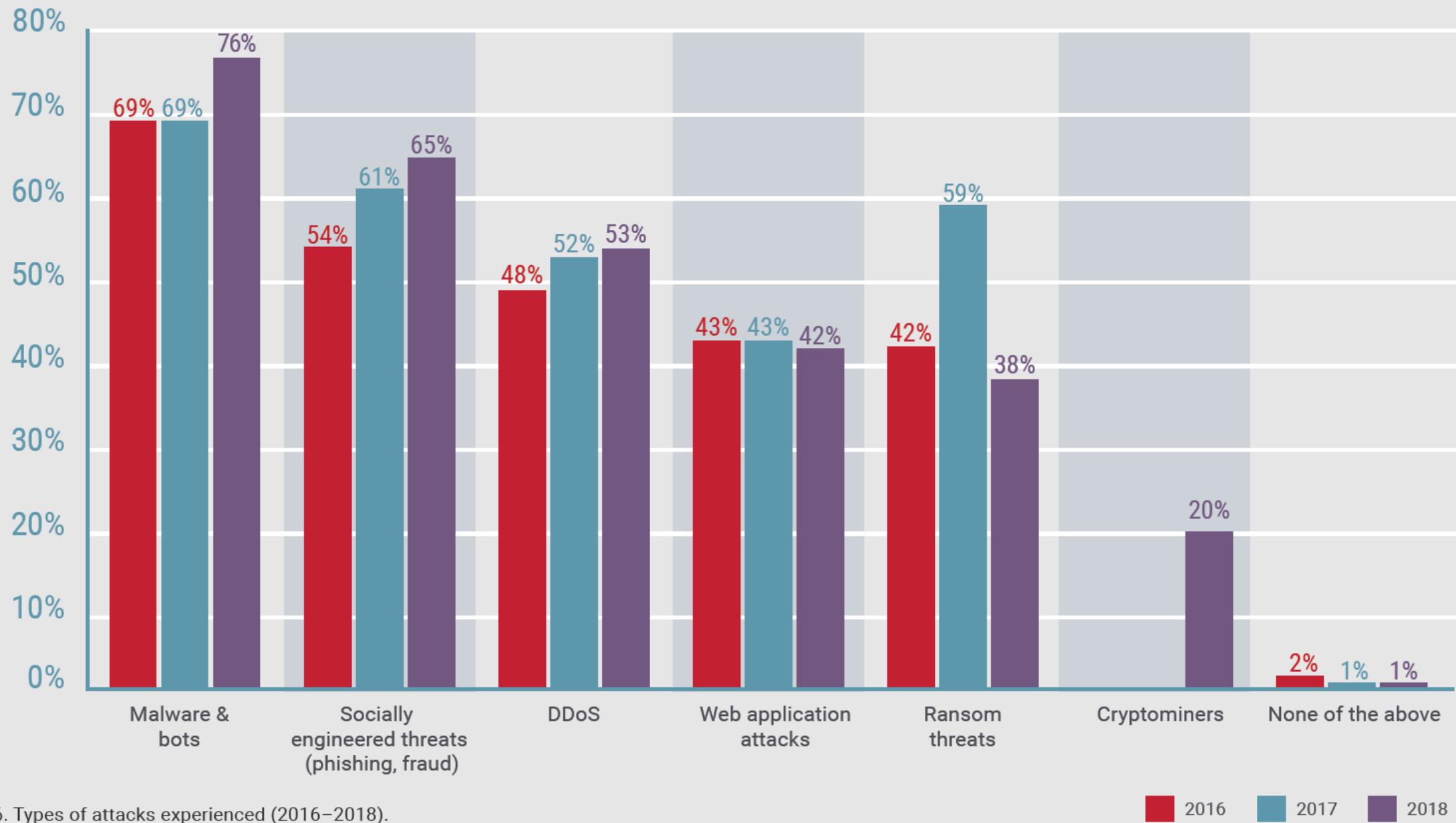


Figure 6. Types of attacks experienced (2016–2018).

## Vectors and Techniques

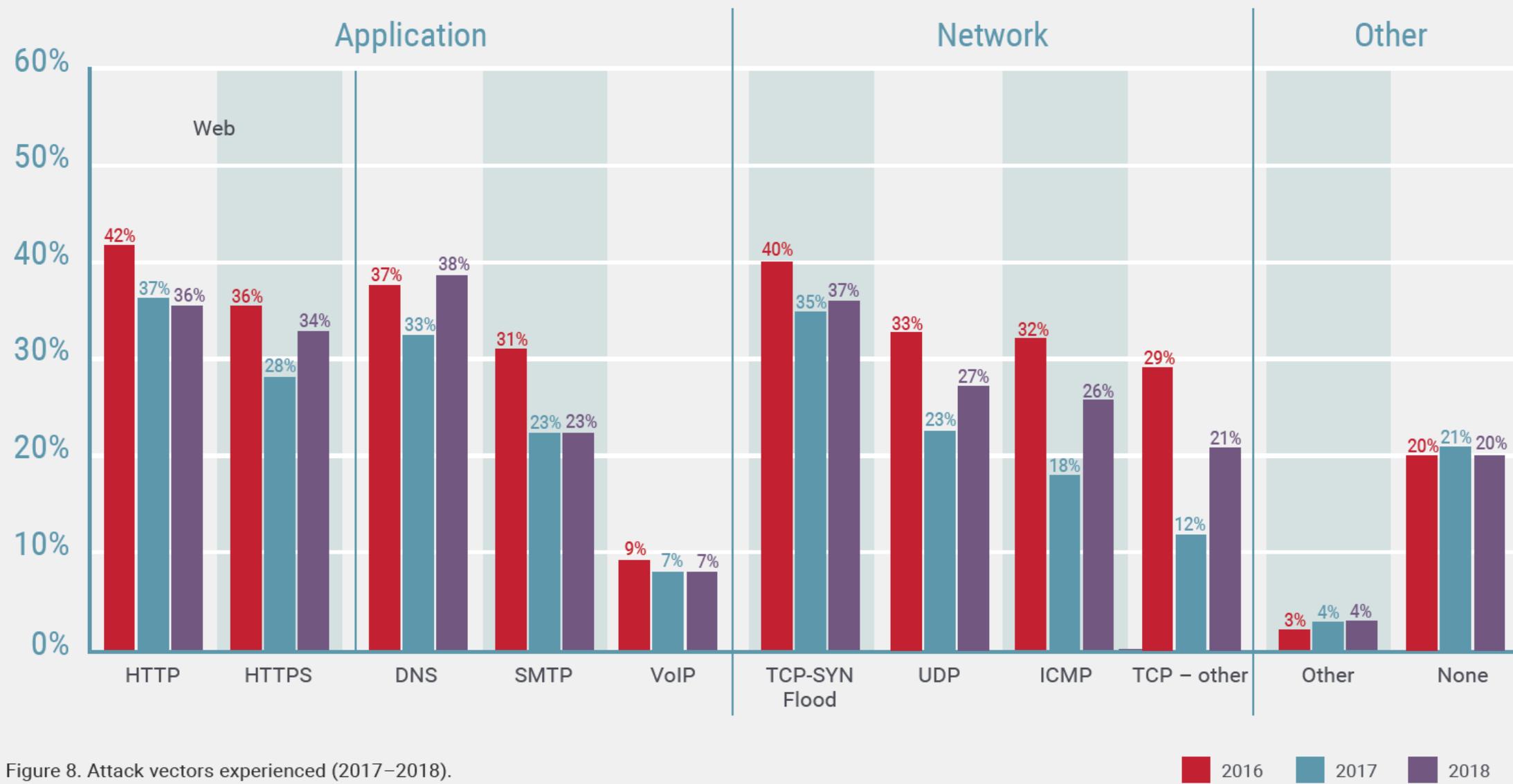


Figure 8. Attack vectors experienced (2017–2018).

