

Enine Boyuna Siber Güvenlik

#whoami



@m3karadag
karadag.mcht@gmail
/in/mucahitkaradag

Mucahit Emin Karadag

Cyber Security Consultant
Invictus Europe/PRODAFT

Project Consultant @CanYouPwnMe
Team Lead @AUCC
Team Member @CDM

GNU/Linux & OpenSource

Instructor	@Hacktrick'16	/ Pwn101
	@LYK'16	/ Ağ Güvenliği ve Sızma Testleri

Second Prize	@STM CTF'16	/ Bulamadık
Third Prize	@Sibermeydan'14	/ OctoSec

Siber?



Siber?

- Siber terimi, **sibernetik** kökeninden gelmekte
- İlk olarak 1958 yılında ortaya atıldı
- Canlılar ve/veya makineler arası iletişim disiplinini incelemekte

Siber + BLABLA

- Siber Güvenlik
- Siber Uzay
- Siber Savaş
- Siber Silah
- Siber Casusluk

Güvenlik?



Siber Güvenlik

- Kime/neye yönelik
 - Kurum
 - Kuruluş
 - Son kullanıcı

Siber Güvenlik

- Varlıkları korumak için kullanılan
 - Araçlar
 - Politikalar
 - Güvenlik Kavramları
 - Güvenlik Teminatları
 - Kılavuzlar
 - Risk Yönetimleri
 - Faaliyetler
 - Eğitimler
 - Uygulama ve Teknolojiler bütünüdür.

Siber Uzay



Siber Uzay

- Internet
- Telekomünikasyon
- Bilgisayar sistemleri

Siber Uzay

- Yazılım
 - İşletim Sistem
 - Veritabanı
 - Uygulama ve Yönetimsel yazılımlar
- Donanım
 - Sunucu
 - İstemci
- Altyapı
 - Kablolu/kablosuz iletişim ağları
 - Telsizler
 - Uydu sistemleri
 - İnternet

Siber Uzay

- Elemanları
 - Askeri Ağlar
 - Enerji Dağıtım Ağları
 - Cep Telefonları
 - Uydu Sistemleri
 - Bankalar
 - Sağlık Bilgi Sistemleri

Siber Savaş?



Siber Savaş

- Siber Uzay varlıklarını koruma
- Siber Uzay varlıklarına hasar verme/sızma
- Espiyonaj
 - Snowden
- Sabotaj
 - Stuxnet
 - DoS

Stuxnet

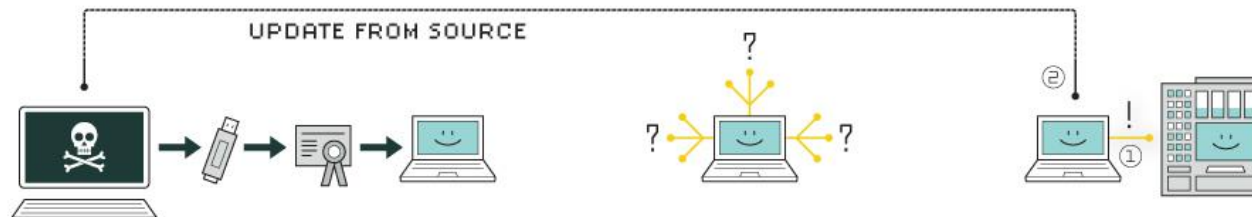
```
CuteMouse v1.9.1 alpha 1 [FreeDOS]
Installed at PS/2 port    CuteMouse v1.9.1 alp
C:\>ver
           in drive C is FREEDOS_C95
FreeCom version 0.82 pl 3 XMS_Swap [Dec 10 2
C:\>dir
           v1.9.1 alph
Volume in drive C is FREEDOS_C95
Volume Serial Number is 04F-192B
Directory of C:\

STUXNET

FDOS             DIR>      08-26-04   6:23p
AUDEX.C  BAT      35      08-26-04   6:24p
BOOT.LT  BIN      512      08-26-04   6:23p
COMMAND  COM     93,963   08-26-04   6:24p
CONFIG   SYS       801    08-26-04   6:24p
FDOSBOOT BIN      512    08-26-04   6:24p
KERNEL   SYS     45,815   04-17-04   9:19p
6 file(s) 6 file(s)      142,038 bytes
1 dir(s)  1,064,517,632 bytes free
C:\>_ CuteMouse v1.9.1 alpha 1 [FreeDOS]
```

Stuxnet

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

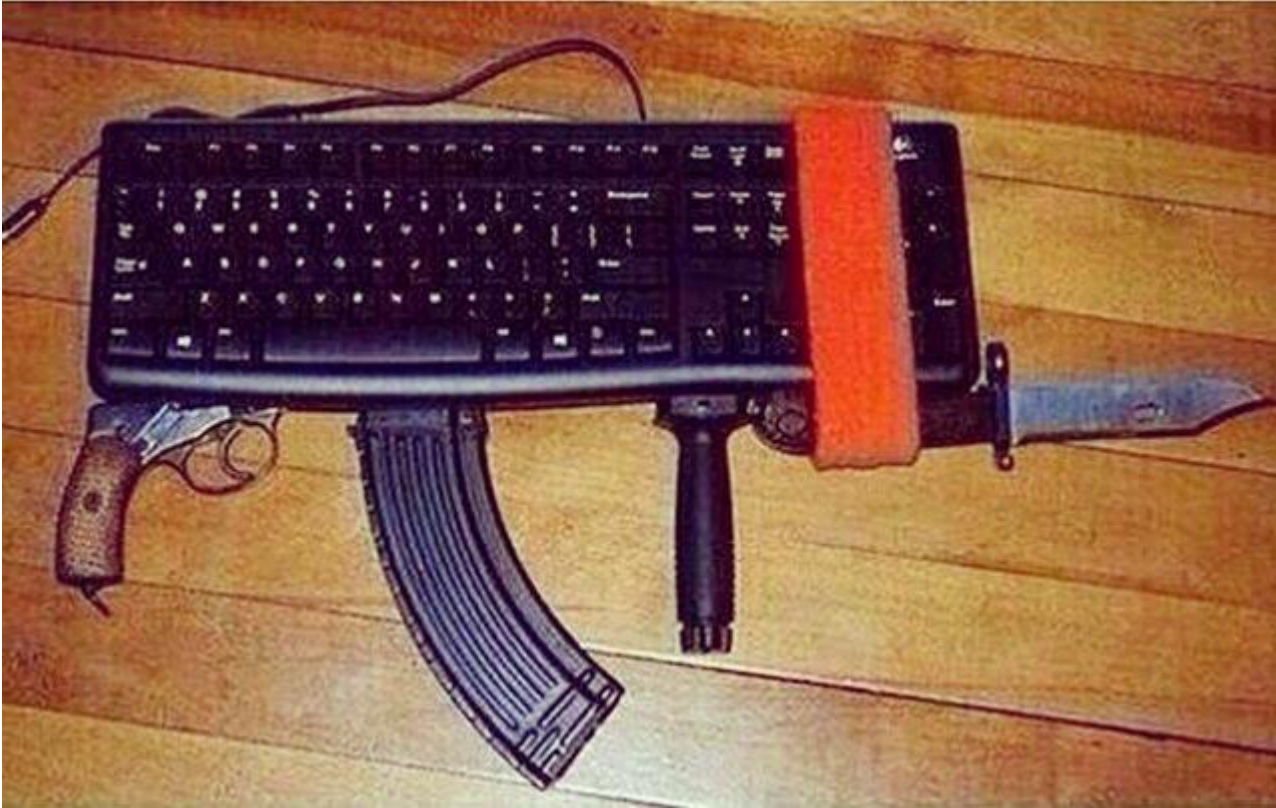
6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Siber Savaş

