Bilgi Güvenliğine Giriş
Gelişmiş Siber Tehditler (APT)

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabilir ancak değiştirilemez ve ticari amaçla kullanılamaz.
Detaylı bilgiye https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr bağlantısından erişebilirsiniz.

Sunum İçeriği

- Gelişmiş Siber Tehdit (APT) nedir?
- APT savunma ve tespit yöntemleri
- Güncel APT saldırıları
- APT Analiz Teknikleri
- Sonuç

APT nedir?

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

Gelişmiş Siber Tehdit (APT) Nedir?

Gelişmiş Siber Tehdit (APT) nedir ?

Gelişmiş (Advanced)

- Sıfırıncı gün açıklıkları
- Özel hazırlanmış saldırı teknikleri
- Gerektiği kadar karmaşık

Tehdit (Threat)

- Organize çalışma
- Yüksek motivasyon
- İyi finanse edilme

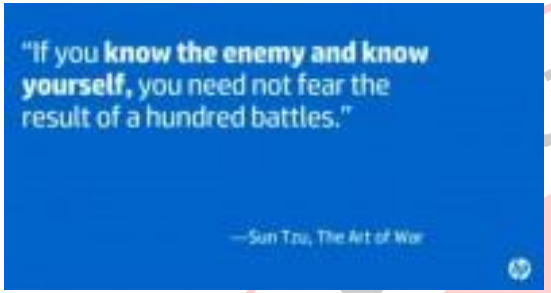
APT

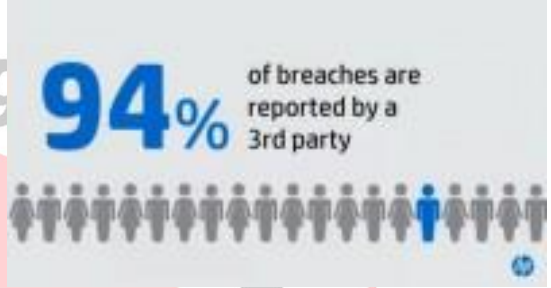
Kalıcı (Persistent)

- Hedefli
- Bütün zayıf noktaları arama
- Uzun süre sistemde kalma
- İz bırakmama

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Eğitim ve Araş
CC BY NC ND

APT Nedir? – Siber Sayılar





94 - 416 - 71 – 84*

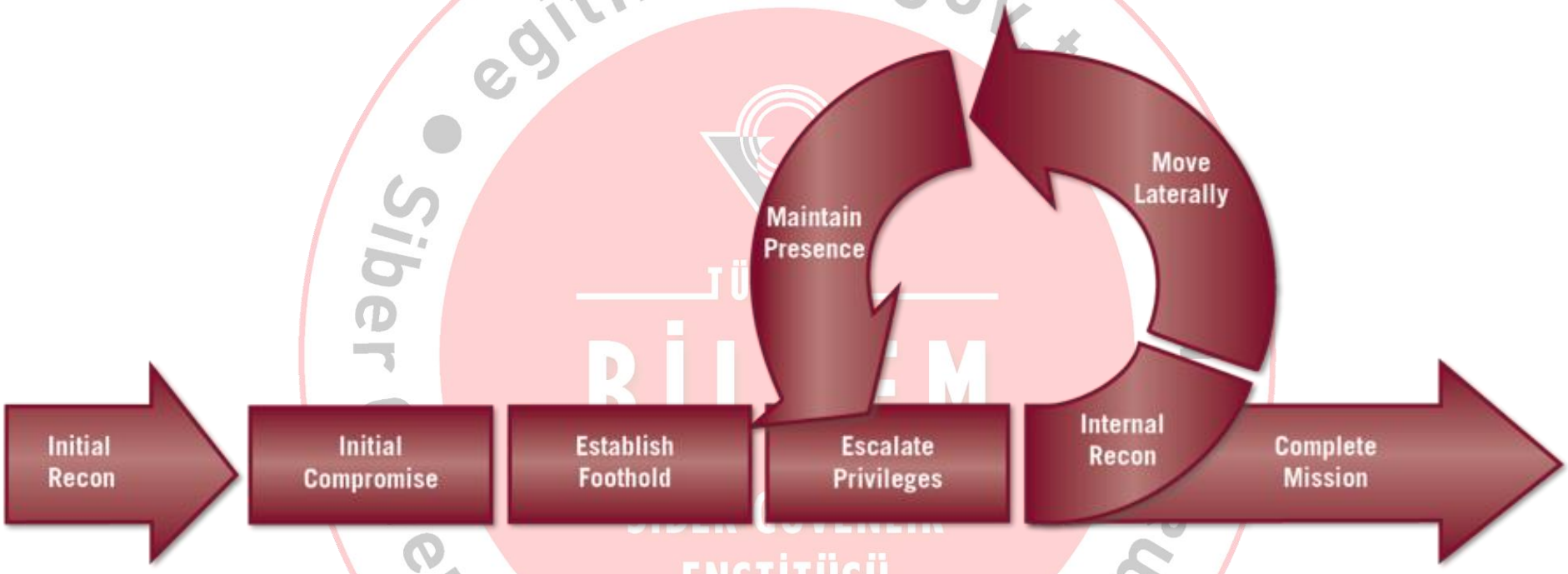
* Art Gilliland, RSA Conference

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Siber Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

APT Nedir? – Saldırı Yaşam Döngüsü

APT Saldırı Yaşam Döngüsü *



*Mandiant, «"APT1Exposing One of China's Cyber Espionage Units"»

egitim.sge.gov.tr • Siber Güvenlik Eğitim ve Araştırma
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Gelişmiş Siber Tehdit (APT) Nedir?

Gelişmiş Siber Tehdit (APT) saldırılarının genel karakteristiği *

Eposta listeleri, sosyal ağ madenciliği, konferanslar, beşeri istihbarat, vs...