# Endüstriyel Sistemlerde(ICS) Zaafiyetler

Tehdit bileşenleri, saldırıları kolaylaştmak için pivot noktaları tespitinde aktif olarak yer almaktadır



Internete Bağlı Olmak



Bilinen Zaafiyetlerin  
Nadiren Patchlenmesi



Bilgi Yetersizliği



Aktörler Uzman

Source: TrapX

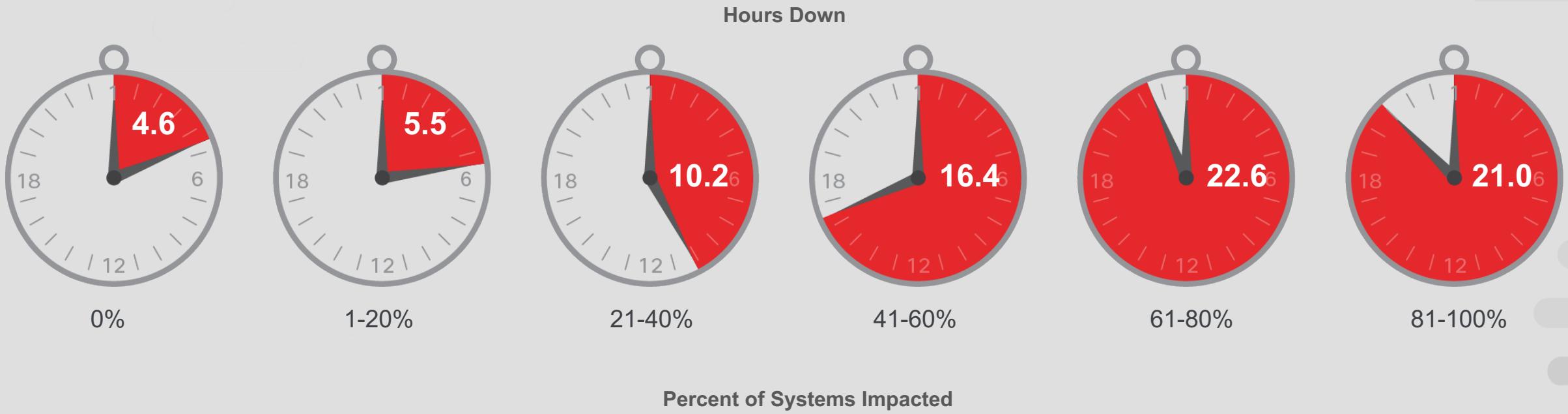
# IT/OT Saldırı Yaklaşımı

69%

Kurumların 2019  
içerisinde OT üzerinden  
saldırı olacağını  
düşünüyor

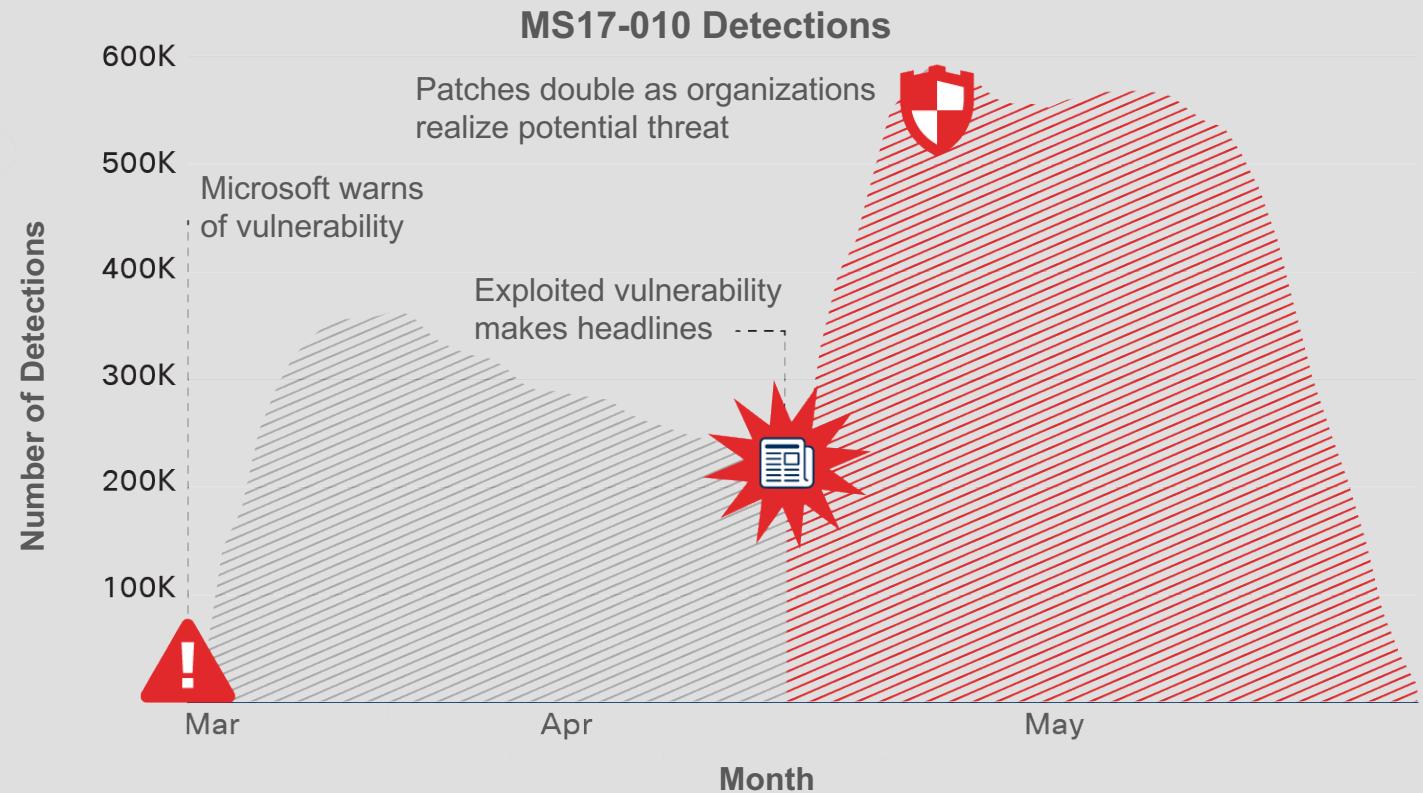


# Kesinti ve Sistem Etkisi



# Yüksek Seviyeli Zaafiyetler ve Patch Yönetimi

Her gün çok sayıda yüksek seviyeli zaafiyetler yayınlanıyor



Patch yönetimi süreçlerini iyileştirmek için daha iyi bir yola ihtiyacımız var

# Whatsapp Güvenlik Açığı



## Latest Vulnerability Reports

### New ZeroDay Reports

TALOS REPORT ID	VENDOR	REPORT DATE
TALOS-2019-0818	AMD ATI	2019-05-08
TALOS-2019-0822	Schneider Electric	2019-05-08
TALOS-2019-0821	Simple DirectMedia Layer	2019-05-08
TALOS-2019-0823	Schneider Electric	2019-05-08
TALOS-2019-0820	Simple DirectMedia Layer	2019-05-08