- Hastanelerin servis veremez hale gelmesi
- Enerji sistemlerinin çökmesi
- Elektronik sisteme sahip savaş elemanları
- Bankalar

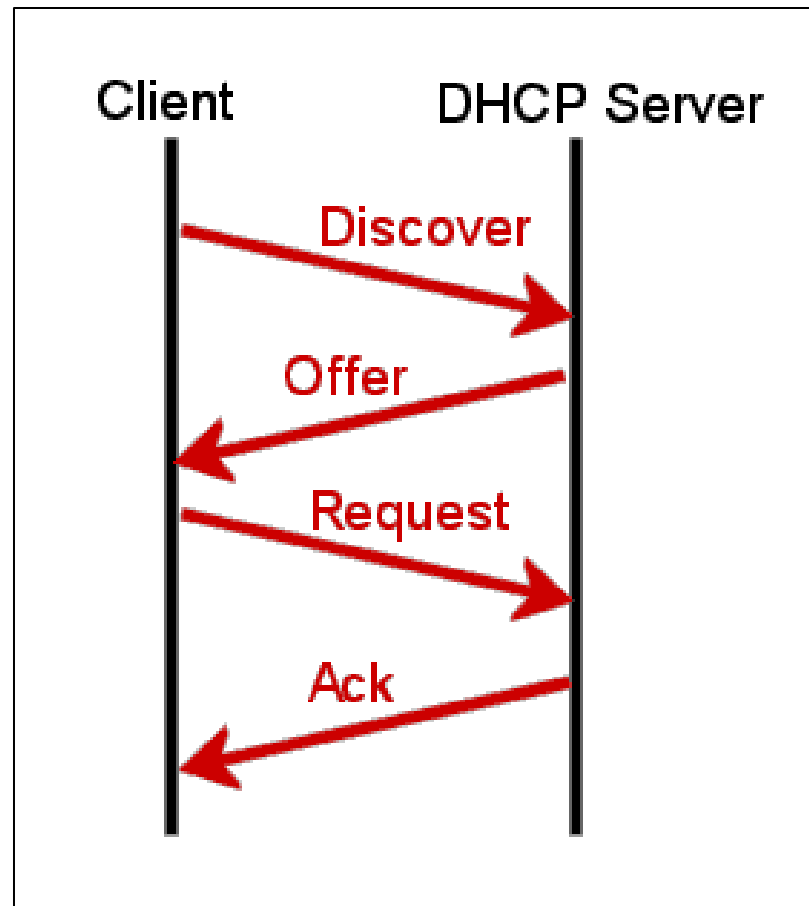
Siber Saldırı



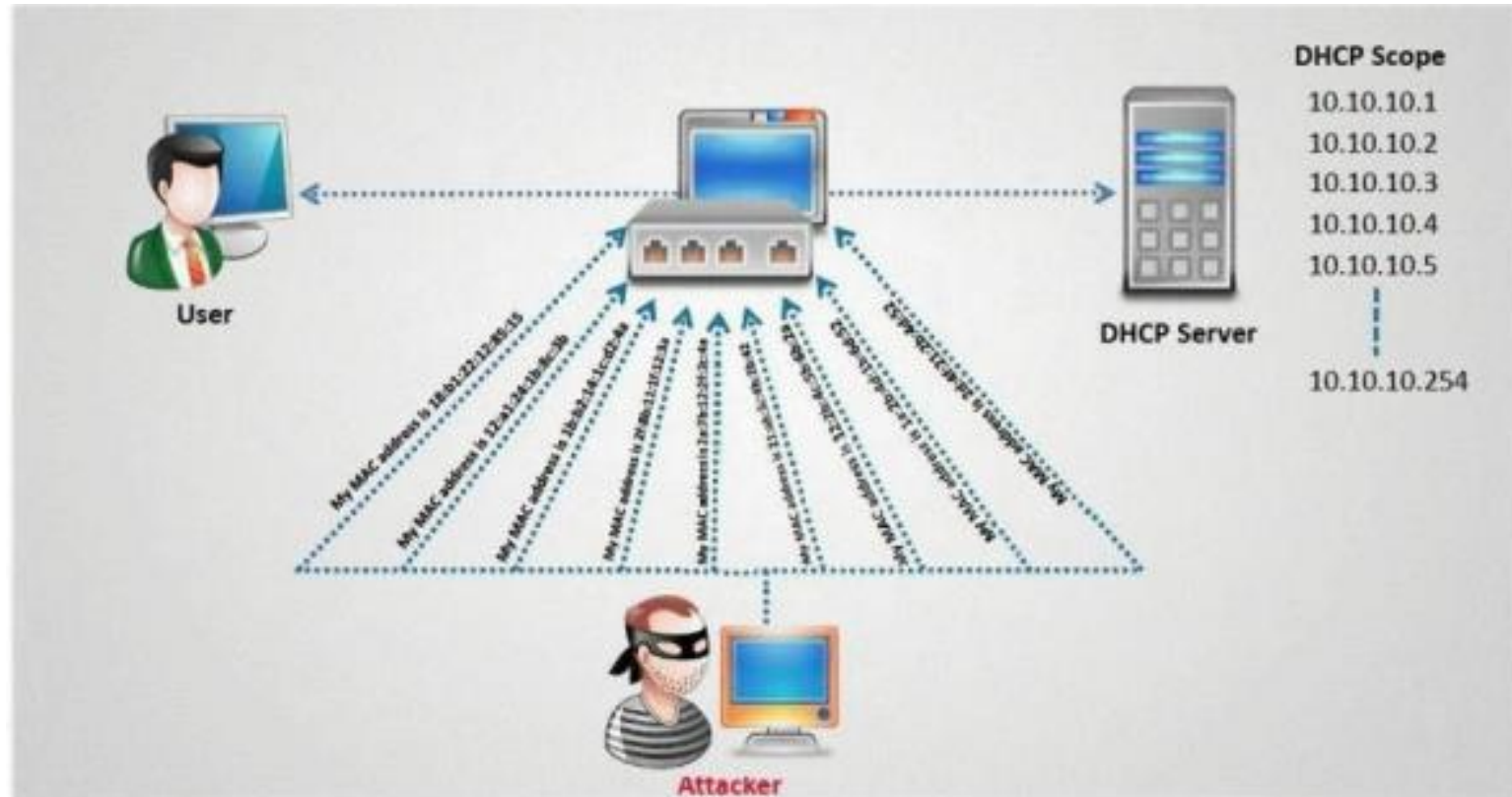
Siber Saldırı

- Ağ
- Web Uygulama
- Hizmet Dışı Bırakma
- Zararlı Yazılım
- Sosyal Mühendislik
- ...