Maskeli exe dosyaları, exe-dışı çalıştırılır dosya türü, zararlı DOC/XLS/PPT dosyaları, otomatik bulaşır çıkarılabilir medya

Stratejik web saldırısı, hedefli eposta saldırısı ile gönderilen URL'ler, zararlı eposta ekleri, USB çıkarılabilir medya

0. gün tarayıcı/uygulama açıklıkları, sosyal mühendislik

Özellikli uzaktan erişim araçları (RAT), temel seviye özel araçlar, iyi-yapım hedefli solucanlar

Özel/standart gömülü kodlu HTTP, açık HTTP, şifreli haberleşme, tam SSL kripto, tek kullanımlık C2 düğüm

*FireEye, «World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks Report»
** Lockhead Martin, «Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains»

BY NC ND

APT Nedir? – Neden Kolay?

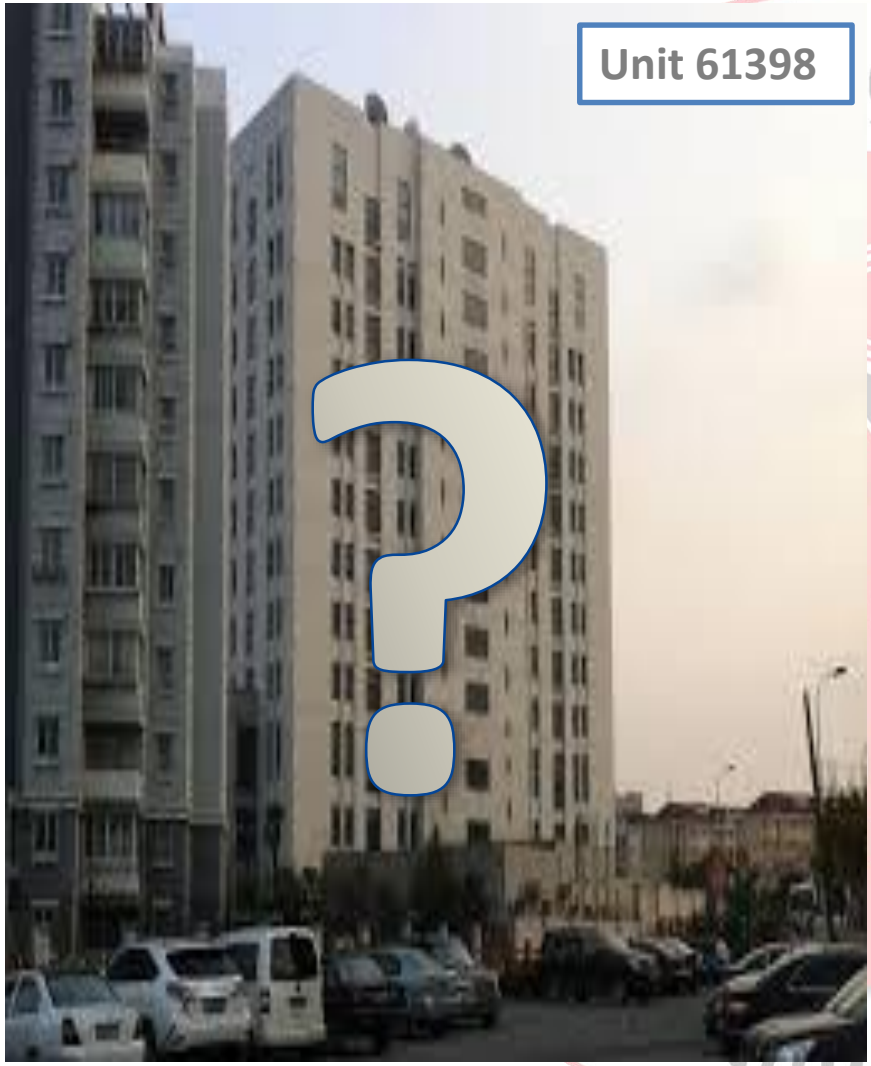
Savunma teknolojilerinin maliyeti *

Ortalama bir siber silah	**$1 M**
Tomahawk (Tactical) füzesi	$1.45 M
Patriot füzesi	$4.54 M
Stuxnet	**$5M - $10 M**
15 MH-60S helikopter	$19.7 M
Siber ordunun yıllık maliyeti *	**$49 M**
F35(A) uçağı	$107 M
DDG-51 Guided Missile Destroyers	$1.100 M

* Charlie Miller, How to build a cyber army to attack the U.S

BY NC ND

Gelişmiş Siber Tehdit (APT) Nedir?



Gelişmiş Siber Tehdit (APT) örneği: APT1*

- 2006 yılından bu yana
  - 20 sektörü kapsayan çalışma
  - 141 kurumda APT tespiti
- Yüzlerce terabyte veri
- Ort. kurumda kalış süresi: 356 gün
- En uzun süre: 1,764 gün
- Bir kurumdan 10 ayda çalınan veri: 6.5 terabyte
- Çin Telekom tarafından özel fiber altyapı ve 1000 civarı sunucu
- Hedefler: Çin'in 12. kalkınma planında yer alan öncelikli 7 sektörden 4'ü

*Mandiant, «"APT1Exposing One of China's Cyber Espionage Units"»

BY NC ND

APT Savunma ve Tespit Yöntemleri

TÜBİTAK
egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma Merkezi
SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