### New Disclosed Vulnerabilities Reports

TALOS REPORT ID	VENDOR	CVE NUMBER
TALOS-2019-0761	Wacom	CVE-2019-5013
TALOS-2019-0760	Wacom	CVE-2019-5012
TALOS-2019-0792	Antenna House	CVE-2019-5030
TALOS-2019-0778	Adobe	CVE-2019-7761
TALOS-2019-0796	Adobe	CVE-2019-7831

Microsoft 26 Mayıs 2019

24 Saat İçerisinde 4 Yeni Microsoft  
Zero Day Exploit Yayınladı



- \* AngryPolarBearBug2 Windows Bug
- \* Internet Explorer 11 Sandbox Bypass

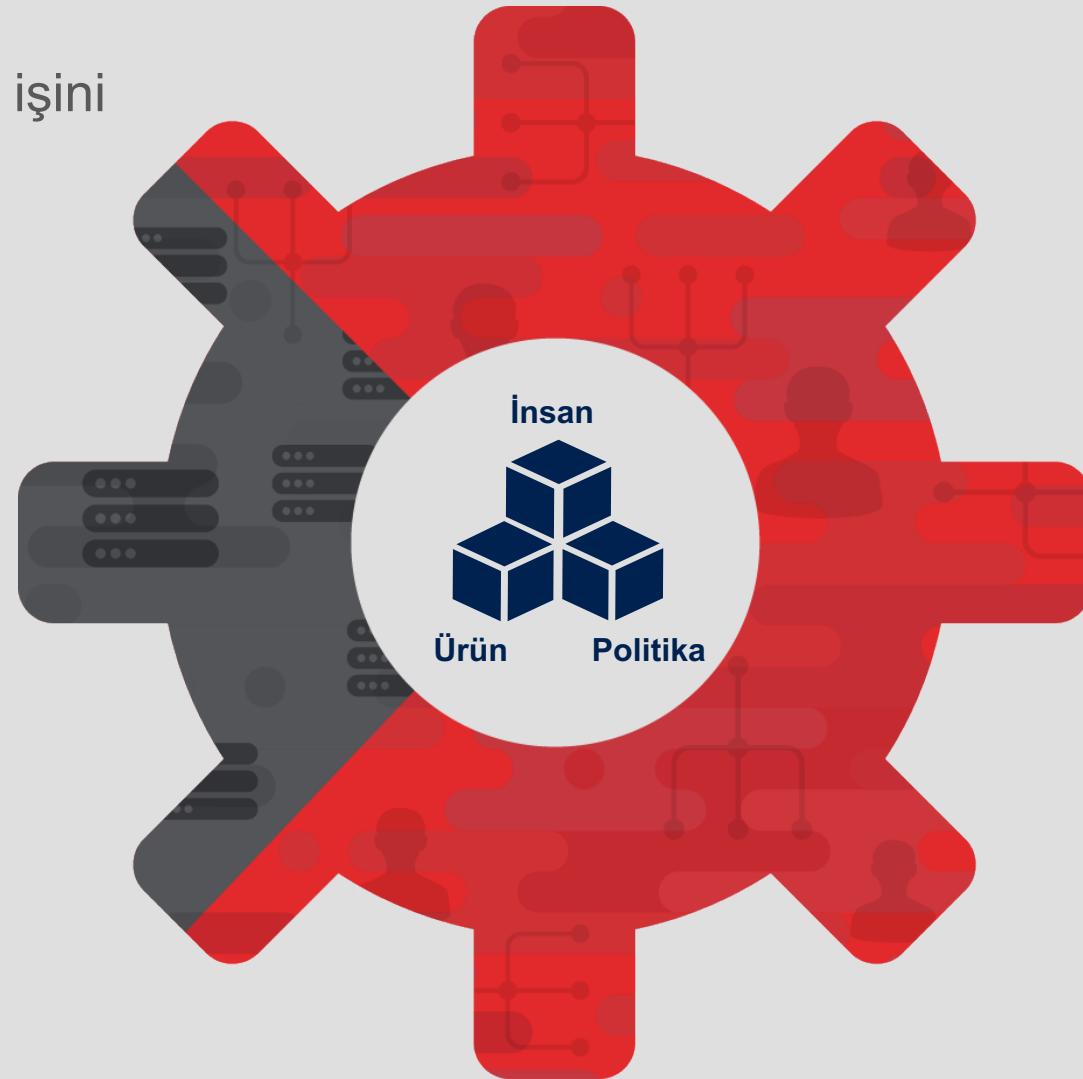
Kaynak : <https://www.cozumpark.com/24-saat-icerisinde-4-yeni-microsoft-zero-day-exploit-yayinlandi/>

<https://www.talosintelligence.com>

# Stratejik, Operasyonel ve Taktiksel Sorunlar

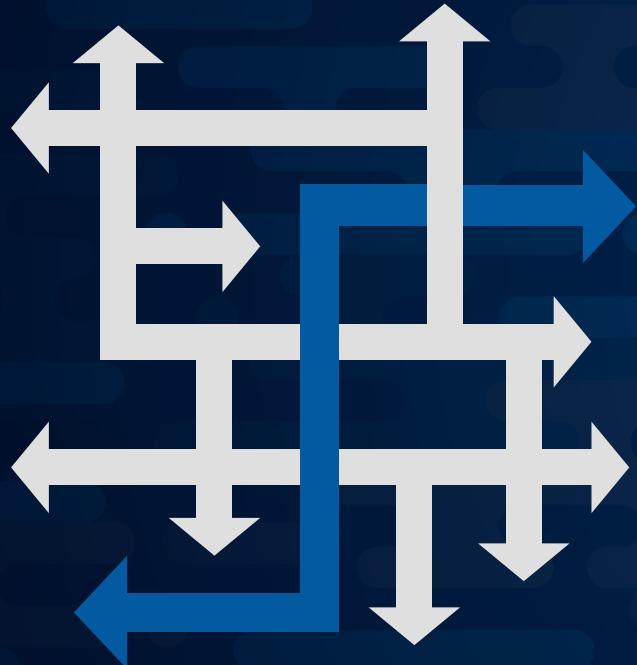
Sorunların ürün kaynaklı  
düşünmek salgırganların işini  
kolaylaştırıyor