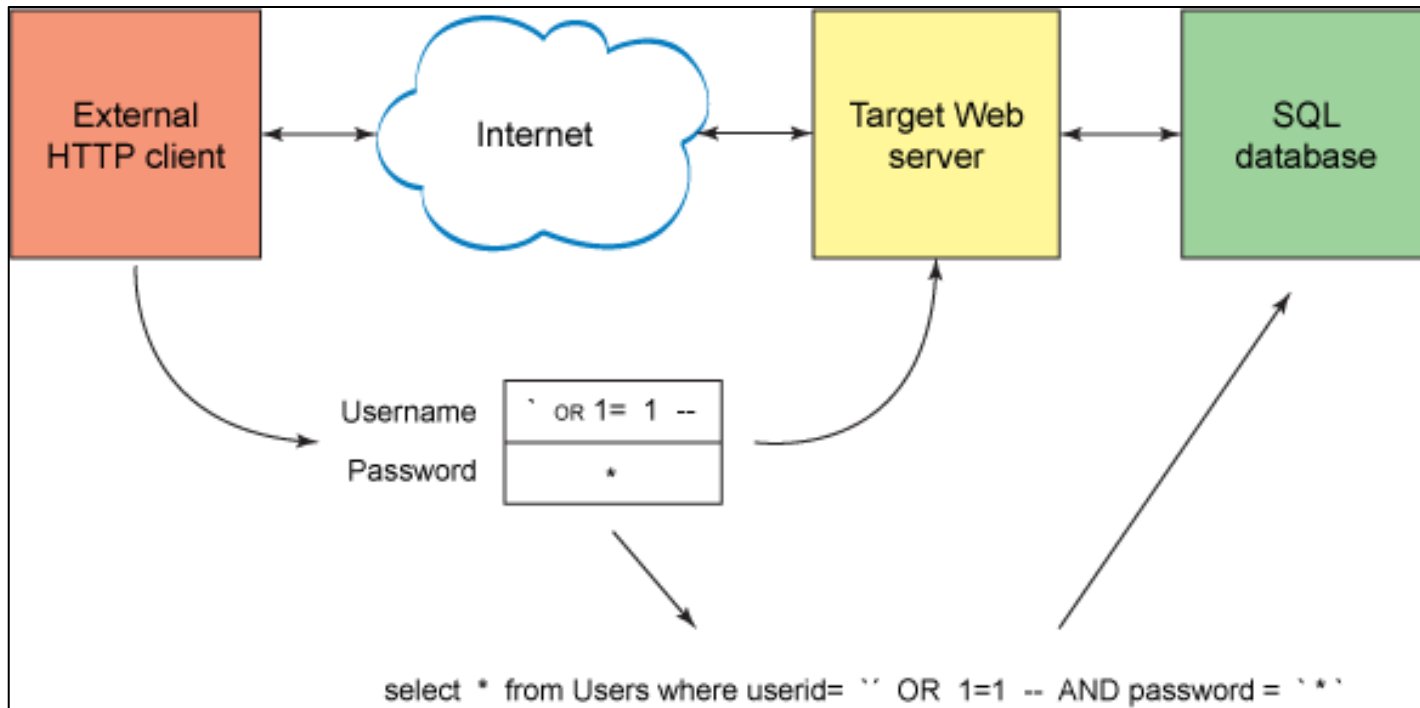
Siber Saldırı



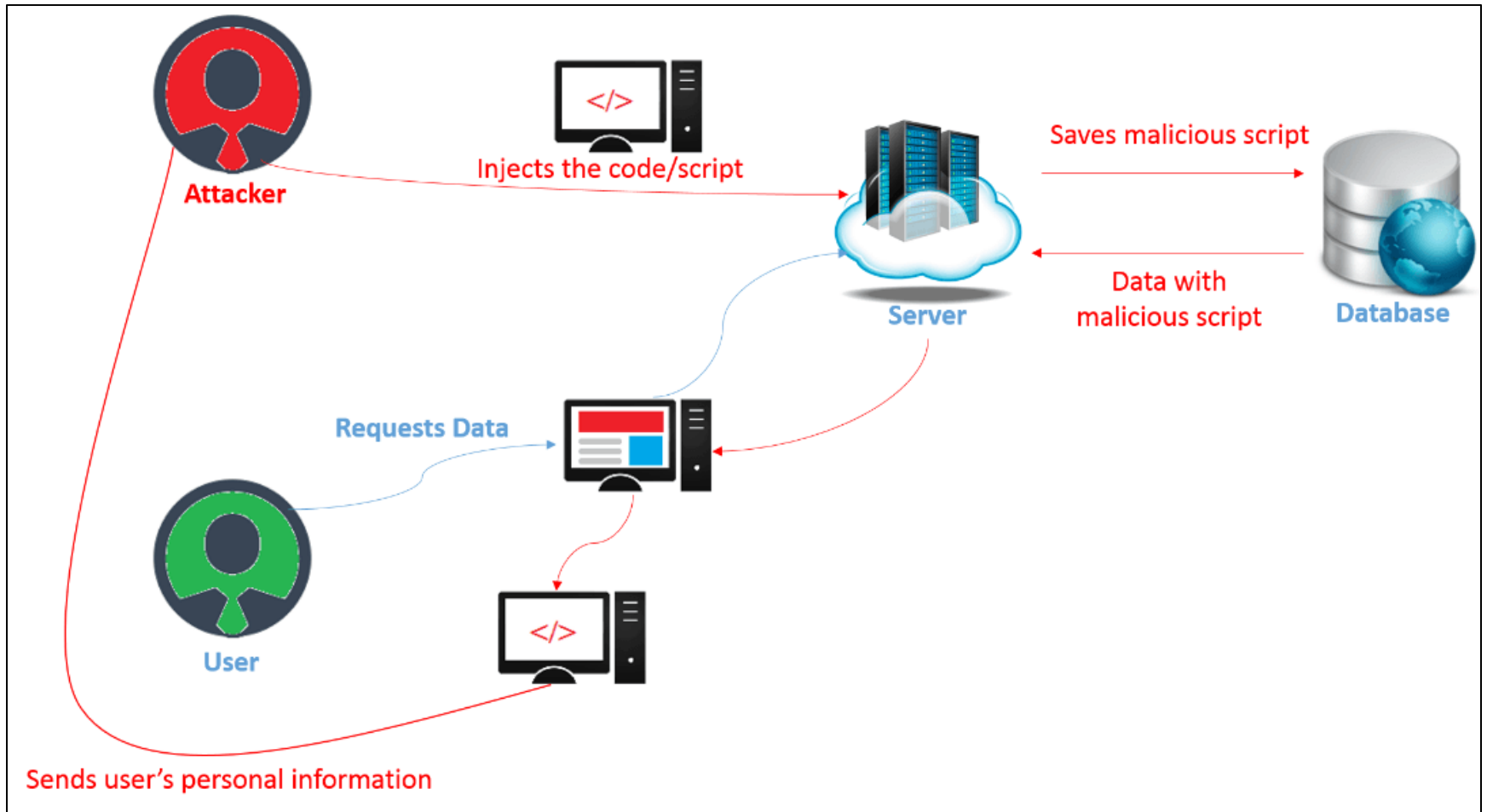
Siber Saldırı



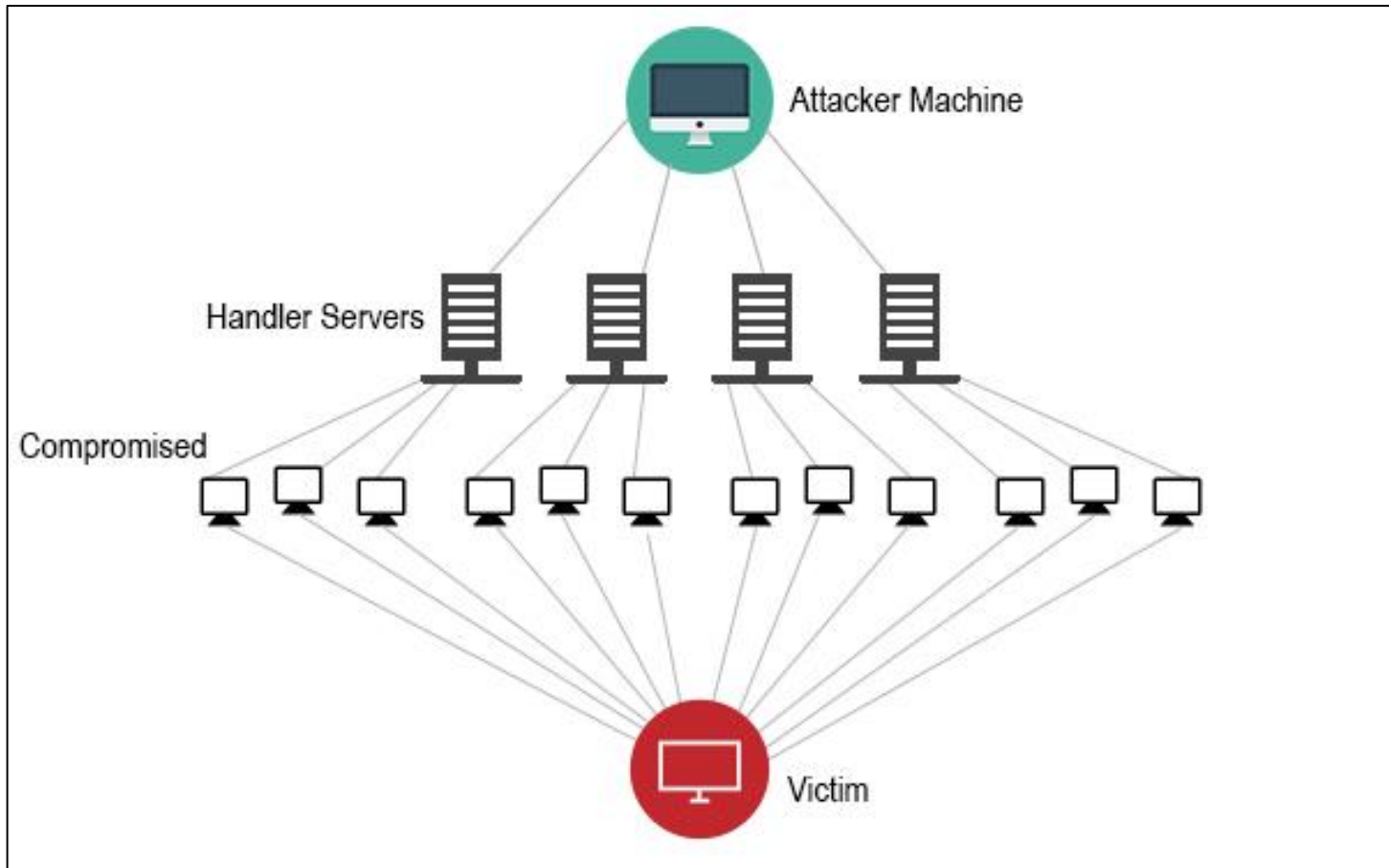
Siber Saldırı



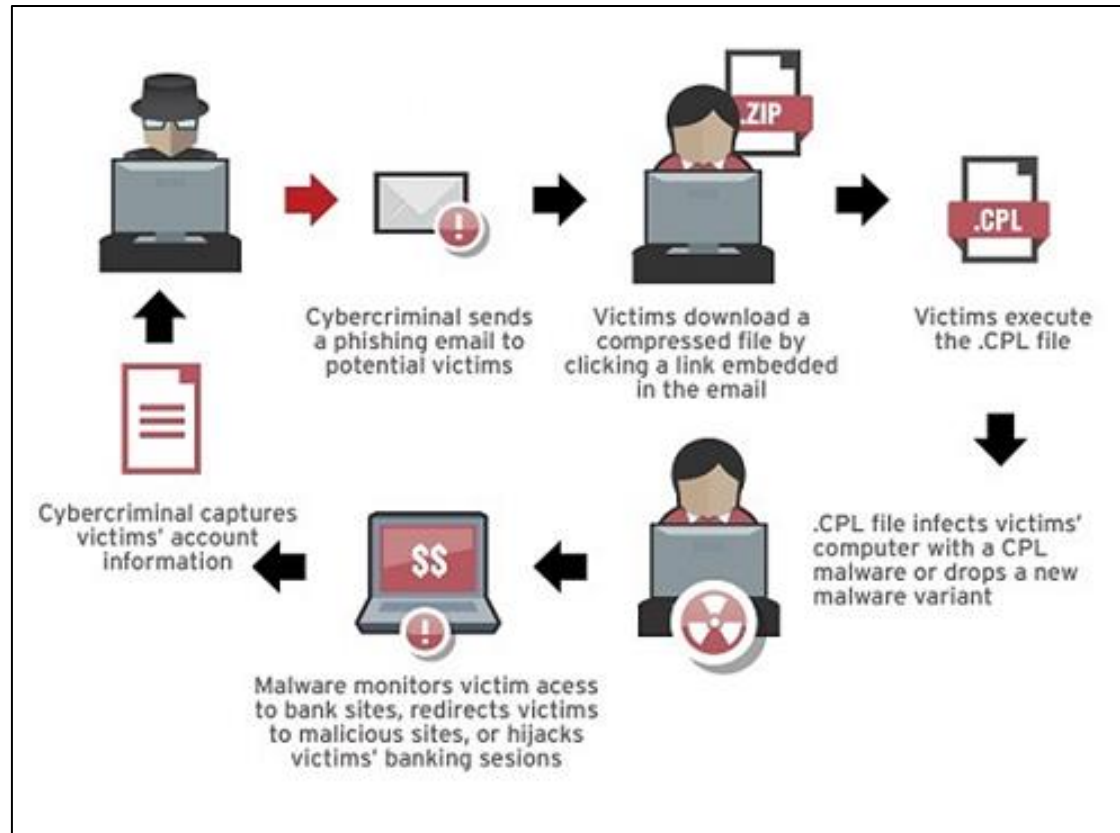
Siber Saldırı



Siber Saldırı



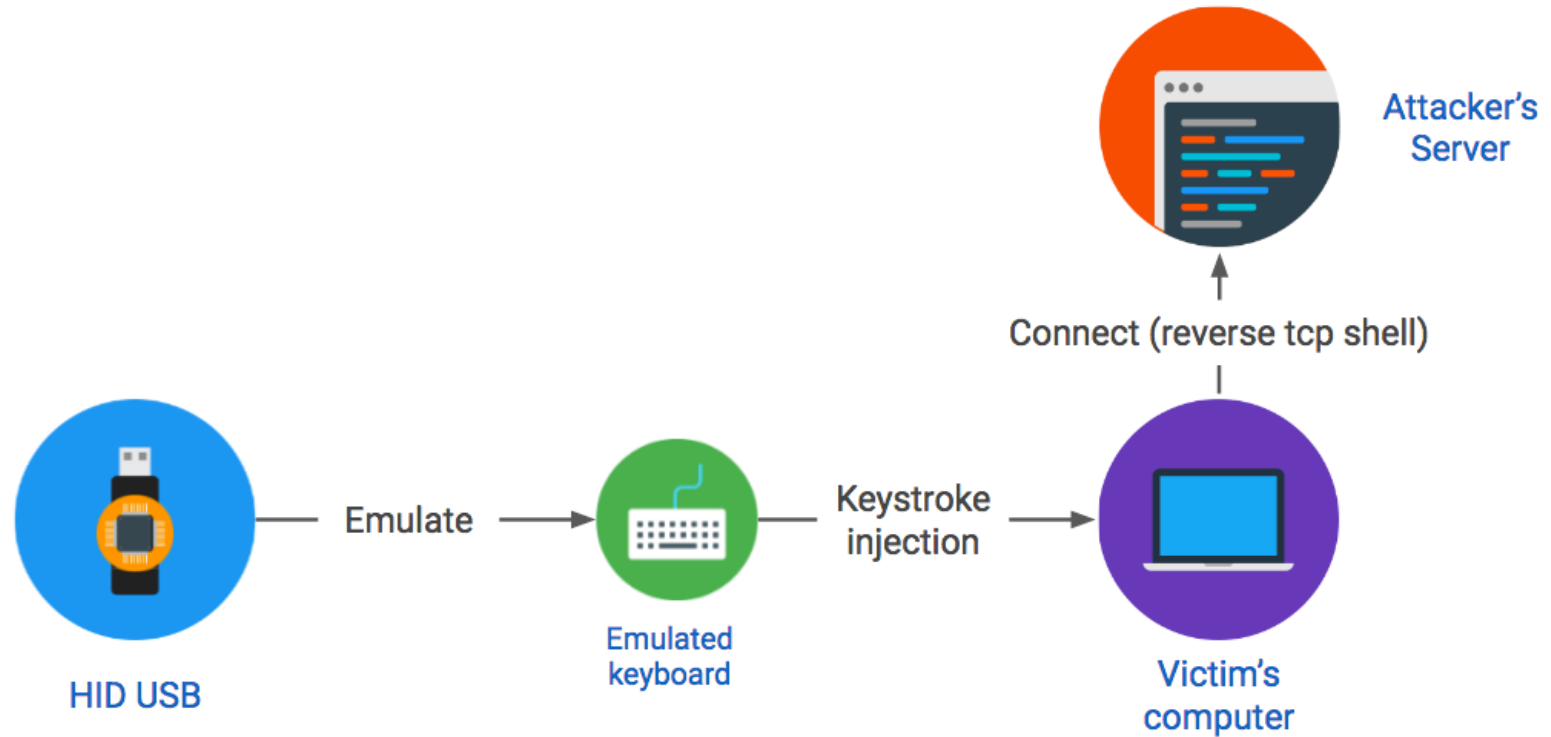
Siber Saldırı