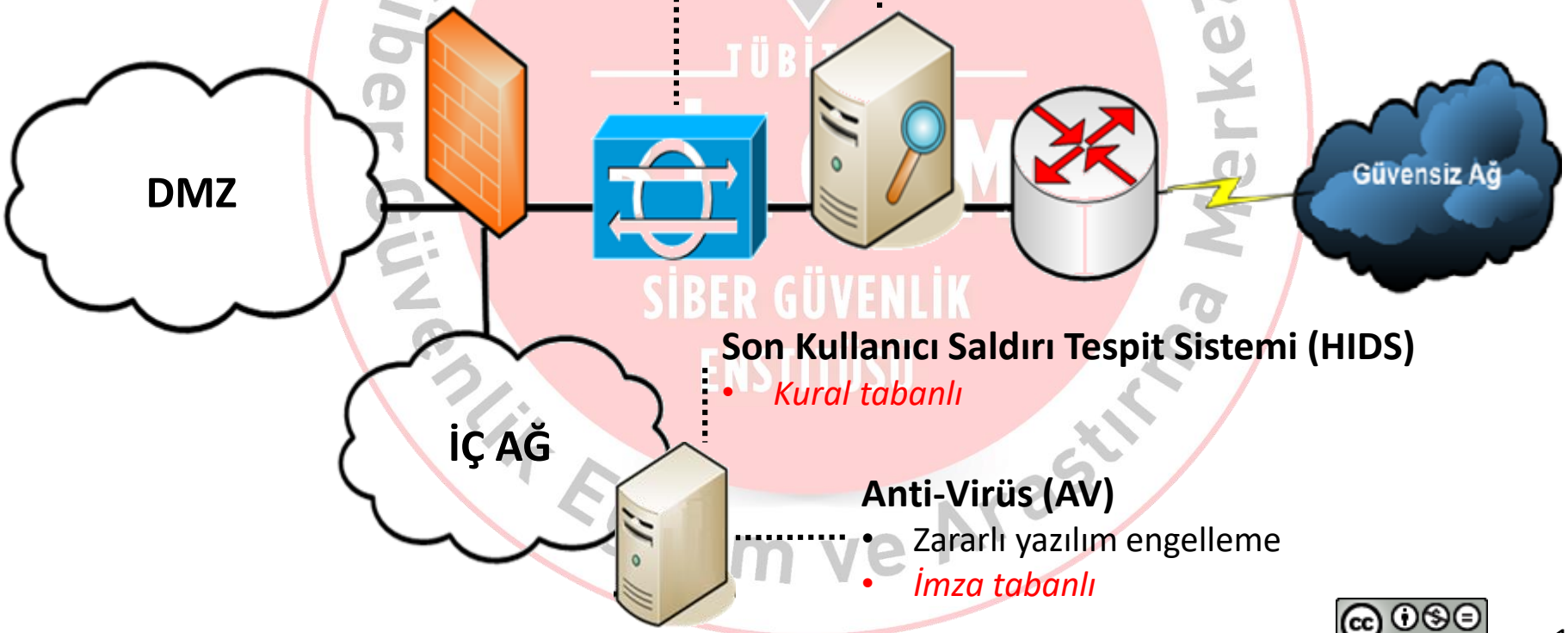
APT Savunma ve Tespit Yöntemleri

Geleneksel güvenlik mekanizmaları

Güvenlik Duvarı (FW)
- IP/Port engelleme
- *Kural tabanlı*

Saldırı Tespit/Engelleme Sistemi (IDS/IDS)
- *İmza tabanlı*

İçerik Kontrolcüsü (Proxy)
- HTTP, FTP, SMTP, POP3 filtreleme
- *Kelime veya konu* tespiti



Son Kullanıcı Saldırı Tespit Sistemi (HIDS)
- *Kural tabanlı*

Anti-Virüs (AV)
- Zararlı yazılım engelleme
- *İmza tabanlı*

egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK
SİBER GÜVENLİK ENSTİTÜSÜ

APT Savunma ve Tespit Yöntemleri

Gelişmiş Siber Casusluk Tehdidi'ne karşı yeni nesil çözümler *

Ağ

- **Ağ Trafik Analizi (NTA)** *gerçek-zamanlı*
  - Gerçek zamanlı tespit (anomali/protokol/içerik analizi)
- **Ağ Forensik Analizi (NF)**
  - Tüm paketleri yakalama ve saklama (yeniden akıtma)

Çalıştırılır Dosya

- **Çalıştırılır Dosya/Döküman Analizi (PA)** *gerçek-zamanlı*
  - Kumhavuzunda (sandbox) çalıştırıp davranış yoluyla tespit