**26%**  
Ürün kaynaklı



**74%**  
insan ya da hatalı  
yapılan bir  
işlemden/politika  
kaynaklı

# Market Beklentisi: Tehdit Görünümü

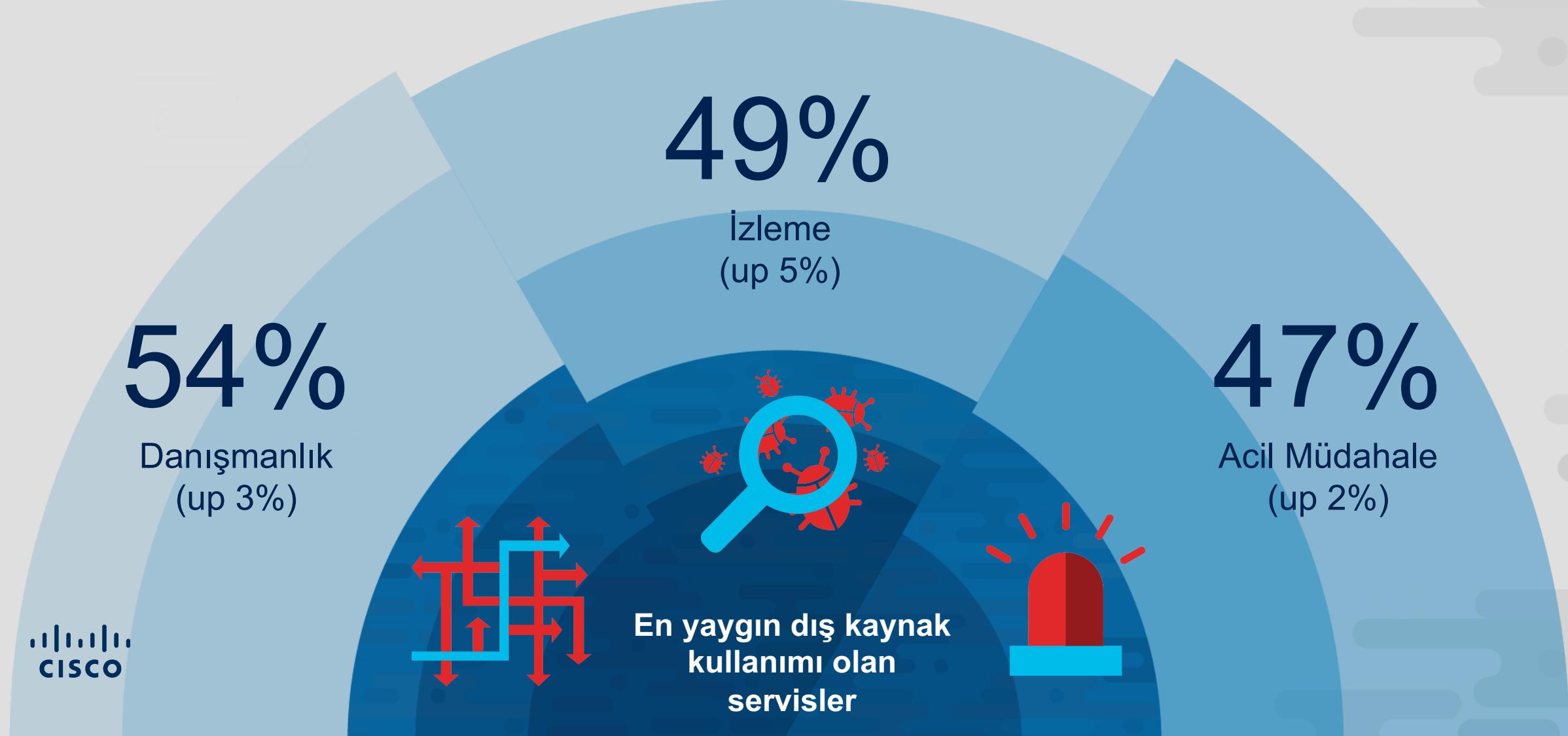


## Tehditler karmaşık ve zorlayıcı olmaya devam edecek

- Çok az kişi, ileride radikal yeni tehditler öngörüyor, daha yetenekli ve daha zorlayıcı kötü aktörler öngörüyorlar
- Kötü aktörleri uzak tutmak için daha gelişmiş güvenlik sistemlerine ihtiyaç duyacaklarına inanıyorlar

# Dış Kaynak Kullanımı İhtiyacı

Güncel kalabilmek için, kurumlar dışında yardım arayışındalar



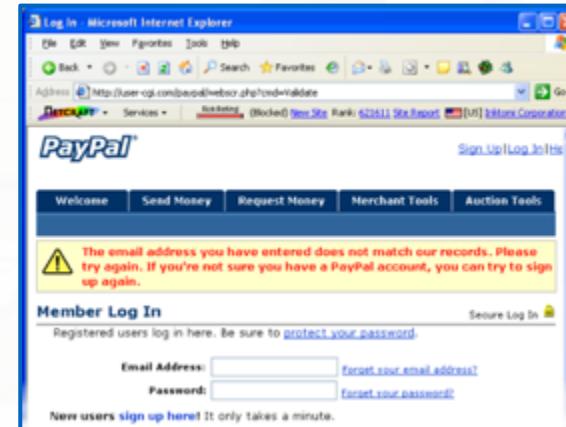
# En yaygın Saldırı ve Tehdit Metotları

## MALWARE



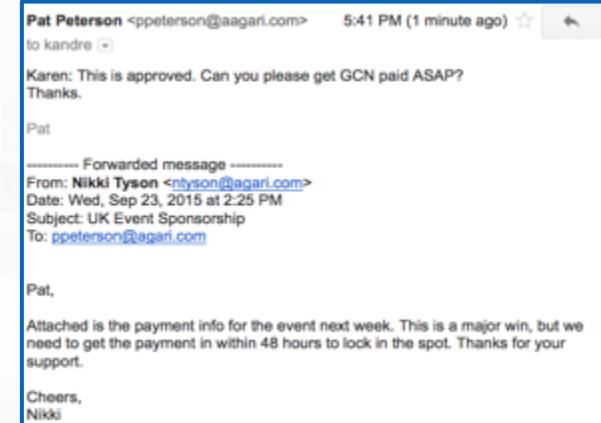
**Content:** Attachment or URL to drive-by website