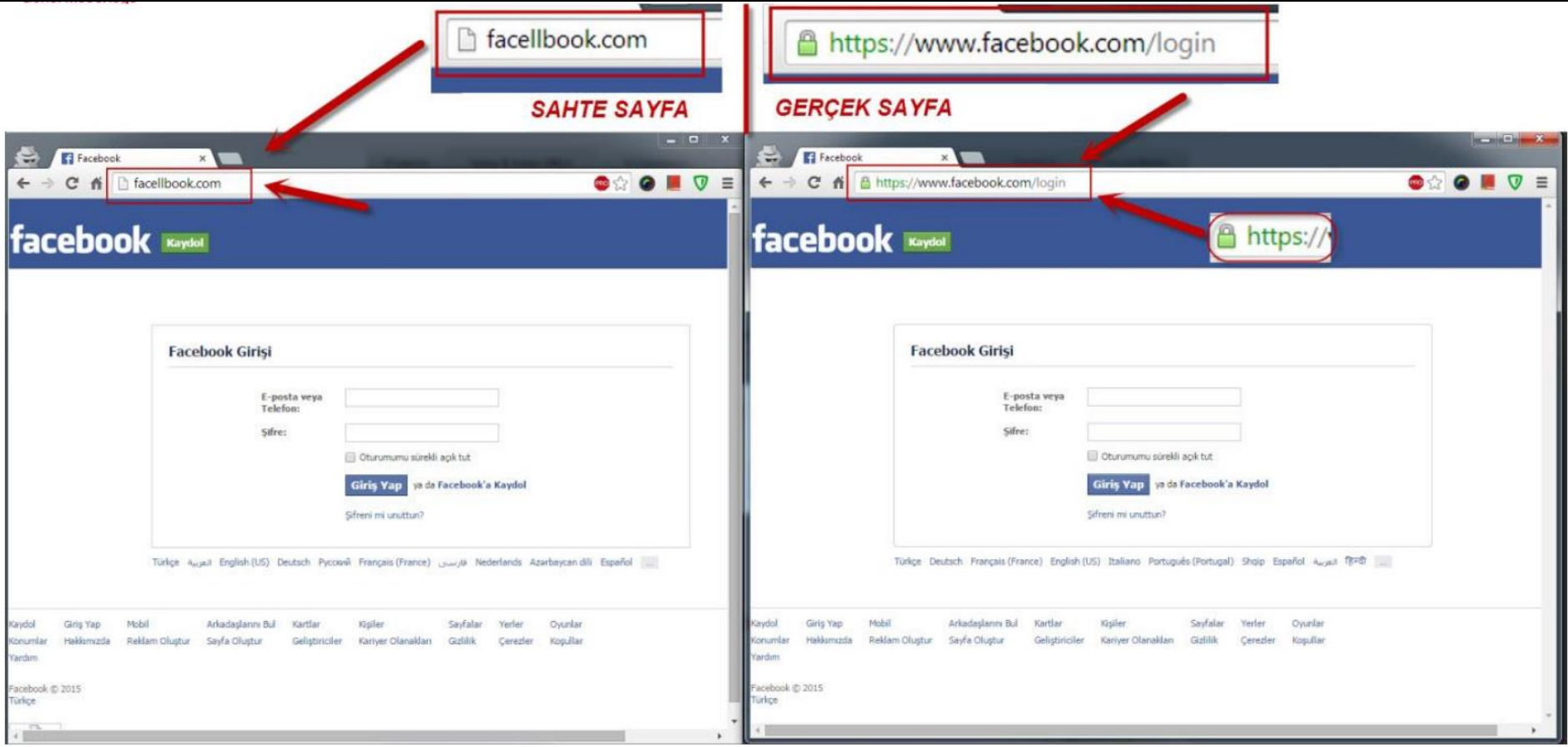
Siber Saldırı



Siber Saldırı



Siber Saldırı



Yaşanmış Örnekler



Yahoo Leak

ANDY GREENBERG SECURITY 09.22.16 12:15 PM

HACK BRIEF: YAHOO BREACH HITS HALF A *BILLION* USERS



Yahoo Leak



Mernis Leak

turkish citizenship database

f t şükela: tümü | bugün

1 ▼ / 18 »

kanım donmuş durumda. türkiye cumhuriyeti vatandaşlarının tüm nüfus bilgileri veri tabanı bizim hükümetimizin teknik çapsizliğinden dolayı şu an bir torrent tığında. herkes şakır şakır indiriyor. ekşi sözlük'e yazmayacaktım bir daha ama sırf şunun için girdim.

49,611,709 türkiye cumhuriyeti vatandaşının tüm kimlik bilgilik bilgileri yahu! el insaf!

f t ^ v

03.04.2016 15:13 ~ 17:35 lovely rita ...


Mernis Leak

← → ↻ 🏠 [https://\[redacted\]](https://[redacted]) 🌐 ⭐ 🔍 📄 📧 📧 📧 ⋮

TurkeyDB Home

Turkish citizenship database

To search use form below.

[View larger map](#)