Uç Bilgisayar

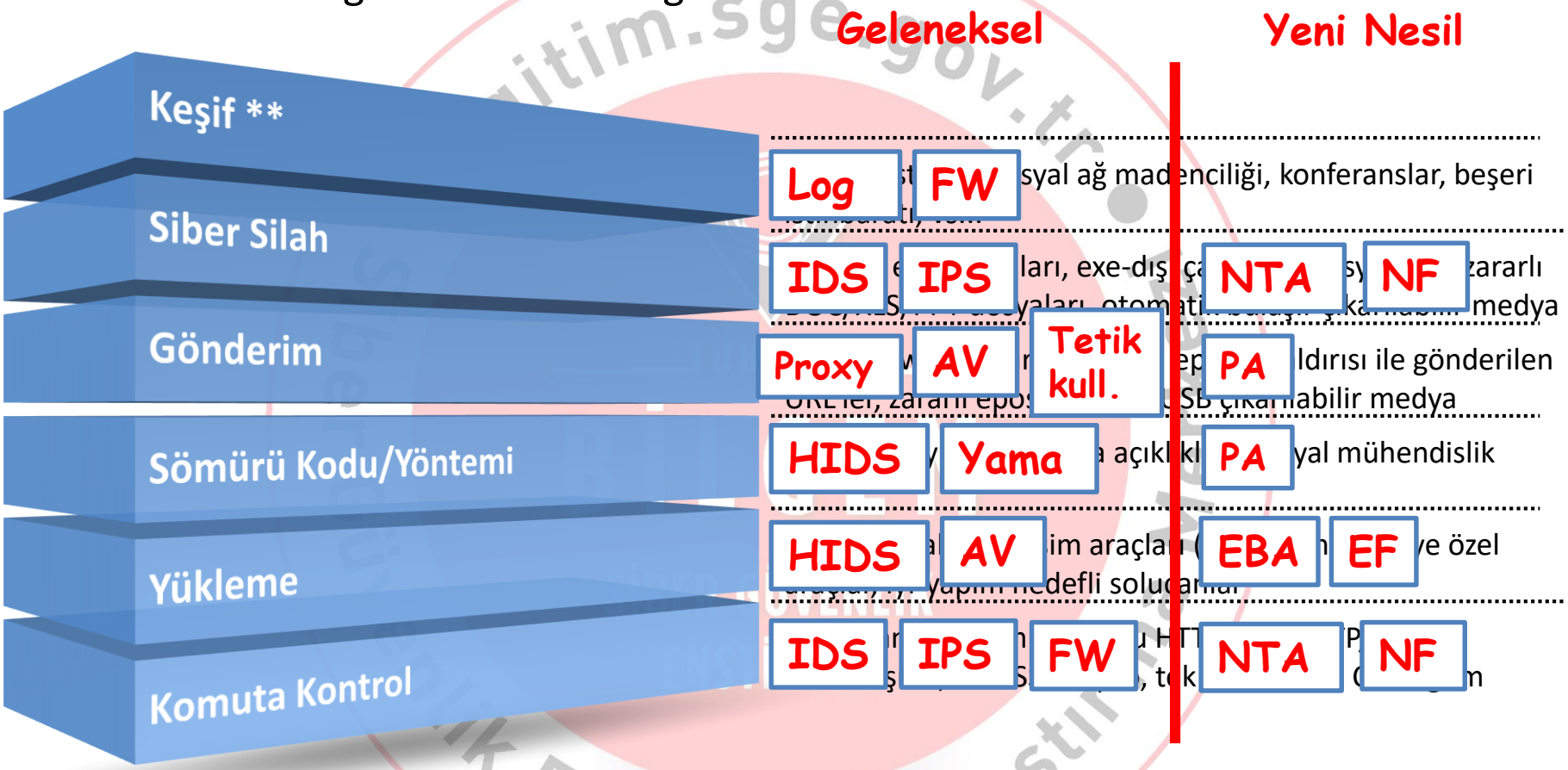
- **Uç Bilgisayar Davranış Analizi (EBA)** *gerçek-zamanlı*
  - Uygulama sınırlama, hafıza izleme, sistem ayar/proses izleme
- **Uç Bilgisayar Forensik Analizi (EF)**
  - Uç bilgisayar izleme ve şüpheli olay takibi

* Gartner: Five Styles of Advanced Threat Defense

cc BY NC ND

APT Savunma ve Tespit Yöntemleri

APT saldırılarının genel karakteristiği *



*FireEye, «World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks Report»

** Lockhead Martin, «Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains»

BY NC ND

Tarihsel APT Saldırıları

TÜBİTAK
egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

Cuckoo’s Egg

- 1980’lerde Batı Almanyalı hackerlar tarafından California’da bulunan Lawrence Berkeley Ulusal Laboratuvarı hatları kullanılarak çeşitli Amerikan kamu kurum ve kuruluşlarının bilgisayarlarına izinsiz erişim sağlanması

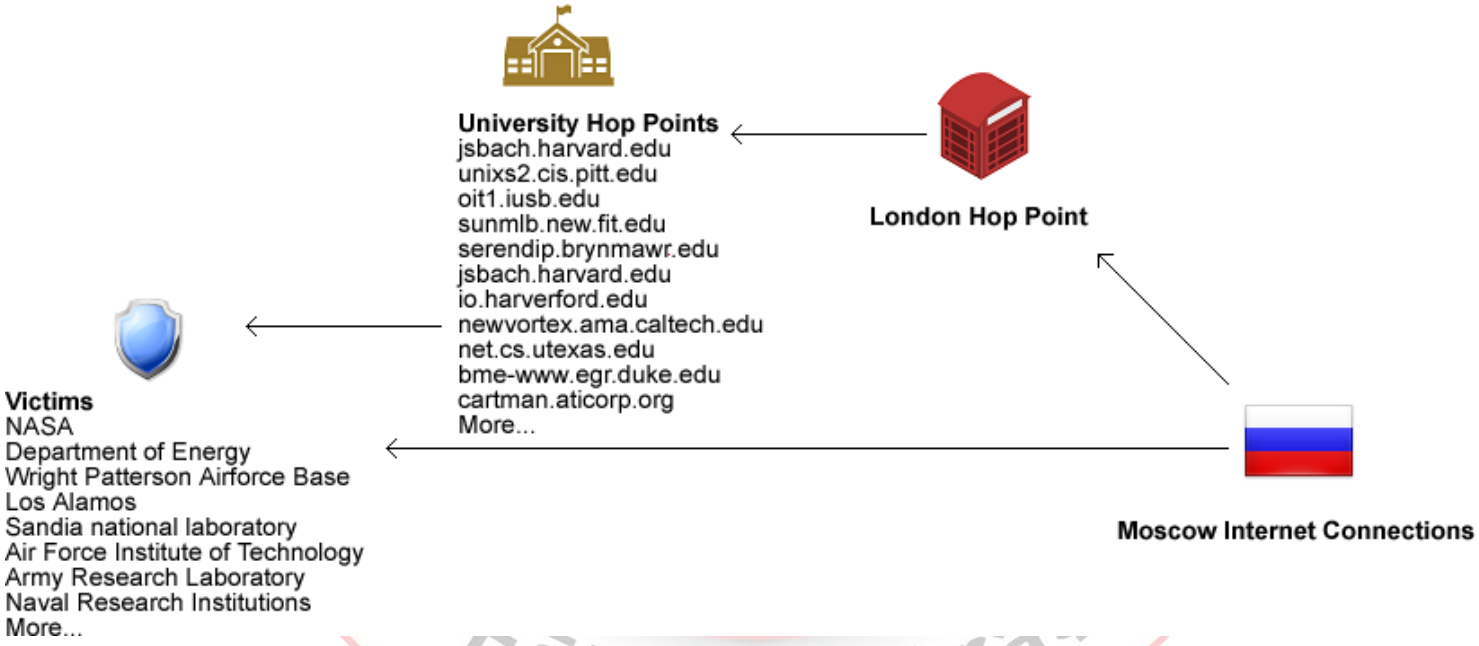
- Lawrence Berkeley Ulusal Laboratuvarı’nda çalışan Clifford Stoll adındaki bir sistem yöneticisi tarafından fark edilmiştir.
- Batı Almanya’da Markus Hess adındaki bir öğrencinin bilgileri Sovyet KGB’ye sattığı tespit edilmiştir.