## PHISHING (OLTALAMA)



**Content:** URL to fake or compromised website

## SOSYAL MÜHENDİSLİK

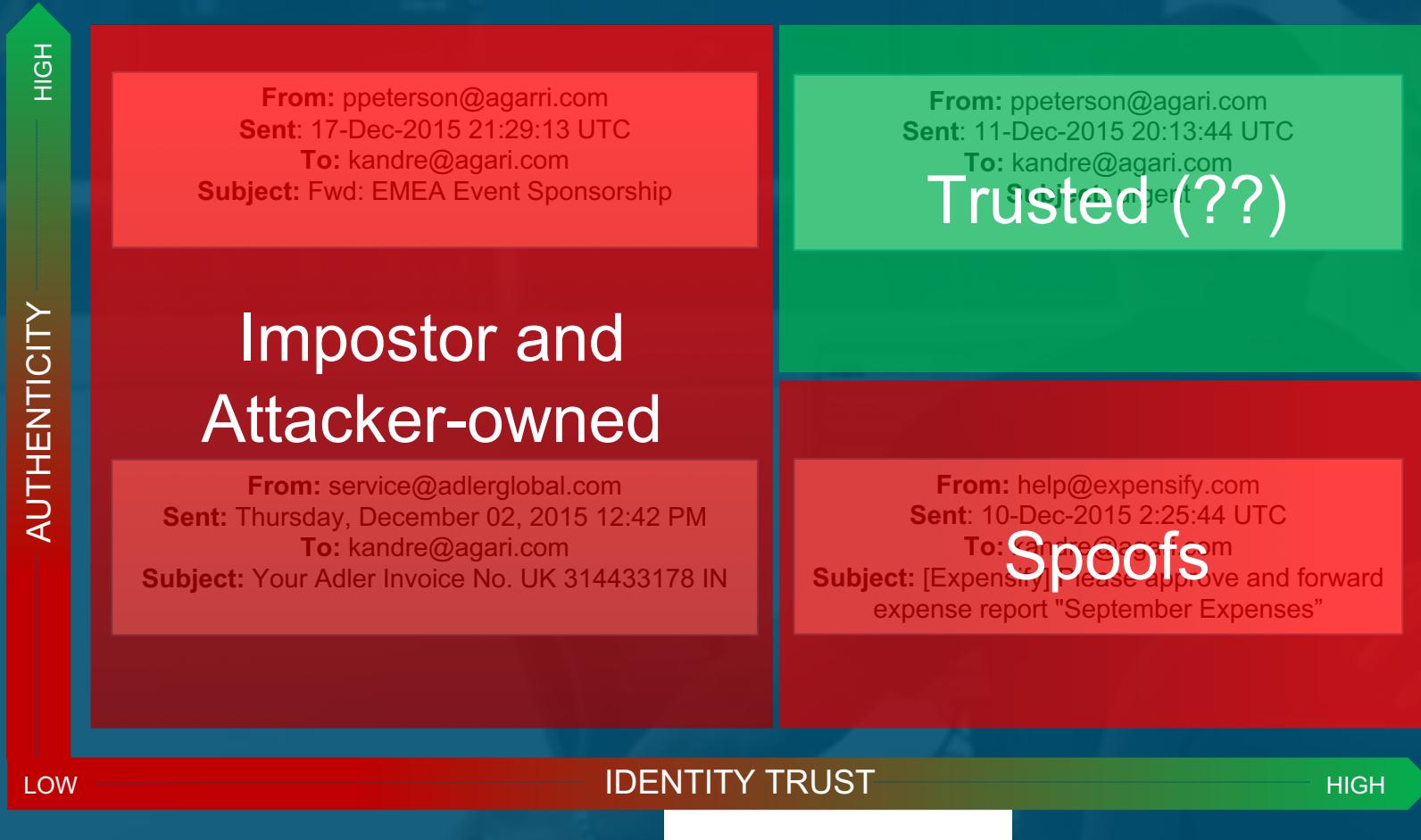


**Content:** Socially engineered text and benign attachments

# Email malware vektörü

- Tehditler içerisinde en popular saldırı vektörü.
- Saldırganlar düzenli olarak yeni phishing kampanyaları başlatıyorlar
- Spam gönderimleri, kullanıcıları şifre öğrenme yazılımını indirmeleri için sürekli kandırmaya çalışır

# Cisco Güven Analizi



# Email içerisinde Zararlı(Malicious) Döküman

Zararlı eklerin yılın ilk kısmından ikincisine kıyasla kullanımı

Office



Archive



PDF



● Ocak-Haziran

● Temmuz-Aralık

# Eki Açıñ...

Oops!

Message

**Revised Tax Statement**

Heather Cole

Sent: Thursday, 7 April 2016 at 12:12

To: Martin Lee (martinle)

📎: Financial\_Statement.doc (15.7 KB) [Preview](#)

Hello,

Attached is the revised tax statement you requested, kindly check and get back to me.

Regards,  
Heather Cole

Attached: Financial\_Statement.xls

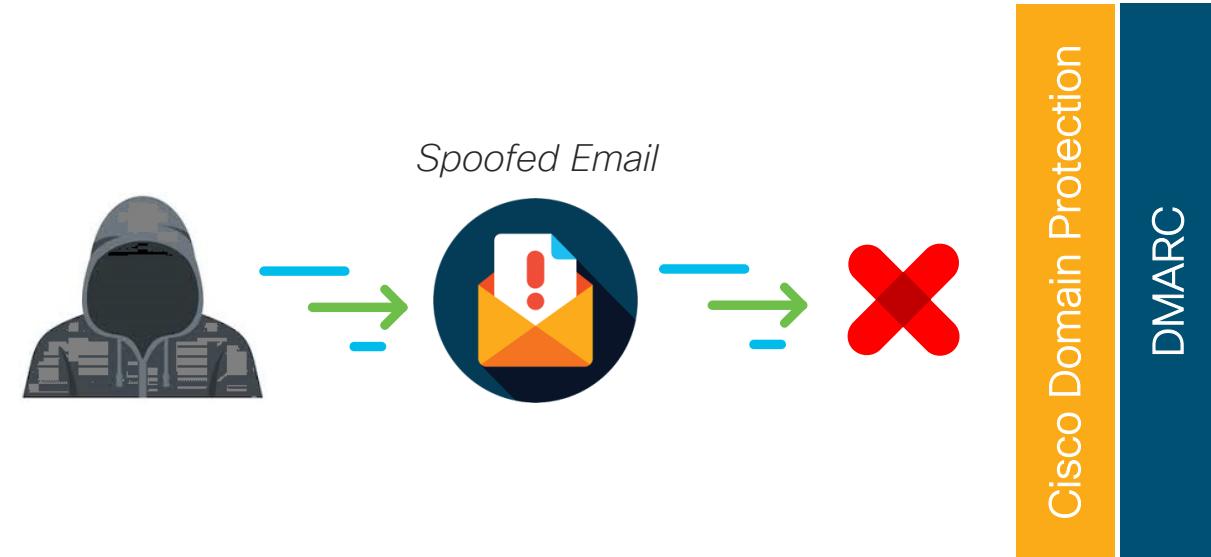
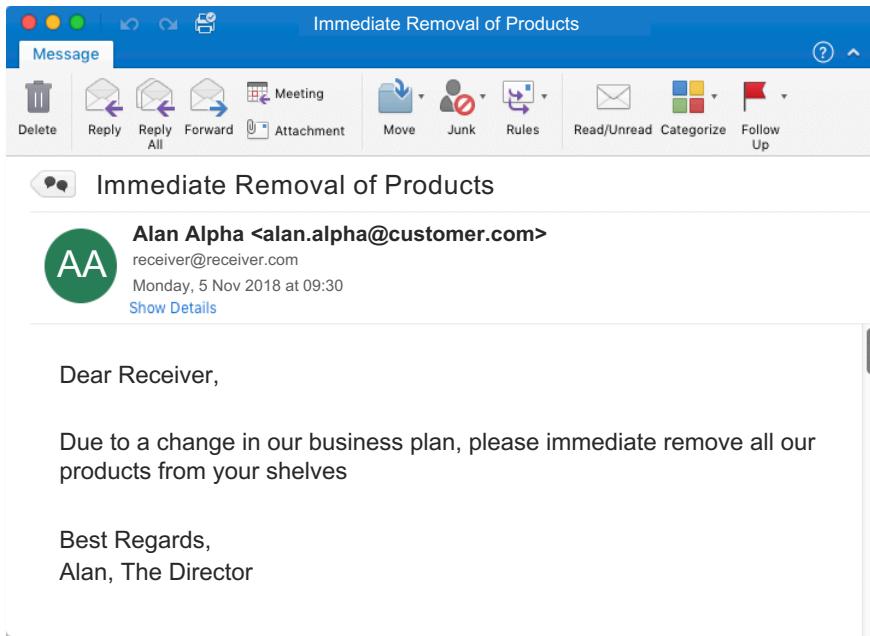
The information contained in this electronic message and any attachments to this message are intended for the exclusive use of the addressee(s) and may contain proprietary, confidential, or privileged information. If you are not the intended recipient, you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately and destroy all copies of this message and any attachments contained in it.

# Müşteri (Gönderen) Email Domain Spoof Edilmesi

SEVERITY: HIGH

EXPLOITATION DIFFICULTY: TRIVIAL

**SALDIRI TEKNİĞİ:** Acemi bilgisayar bilgisine sahip bir saldırgan, herhangi bir müşterinin e-posta kullanıcısının istediği konuya kolayca gelen e-posta gönderebilir. Saldırganın, "Kimden" alanlarına e-posta kullanıcısına ve istediği etki alanına girmesini sağlayan bir araç kullanması yeterlidir.