©2016 Google Map data ©2016 Google, INEGI Terms of Use Report a map error

Find by location

Select city: 81 total

ADANA	1390497
ADIYAMAN	353122
AFYONKARAHISAR	487813
AGRI	265536

NSA



NSA

bglidr1-a-fixed.sancharnet.in__61.1.128.17	mail.issas.ac.cn__159.226.121.1	orange.npix.net__211.43.194.48
bglippi-a-fixed.sancharnet.in__61.1.128.71	mail.pmo.ac.cn__159.226.71.3	orion.platino.gov.ve__161.196.215.67
bj02.cww.com__202.84.16.34	mailscan3.cau.ctm.net__202.175.36.180	outweb.nudt.edu.cn__202.197.0.185
butt-head.mos.ru__10.30.1.130	mails.cneic.com.cn__218.247.159.113	pdns.nudt.edu.cn__202.197.0.180
dcproxy1.thrunet.com__210.117.65.44	mail.siom.ac.cn__210.72.9.2	petra.nic.gov.jo__193.188.71.4
dmn2.bjpeu.edu.cn__202.204.193.1	mailsrv02.macau.ctm.net__202.175.3.120	pop.net21pk.com__203.135.45.66
dns2.net1.it__213.140.195.7	mailsvra.macau.ctm.net__202.175.3.119	postbox.mos.ru__10.30.10.32
doors.co.kr__211.43.193.9	mail.tropmet.res.in__203.199.143.2	post.netchina.com.cn__202.94.1.48
enterprise.telesat.com.co__66.128.32.67	mail.tsinghua.edu.cn__166.111.8.17	public2.zz.ha.cn__218.29.0.200
eol1.egyptonline.com__206.48.31.2	mail.zzu.edu.cn__222.22.32.88	rayo.pereira.multi.net.co__206.49.164.2
fw433.npic.ac.cn__168.160.71.3	mbi3.kuicr.kyoto-u.ac.jp__133.103.101.21	sea.net.edu.cn__202.112.5.66
gambro3.cs.tin.it__194.243.154.62	mcd-su-2.mos.ru__10.34.100.2	sedesol.sedesol.gob.mx__148.233.6.164
gate.technopolis.kirov.ru__217.9.148.61	metcoc5cm.clarent.com__213.132.50.10	segob.gob.mx__200.38.166.2
hakuba.janis.or.jp__210.232.42.3	mipsa.ciae.ac.cn__202.38.8.1	sky.kies.co.kr__203.236.114.1
imms1.macau.ctm.net__202.175.36.54	mn.mn.co.cu__216.72.24.114	smmu-ipv6.smmu.edu.cn__202.121.224.5
indy.fjmu.edu.cn__202.112.176.3	most.cob.net.ba__195.222.48.5	smtp.2911.net__218.245.255.5
jur.unn.ac.ru__62.76.114.22	mpkhi-bk.multi.net.pk__202.141.224.40	smtp.macau.ctm.net__202.175.36.220
kacstserv.kacst.edu.sa__212.26.44.132	msgstore2.pldtpv.net__192.168.120.3	sonatns.sonatrach.dz__193.194.75.35
known.counsellor.gov.cn__61.151.243.13	mtccsun.imtech.ernet.in__202.141.121.198	sparc.nour.net.sa__212.12.160.26
kserv.krldysh.ru__194.226.57.53	mx1.freemail.ne.jp__210.235.164.21	sps01.office.ctm.net__202.175.4.38
laleh.itrc.ac.ir__80.191.2.2	n02.unternehmen.com__62.116.144.147	sunhe.jinr.ru__159.93.18.100
laleh.itrc.ac.ir__80.191.2.2	nd11mx1-a-fixed.sancharnet.in__61.0.0.46	sussi.cressoft.com.pk__202.125.140.194
m0-s.san.ru__88.147.128.28	ndlimc1-a-fixed.sancharnet.in__61.0.0.46	tx.micro.net.pk__203.135.2.194
mail1.371.net__218.29.0.195	ndlimx1-a-fixed.sancharnet.in__61.0.0.46	ultra2.tsinghua.edu.cn__166.111.120.10
mail.bangla.net__203.188.252.3	ndl1pp1-a-fixed.sancharnet.in__61.0.0.71	unknown.counsellor.gov.cn__61.151.243.13
mail.edi.edu.cn__218.104.71.61	noi.unternehmen.com__62.116.144.150	unk.vver.kiae.rr__144.206.175.2
mailgate.sbell.com.cn__202.96.203.173	no3.unternehmen.org__62.116.144.190	voyager1.telesat.com.co__66.128.32.68
mail-gw.jbic.go.jp__210.155.61.54	ns1.2911.net__202.99.41.9	web-ccfr.tsinghua.edu.cn__166.111.96.91
mailgw.thtf.com.cn__218.107.133.12	ns1.multi.net.pk__202.141.224.34	webnetra.entelnet.bo__166.114.10.28
mail.hallym.ac.kr__210.115.225.25	ns2.rosprint.ru__194.84.23.125	webserv.mos.ru__10.30.10.2
mail.hangzhouit.gov.cn__202.107.197.199	ns2.xidian.edu.cn__202.117.112.4	ws.xjb.ac.cn__159.226.135.12
mailhub.minaffet.gov.rw__62.56.174.152	ns.cac.com.cn__202.98.102.5	www21.counsellor.gov.cn__130.34.115.132
mail.hz.zh.cn__202.101.172.6	ns.huawei.com.cn__202.96.135.140	www21.counsellor.gov.cn__61.151.243.13
mail.imamu.edu.sa__212.138.48.8	ns.nint.ac.cn__210.83.3.26	www.caramail.com__195.68.99.20
mail.interq.or.jp__210.157.0.87	opcw dns.opcw.nl__195.193.177.150	www.siom.ac.cn__202.127.16.44
mail.ioc.ac.ru__193.233.3.6	opserver01.iti.net.pk__202.125.138.184	



Celil ÜNÜVER

@celilunuver

Follow

#theshadowbrokers in yayınladığı belgelerde NSA ' in 2001 yılında #Roketsan ' a ait bir Solaris sunucuya sızdığı görülüyor.

```
GRAPEUNIQUE war.rkts.com.tr 195.142.144.125 20011101-171614() {  
#  
# RETICULUM Version:6.6 OS:sparc-sun-solaris2.7  
#  
set host war.rkts.com.tr  
set ip 195.142.144.125  
set hostType "Solaris27"  
set len 476  
set cv0 b18aedc2  
set cv1 33ca08ea  
set cv2 c9af0874  
set timeout 10  
set retries 5  
set baduids { }  
set maxdelay 1.5  
set mindelay 1.0
```

RETWEETS

81

LIKES

84



1:37 PM - 31 Oct 2016



81



84



Celil ÜNÜVER @celilunuver · Nov 1

@omerkartal shadow brokers grubu , NSA in bilgi belgelerini ve toollarini leak ediyor



1



HackingTeam

]HackingTeam[

Rely on us.

Remote Control System

THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION

HackingTeam



HackingTeam

← → ↻ 🏠 pastebin.com/raw/OSNSvyj

[4] https://securelist.com/sites/2013/02/Carbanak_APT_eng.pdf

[5] <http://madrid.cnt.es/noticia/consideraciones-sobre-el-ataque-informatico-a-gamma-group>

--[2 - Hacking Team]-----

Hacking Team was a company that helped governments hack and spy on journalists, activists, political opposition, and other threats to their power [1][2][3][4][5][6][7][8][9][10][11]. And, occasionally, on actual criminals and terrorists [12]. Vincenzetti, the CEO, liked to end his emails with the fascist slogan "boia chi molla". It'd be more correct to say "boia chi vende RCS". They also claimed to have technology to solve the "problem" posed by Tor and the darknet [13]. But seeing as I'm still free, I have my doubts about its effectiveness.