Siber Güvenlik Enstitüsü • Bilgi Güvenliği Eğitim ve Araştırma Merkezi

CC BY NC ND

Moonlight Maze

- 1998'de Amerikan askeri sistemleri, NASA, üniversiteler ve laboratuvarlar gibi kritik kurumlardan bilgi çalınması.
- ATI-Corp şirketinde bir teknisyenin Pazar sabah 03:00'te kendi ağlarından Wright Patterson Hava Kuvvetleri Üssü'ne bir bağlantı farketmesi.



https://medium.com/@chris_doman

CC BY NC ND

Titan Rain

- 2003’te farkedilen ve en az 3 yıl sürdüğü tahmin edilen ve Amerikan savunma şirketleri başta olmak üzere ulusal laboratuvarlar ve NASA gibi kuruluşları da kapsayan bir APT saldırısı.
- Çin menşei olduğu tahmin edilmektedir.

egitim.sgb.gov.tr

CC BY NC ND

Sykipot

- 2006'da Adobe Reader and Acrobat açıklıklarına kullanarak sistemlere erişim sağlanması.
- Çoğunlukla Amerikan ve İngiliz savunma, telekomünikasyon firmaları hedef alınmıştır.
- Genel olarak phishing ile bulaşmıştır.

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

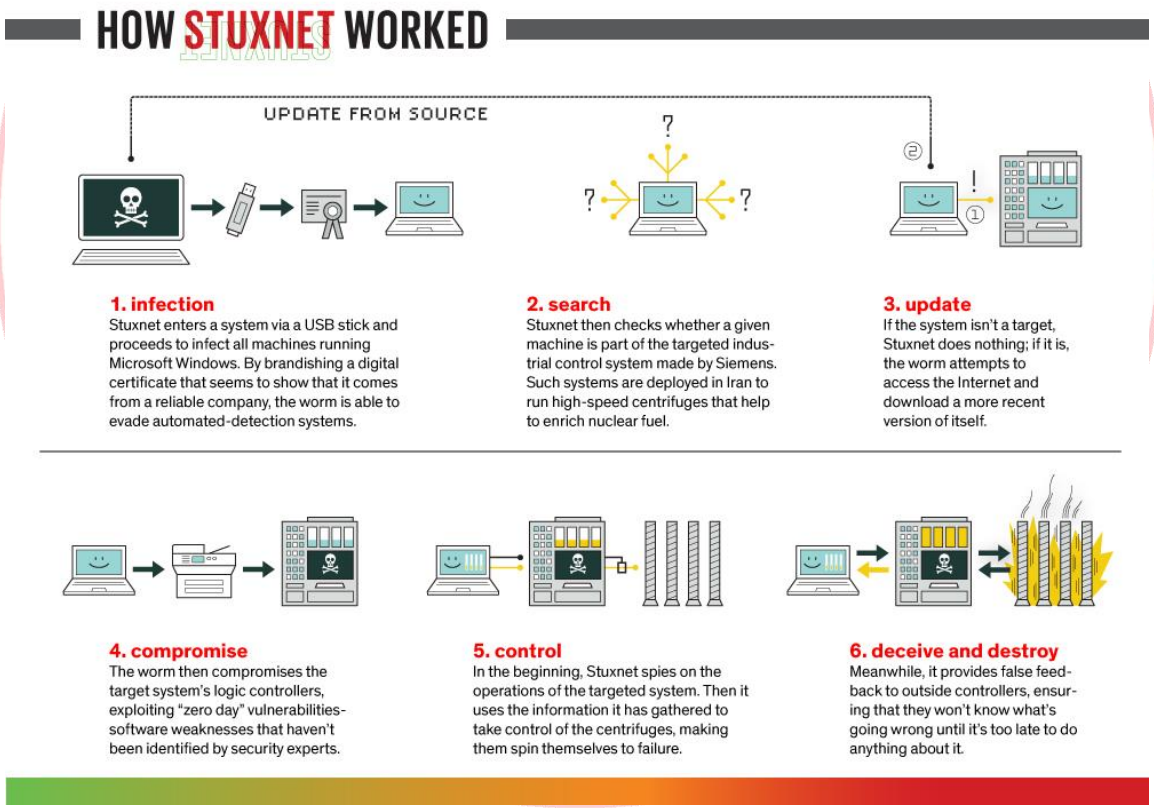
GhostNet

- 2009'da sistemlerin ses ve görüntü kayıt aygıtlarını kullanmak üzere enfekte edilmesini kapsayan APT saldırıları.
- Çin menşei olduğu değerlendirilmektedir.
- Genellikle büyükelçilikler gibi diplomatik temsilciliklere yönelik gerçekleşmiştir.
- 100 ülkede etkili olmuştur.
- E-mail üzerinden phishing ile yayılmıştır.

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

Stuxnet

- 2010'da İran'ın nükleer tesislerine yönelik yapılan ve sadece devlet aktörlerinin yüklenebileceği seviyede karmaşık bir saldırıdır.
- Internet bağlantısı olmadan Windows makinelere USB bellekler ile bulaşacak ve programmable logic controller (PLC) cihazlarını etkileyecek şekilde tasarlanmıştır.