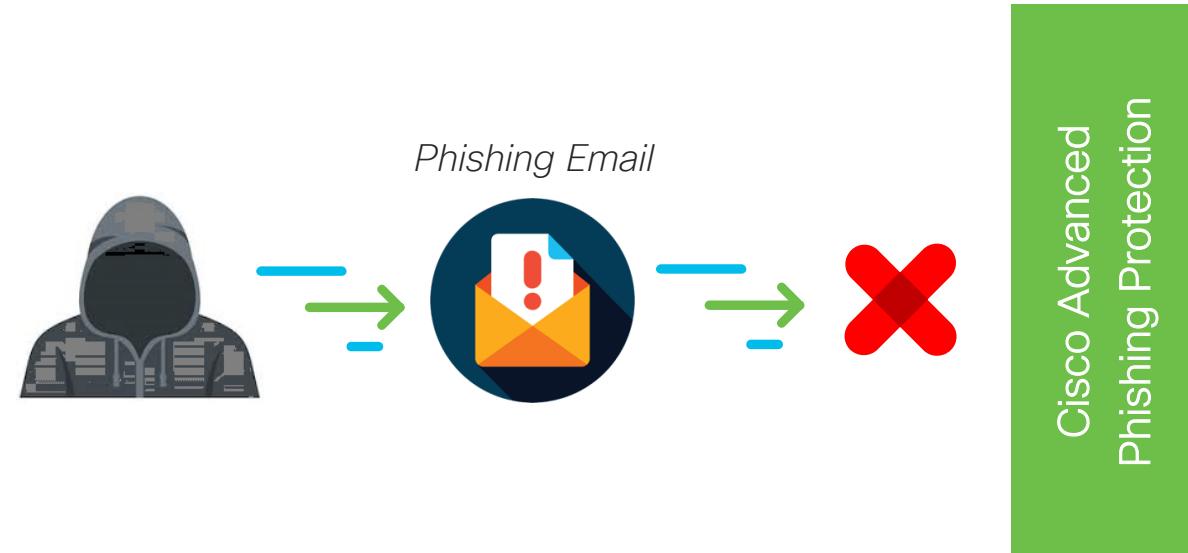
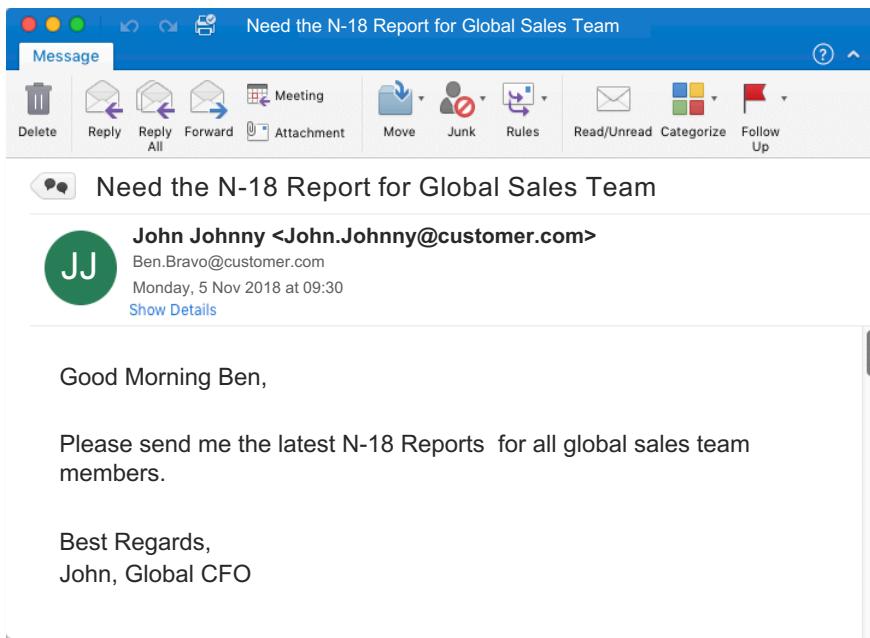
**MITIGATION:** Bring customer (sender) domain to "DMARC Reject" which will only allow actual sender's email from designated sources to be delivered through the Internet

# Müşterinin Kendi Çalışanlarının Spoof Edilmesi

SEVERITY: HIGH

EXPLOITATION DIFFICULTY: TRIVIAL

**SALDIRI TEKNİĞİ:** Acemi bilgisayar bilgisine sahip bir saldırgan, herhangi bir müşterinin çalışanından başka bir çalışana gelen e-postaları kolayca gönderebilir.



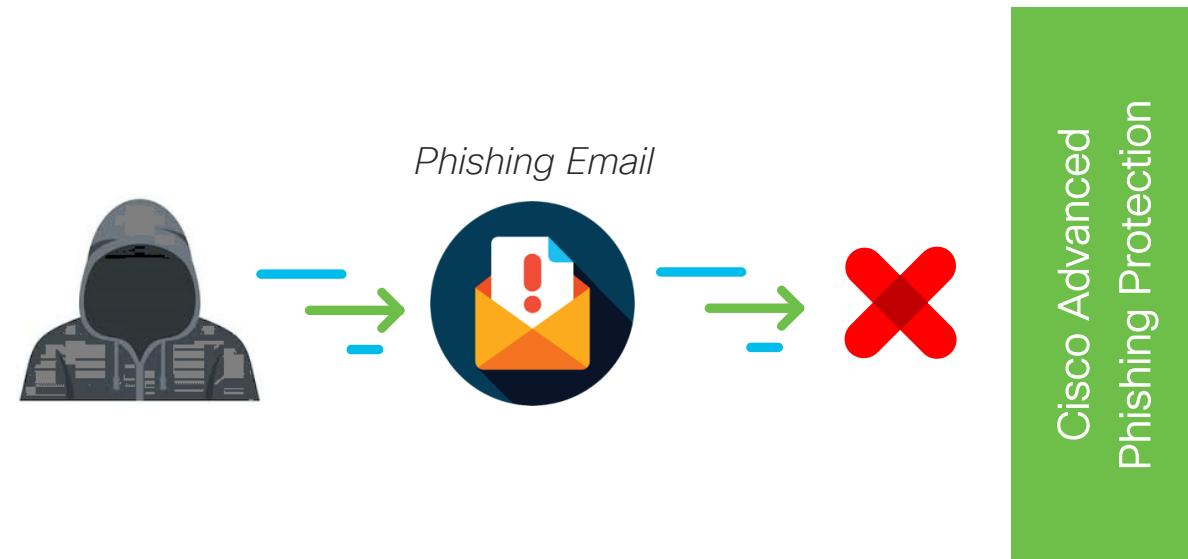
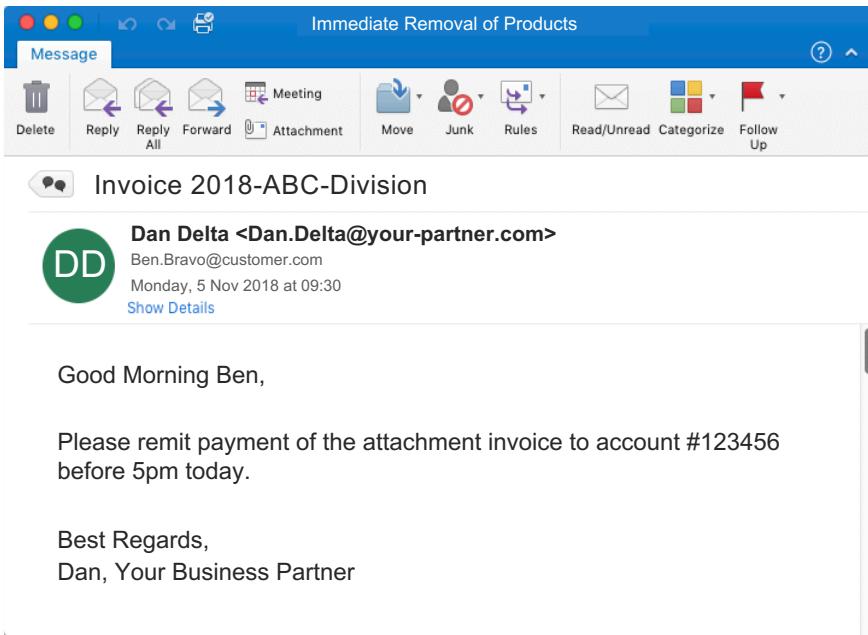
**MITIGATION:** Implement an intelligent email security technology that verifies the identity and trust of every email being delivered to customer's employee.