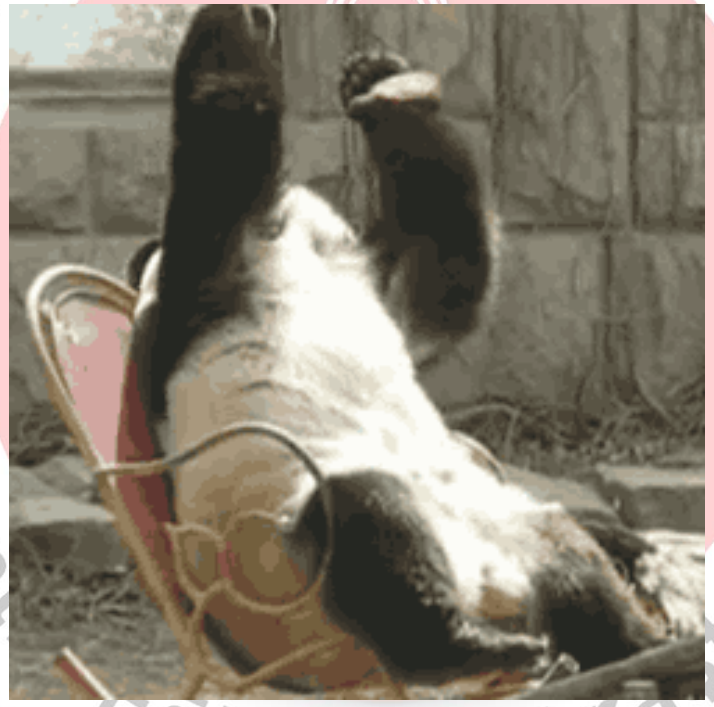


http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

cc BY NC ND

Deep Panda

- 2015’te A.B.D. Personel Yönetim Ofisi’ne (US Government's Office of Personnel Management) yönelik bir APT saldırısıdır.
- Gizli servis çalışanları da dahil olmak üzere 4 milyon çalışanın bilgileri ele geçirilmiştir.



Siber Güvenlik Eğitim ve Araştırma Merkezi
eğitim.sgc.gov.tr

APT Analiz Teknikleri

TÜBİTAK
egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

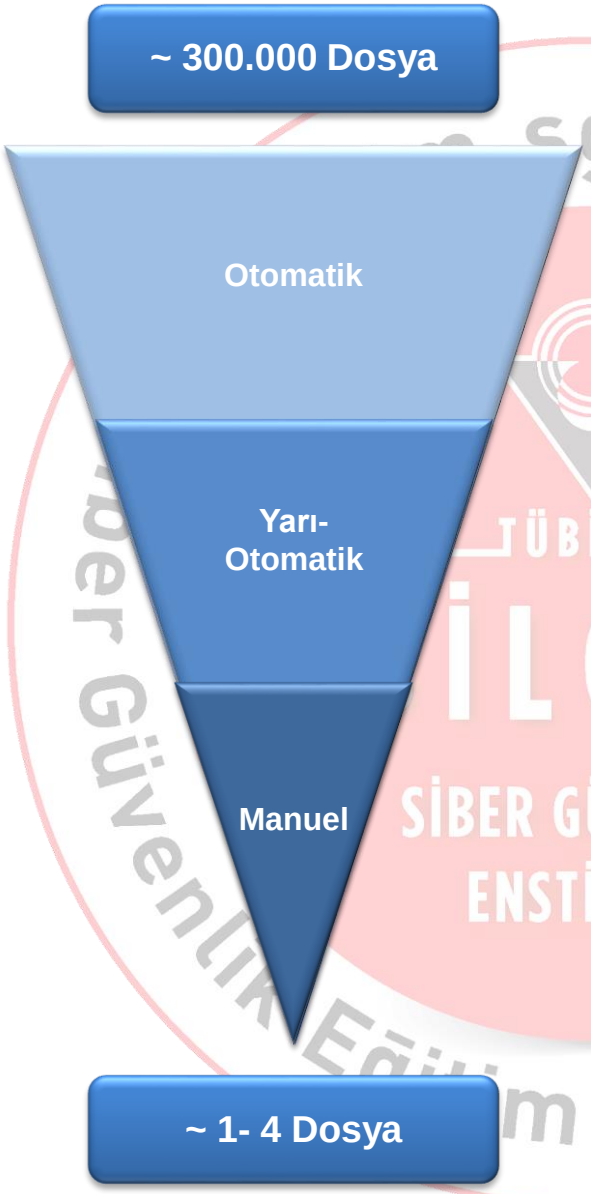
APT Analiz Teknikleri

BY NC ND

APT Analiz Teknikleri

cc BY NC ND

APT Analiz Teknikleri

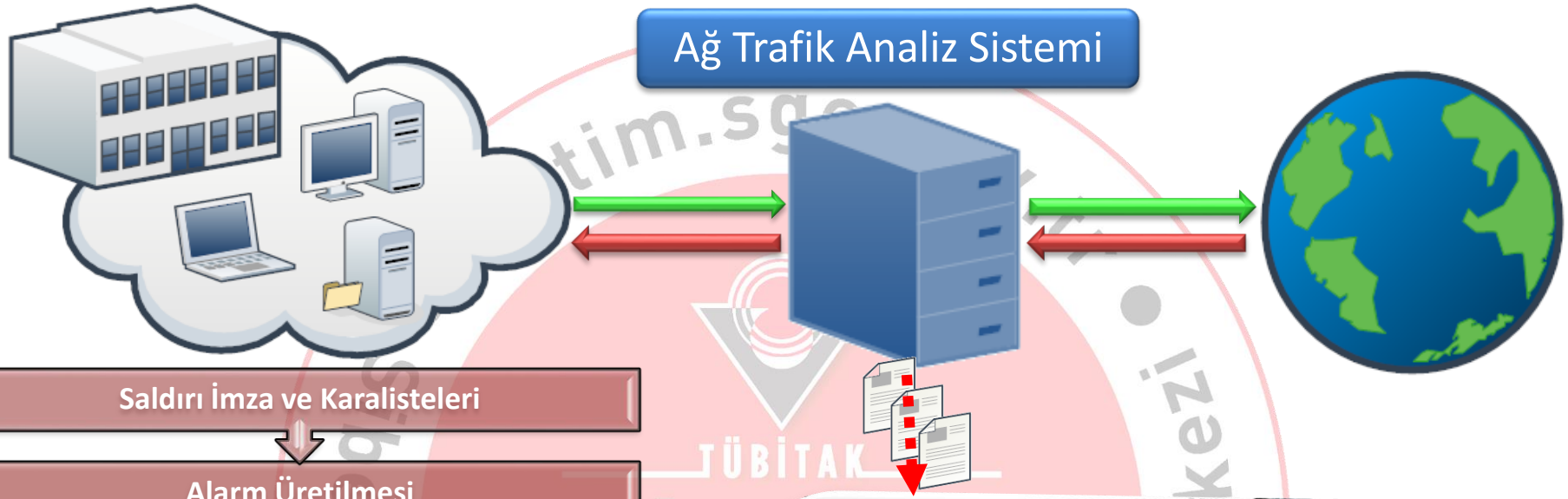


- Veri toplama
- Anti-Virus Taramaları
- Ele Geçirme Göstergeleri (IOC)
- Otomatik Hafıza Analizi
- Sistemde Kalıcılık Tespiti
- Paketlenmiş Dosya / Entropy Analizi
- Log Analizi
- Zaman Çizelgesi ile Analiz
- Toplanan Verilerde Korelasyon
- Manuel Hazıfa Analizi
- Şüpheli Dosya
- MFT Anomalileri

*https://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf

cc BY NC ND

APT Analiz Teknikleri



Saldırı İmza ve Karalisteleri

↓

Alarm Üretilmesi

↓

Şüpheli Dosya Antivirüs Taraması

↓

Ağ Akış Bilgisi Elde Edilmesi

↓

Ağ Trafik Özeti Çıkarılması (HTTP, DNS, FTP, vb.)

↓

İstatistiksel Tablo ve Görsel Arayüzler

↓

Nitelikli Sorgular ve Korelasyonlar

↓

Anomali /Tehdit Tespiti

BY NC ND

APT Analiz Teknikleri

Çalışan uygulamaların kurduğu bağlantıların tehdit puanları

New Search

Save As | Close

```
sourcetype=mir_ports | dedup PortItem.remoteIP, host | lookup threatscore clientip as PortItem.remoteIP |
search threatscore!=0 | sort threatscore | reverse | table threatscore, host, PortItem.remoteIP,
PortItem.remotePort, PortItem.path
```

All time

6 events (before 2/19/14 3:53:52.000 PM)

Events | Statistics (6) | Visualization

20 Per Page | Format | Preview

threatscore	host	PortItem
40	10.50.0.99	88.191.1
28	[illegible]	[illegible]
26	[illegible]	[illegible]

Hafıza analizi şüpheli modüller

Report | Objects | Timeline | Canvas | Binary: APT.img | Digital DNA | Script

Digital DNA Sequence	Name	Process Name	Size	Severity	Weight
042D970F163...	MEMORYMOD-CODE-0x0181000...	explorer.exe	4096		74.8
042D970F163...	MEMORYMOD-CODE-0x0167000...	explorer.exe	4096		74.8
00B4EE00C7C...	irykmmww.dll	iexplore.exe	36864		45.2
00B4EE00C7C...	irykmmww.dll	svchost.exe	36864		45.2
01685A0F6F0...	irykmmww.dll	vmwaretray.exe	49152		43.6
01685A0F6F0...	irykmmww.dll	vmwareuser.exe	49152		43.6
[illegible]	[illegible]	[illegible]	49152		38.6
[illegible]	[illegible]	[illegible]	49152		38.6

Report

0x01810fff)

Summary

Suspicious Modules

Suspicious Module: irykmmww.dll

SUSPICIOUS MODULE -

Traits - irykmmww.dll

Trait

Trait:	68 5A
Description:	Protected storage COM interface DLL - could indicate scanning for username/passwords
Trait:	6F 0E
Description:	Program is accessing a Protected Storage Registry Key for Outlook Express
Trait:	A9 D5
Description:	Program installs hooks into the windows messaging chain. This is very common with keyloggers, but can be used for any windows message type.
Trait:	D3 36
Description:	Program is accessing a Protected Storage Registry Key for FTP, Front Page, password protected web sites
Trait:	49 C1
Description:	Program is accessing a Protected Storage Registry Key for Internet Explorer
Trait:	4F 28

Ele geçirilme göstergesi (IOC) taraması

MFE_Operation_Troy+ (UID: 021f918e)
Ponmocup DLL imports+ (UID: 32a6b675)
Kuluoz_Malware+ (UID: 356ad262)
Kimsucky- (UID: 4849849b)

C:\Projeler\[illegible]Audits\Audits71\[illegible]\[illegible]mir.w32apifiles.72771707.xml

Full Path	Size in Bytes	MD5
C:\Windows\System32\sm\1\taskmgr.exe	1193472	c54e2e5f35ece1b57c36ee935080fa3f
C:\Windows\Temp\SETUP.LOG	184	f0244c24ae27d00819dd5b79ef5da175

C:\Projeler\[illegible]Audits\Audits71\[illegible]\[illegible]mir.w32apifiles.49522907.xml

C:\Projeler\[illegible]Audits\Audits71\[illegible]\[illegible]mir.w32apifiles.5b5e280e.xml

Event #136+ (UID: 4ffeb060)
Event #137+ (UID: 4ffeb539)
Event #139+ (UID: 4ffec233)
Event #744+ (UID: 525bb51c)
Event #780+ (UID: 527a00cc)
Batchwiper+ (UID: 548cfc54)
zwshell+ (UID: 592c059c)
DUQU+ (UID: 5add2090)
Ramnit+ (UID: 5c03d9e7)
Generic Process Path Indicator+ (UID: 7fe9ed86)
Trojan-Bredolab+ (UID: 8ec4e9b3)