# Müşterinin İş Ortağının Spoof Edilmesi

SEVERITY: HIGH

EXPLOITATION DIFFICULTY: TRIVIAL

**SALDIRI TEKNİĞİ:** Acemi bilgisayar bilgisine sahip bir saldırgan, herhangi bir müşterinin iş ortağınından herhangi bir müşterinin çalışanına gelen bir e-postayı kolayca gönderebilir.



**MITIGATION:** Implement an intelligent email security technology that verifies the identity and trust of every email being delivered to customer's employee. Encourage business partners to obtain "DMARC Reject".

# Ransomware



## Tanımı

- Çok sayıda Aktör
- Bekle ve Dua Et
- Yıkıcı Sonuçlar

## 🔧 Araçlar

- Emotet ve çeşitli yükleme metotları
- Docs, Exec, PDFs, RTFs



## Taktikler

- Zararlı Gömülü Spam Dosyaları
- Link tabanlı Spam
- Tor ve Bitcoin/Crypto currency



## İşlemler

- Dosyaları Şifreler.
- Şifrelerenmiş dosyaları açmak için verilen zamanda para ödemek
- Yedekten geri dönme

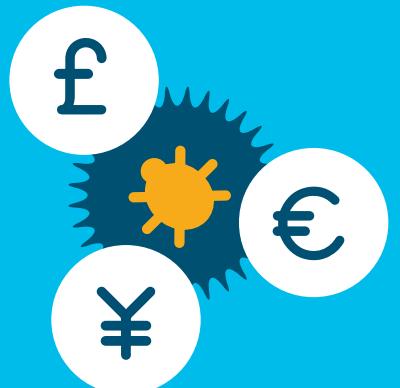
# Olay

## Ransomware: Romantik Seehotel Jaegerwirt



“bilgisayar sistemleri fidye yazılımı tarafından kilitlendi, fidye ödenene kadar yeni anahtar kartları programlanamadı. €1,500 değerinde bitcoin ödemesi yapıldı” Hackerlar bu işlemi 4 kez tekrarladılar. Her seferinde misli olarak para aldılar.

# Emotet



- Emotet birkaç yıl önce çıkmış ve her geçen gün hızla büyümekte.
- Hayatına Banka trojeni olarak başladı.
- Malware'lerin network içerisinde dağıtımında önemli bir bileşen
- Spam emailler üzerinden gönderiliyor.
- Yalnızca verilerinizi sızdırmaktan değil, sistemlerdeki portları yönlendirerek dinlemeye alabiliyor
- US-CERT'in tahminine göre bazı kurumlarda Emotet silinmesinin maliyeti \$1M bulmaktadır



# VPNFilter



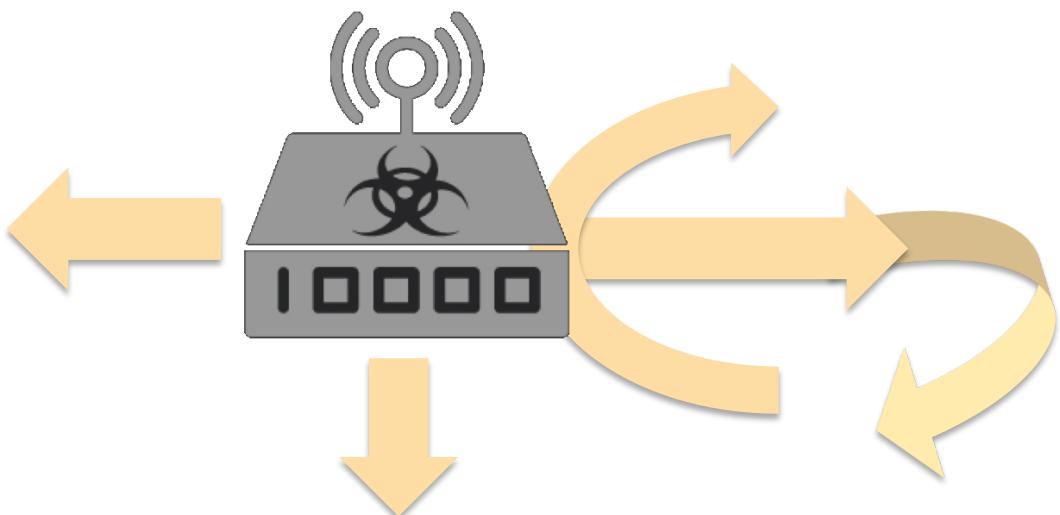
© 2019 Cisco and/or its affiliates. All rights reserved.

- İlk kez Talos tarafından tanımlanmıştır
- IoT tehditinin router ve network üzerinden kullanılan depolama cihazlarını hedef alıyor
- Muhtemelen tehlikeye girmiş cihazlarda güvenlik açıkları kullanarak yayılıyor.
- Veri Sızıntısı oluşturmak temel özelliği.

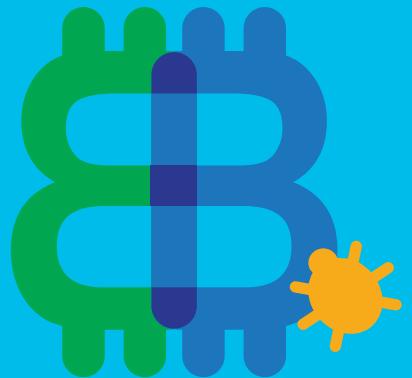


# VPNFilter Yetenekleri

- Internal networku tarar
- Modbus trafiğine bakar.
- https den http ye indirir  
Kimlik Doğrulama Bilgilerini çalar
- Trafiği yönlendirir
- TOR network oluşturur



# Malicious Cryptomining



- Sistemin performansına ve güç tüketimine negative etkisi vardır.
- Network performansını etkiler.
- Muhtemel regulasyon sorunları doğurur.
- Malicious cryptomining üzerinden network içerisindeki diğer güvenlik açık noktaları bulunur.