Details

close panel [x]

Kimsucky
4849849b-0fa7-4fdf-9685-570618dd2b94

Description

Definition

- ServiceItem/name *is* ' WebClientManager'
- ServiceItem/name *is* ' Remote Access Service'
- AND:
  - FileItem/FilePath *contains* ' system32'
  - OR:
    - FileItem/FileName *is* ' kbdlv2.dll'
    - FileItem/FileName *is* ' auto.dll'
    - FileItem/FileName *is* ' netsvcs.exe'
    - FileItem/FileName *is* ' netsvcs_ko.dll'
    - FileItem/FileName *is* ' vcmon.exe'
    - FileItem/FileName *is* ' svcsmon.exe'
    - FileItem/FileName *is* ' svcsmon_ko.dll'
    - FileItem/FileName *is* ' wsmss.exe'
- AND:
  - OR:
    - FileItem/FilePath *contains* ' winnt'
    - FileItem/FilePath *contains* ' windows'
  - OR:
    - FileItem/FileName *is* ' taskmgr.exe'
    - FileItem/FileName *is* ' setup.log'
    - FileItem/FileName *is* ' winlog.txt'
    - FileItem/FileName *is* ' update.log'

INFORMATION

Author:	madvillain (villain@evilthings.org)
Authored On:	2013-10-03T00:28Z
Updated:	2013-10-03T01:08:20Z

REFERENCES

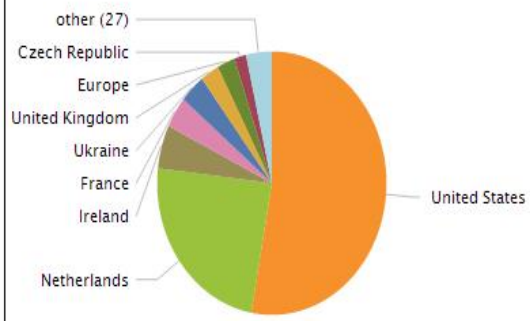
KEYWORDS

CC BY NC ND

APT Analiz Teknikleri

En çok bağlanılan 50 HTTP bağlantısı ve ülkelere dağılımı

HTTP Requests - by COUNTRY



TOP 50 HTTP Connection [without Turkey]

Country	DestinationIP	Url	count	percent
Germany	46.165.232.90	www.ekoayrinti.com	1307261	35.187992
United States	108.162.199.143	i.f5haber.com	66001	1.776572
United States	[illegible]	[illegible]	[illegible]	[illegible]
Sweden	[illegible]	[illegible]	[illegible]	[illegible]
United States	[illegible]	[illegible]	[illegible]	[illegible]
Europe	[illegible]	[illegible]	[illegible]	[illegible]
France	[illegible]	[illegible]	[illegible]	[illegible]
United States	[illegible]	[illegible]	[illegible]	[illegible]
United States	[illegible]	[illegible]	[illegible]	[illegible]

Çok uzunluktaki şüpheli DNS istekleri

Too many same-sized DNS requests from an internal host (Indicating a possible exfiltration)

Url	Length
0lqfaz1i6n1g4uwk10i1axg701753853fc297bf6d4ae2b642621b5a6.bulgaristandaegitim.web.tr	83
012027765dea73f3391c-46328848ae125a3547681ec5d06246c9.r37.cf1.rackcdn.com	73
1f2a292dca0422269d30-0b7e113615eebf298677542280795c6c.ssl.cf1.rackcdn.com	73
285be84fb617dbd13607-633e79af86eef6fa3040b8a64f85b956.r50.cf2.rackcdn.com	73
34a7a1f9164c48c1b61f-84378afe43d6d6b04d77869b7b49ff0e.ssl.cf2.rackcdn.com	73
3bfbfcf1c857f19f8629-084aee1731863a8c068bb2ce733fd518.ssl.cf1.rackcdn.com	73
438424cd093f86f0c7e0-2ed4f1b3b970cf6c05d6a60490c330b4.r88.cf2.rackcdn.com	73
4386b62459dade230dba-c32895c502c77c289149136d[illegible]afb.r55.cf4.rackcdn.com	73
[illegible]	73
[illegible]	73

Her gün belirli zaman aralığında aynı URL'e kurulan bağlantılar

New Search

Save As | Close

```
source="/usr/local/bro/logs/http_filtered.log" | search SourceIP!="[illegible]*" | search DestinationIP!="[illegible]*" | iplocation DestinationIP | streamstats current=f last(_time) as next_time by DestinationIP | eval gap = next_time - _time | stats count avg(gap) var(gap) by Url, DestinationIP, SourceIP, Country | sort + var(gap)
```

All time

Your search is paused. Job | Paused | Verbose Mode

Events (1,237,004) | Statistics (9,072) | Visualization

100 Per Page | Format | Preview | Prev 1 2 3 4 5 6 7 8 9 ... Next

Url	DestinationIP	SourceIP	Country	count	avg(gap)	var(gap)
0.gravatar.com	68.232.35.121	[illegible]102.225	United States	1	35.099330	0.000000
01.creativecdn.com	37.140.238.34	[illegible]102.81	Netherlands	1	0.999793	0.000000
1-ps.googleusercontent.com	173.194.112.12	[illegible]102.161	United States	1	188.184411	0.000000
1-ps.googleusercontent.com	173.194.112.139	[illegible]102.30	United States	1	102.594054	0.000000
1-ps.googleusercontent.com	173.194.112.139	[illegible]102.38	United States	1	2117.476816	0.000000

cc BY NC ND

Sonuç

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma Merkezi

Sonuç

- APT, ülke ve kurumlar için büyük bir tehdit
- Siber saldırılar kolay ama etkisi büyük
- Geleneksel siber savunma mekanizmaları yetersiz
- Tespit için farklı katmanlarda birden koruma ve analiz
- Güncel APTlerde çok sayıda yeni saldırı yöntemi

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

TÜBİTAK

Teşekkürler