# Crypto Mining



## Tanımı

- Kripto Para yaratırken sizin CPU'nuzu kullanır
- Geniş ve Yaygın
- Kısıtlı Ransomware gibi hareket

## 🔧 Araçlar

- Marcos, Docs, PDFs, ve EXEs
- IoT cihazları
- Mimikatz ile Oturum Bilgiler Çalınır



## Taktikler

- Default passwords
- Spam, Link Spam, ya da Phishing



## İşlemler

- CPU kullanımını çalar
- Yavaşlık dışında probleme neden olmadığı için kullanıcı farketmez

# Olympic Destroyer

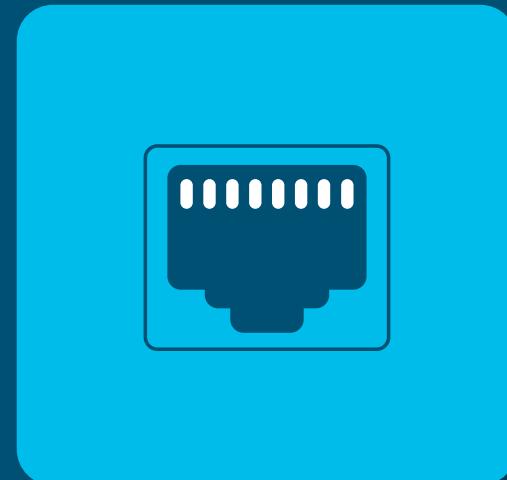


- Olimpiyat Açıılış Seremonilerinde Networkde aksamalara neden oldu (2018 Kış Olimipayatları, 2018 Yüzme Olimpiyatları)
- Talos bu kesintisinin malware kaynaklı olduğunu bildirdi.
- Malware gerçek kaynakları kullanarak hızla yayılım gerçekleştiriyor



# DNS Tünelleme

- DNS tünelleme ile engellenen protokollerin DNS paketleri üzerinden taşınması sağlanır.
- DNS tünelleme, IP protokolünün DNS paketleri içerisinde kodlanmasıyla çalışır.
- DNS haricinde hiçbir protokole izin verilmeyen bir bilgisayardan bu tünelleme ile internette erişim sağlanabilir
- Özellikle Havaalanları ve oteller kablosuz bağlantılar için DNS tünellemesini sıklıkla kullandığı yerlerdir.



# Yaygın Kullanım Amaçları:

Veri Sızıntısı

Komuta Kontrol  
Haberleşmesi

Misafir Kablosuz Ağının  
kötüye kullanılması

IT politikalarından kaçmak



# Uzun Sorgu İsimleri



To attacker



# Koruma Yöntemleri



**Advanced malware detection and protection technology**  
(such as Cisco Advanced Malware Protection, or AMP) can track unknown files, block known malicious files, and prevent the execution of malware on endpoints and network appliances.



**Email security technology**  
(such as Cisco Email Security) deployed on premises or in the cloud, blocks malicious emails sent by threat actors as part of their campaigns. This reduces the overall amount of spam, removes malicious spam, and scans all components of an email (such as sender, subject, attachments, and embedded URLs) to find messages that contain a threat.



**Web scanning at a Secure Web Gateway (SWG) or Secure Internet Gateway (SIG)**  
(such as Cisco Umbrella) means you can block users from connecting to malicious domains, IPs, and URLs, whether users are on or off the enterprise network. This can prevent people from inadvertently allowing malware to access the network, and can stop malware that makes it through from connecting back out to a command and control (C2) server.

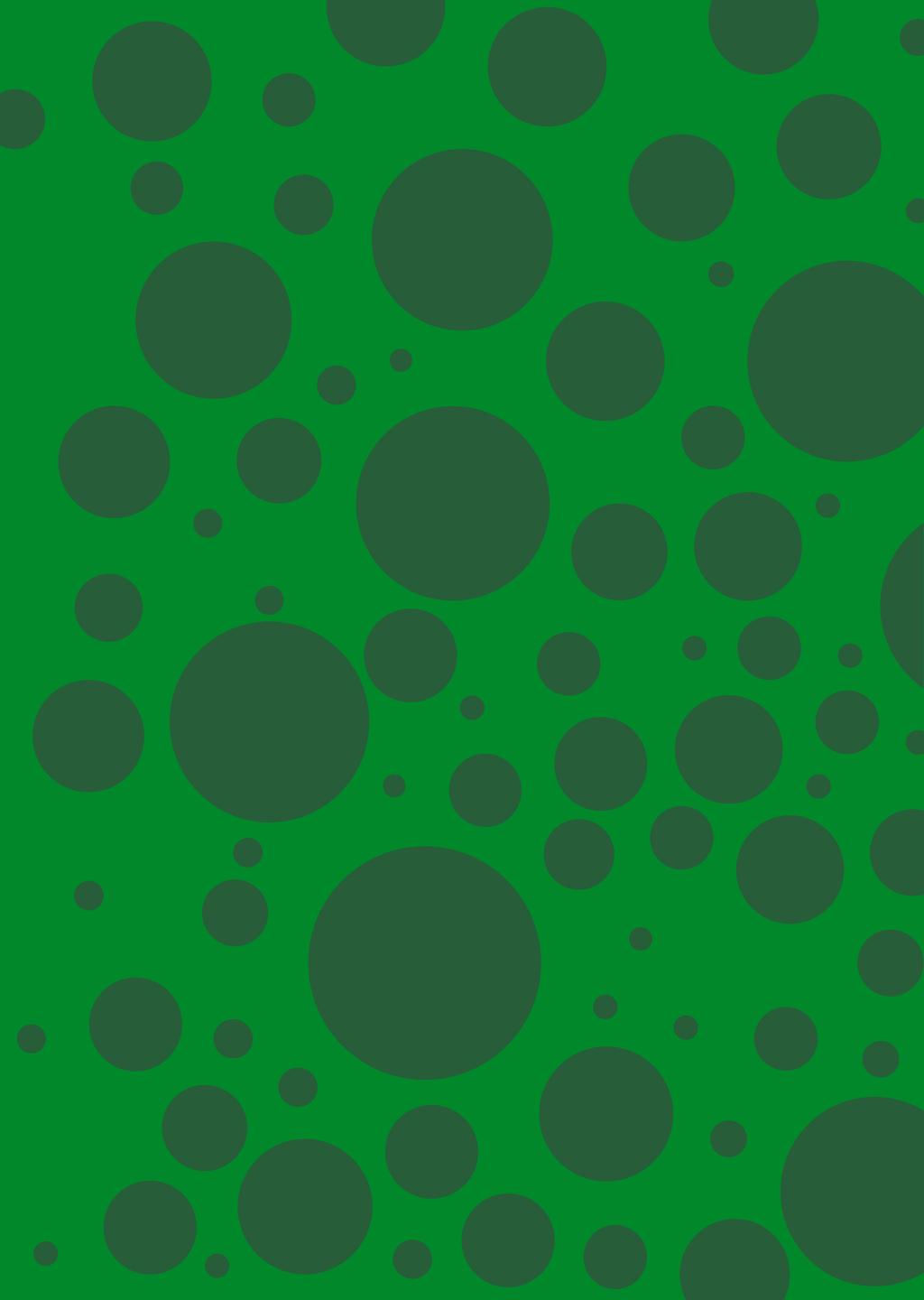


**Network Security**  
(such as the Cisco Next-Generation Firewall (NGFW) and Next-Generation Intrusion Prevention System (NGIPS)) can detect malicious files attempting to enter a network from the Internet or move within a network. Network visibility and security analytics platforms such as Cisco Stealthwatch can detect network anomalies that could signify malware activating its payload.



**Advanced malware detection and protection technology**  
(such as Cisco AMP for Endpoints) can prevent the execution of malware on the endpoint. It can also help isolate, investigate, and remediate infected endpoints for the one percent of attacks that get through even the strongest defenses.

# Demo





# Sorular?



[www.cisco.com](http://www.cisco.com)