[1] <http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/>

[2] http://www.prensa.com/politica/claves-entender-Hacking-Team-Panama_0_4251324994.html

[3] <http://www.24-horas.mx/ecuador-espio-con-hacking-team-a-opositor-carlos-figueroa/>

[4] <https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/>

[5] <https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/>

[6] <https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/>

[7] <http://focusecuador.net/2015/07/08/hacking-team-rodas-paez-tiban-torres-son-espiados-en-ecuador/>

[8] <http://www.pri.org/stories/2015-07-08/these-ethiopian-journalists-exile-hacking-team-revelations-are-personal>

[9] <https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/>

[10] <http://www.wired.com/2013/06/spy-tool-sold-to-governments/>

[11] http://www.theregister.co.uk/2015/07/13/hacking_team_vietnam_apt/

[12] http://www.ilmessaggero.it/primopiano/cronaca/yara_bossetti_hacking_team-1588888.html


[13] http://motherboard.vice.com/en_ca/read/hacking-team-founder-hey-fbi-we-can-help-you-crack-the-dark-web

OVH

securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html

150,000 IoT Devices behind the 1Tbps DDoS attack on OVH

September 27, 2016 By [Pierluigi Paganini](#)

60
 My Page

The hosting provider OVH continues to face massive DDoS attacks launched by a botnet composed at least of 150000 IoT devices.

Last week, the hosting provider OVH faced 1Tbps DDoS attack, likely the largest one ever seen.

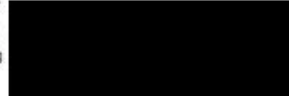
The OVH founder and CTO Octave Klaba reported the 1Tbps DDoS attack on Twitter sharing an image that lists the multiple sources of the attack.

"Last days, we got lot of huge DDoS. Here, the list of "bigger than 100Gbps" only. You can see the simultaneous DDoS are close to 1Tbps !" [said Klaba](#).

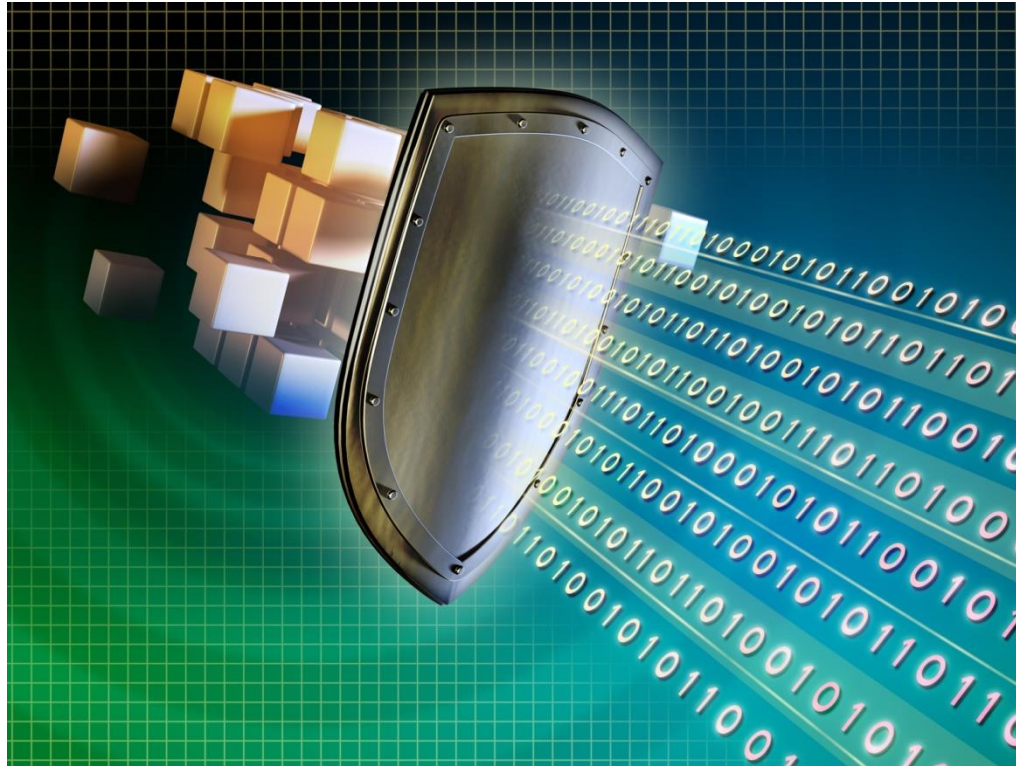
Klaba explained that the servers of its company were hit by multiple attacks exceeding 100 Gbps simultaneously concurring at 1 Tbps DDoS attack. One of the attacks documented by the OVH reached 93 MMps and 799 Gbps.



```
log /home/.../log... | egrep pps | ...  
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ //g" | cut -f  
1,2,3,7,8,10,11 -d '|' | sed "s/.....bps/Gbps/" | sed  
"s/.....pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g  
rep "gone" | sed "s/gone/"/"  
Sep18|10:49:12|tcp_ack|20Mpps|232Gbps
```



Savunma Sistemleri



Savunma Sistemleri

- Kimlik Doğrulama Sistemi
- Zafiyet Tarayıcı
- Güvenlik Duvarı
- IDS / IPS
- AV

Kariyer

IT Leaders



What I Think I Do



What My Mom Thinks I Do



What Finance Thinks I Do



What Business Users
Think I Do



What Business Users
Want Me To Do



What I'm Actually Doing

Kariyer

- Cyber Security Professional
- Information System Auditor
- Security Advisors
- Software Developers
- IT Specialists
- IT System Executives
- IT Consultans
- Software Test Engineer
- R&D Executive
- Security Consultant
- System Engineer
- Network Engineer
- Network Administrator
- Network Architect
- Blablabla....

Kariyer

- Siber Güvenlik Uzmanı
 - Teknik
 - Politika
 - Tarih
 - Disiplin
 - Sosyoloji

Kariyer

- Sızma Testi Uzmanı
 - Programlama
 - Scripting
 - Ağ
 - OSI, TCP/IP, Traffic Analyze
 - Web
 - FrontEnd, BackEnd, DBs
 - Ters-kod
 - x86
 - Okumak
 - Okumak
 - Okumak x 213124

İleri Okuma

- Hacking Exposed 7: Network Security Secrets and Solutions
- Rtfm: Red Team Field Manual
- Black Hat Python: Python Programming for Hackers and Pentesters
- Gray Hat Python: Python Programming for Hackers and Reverse Engineers
- Hacking: The Art of Exploitation, 2nd Edition
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws
- Metasploit: The Penetration Tester's Guide





Eğitim Planları

- GNU/Linux Sistem Yönetimi
- MS Windows Sistem Yönetimi
- Ağ Güvenliği
- Web Uygulama Güvenliği
- Kriptografi

Takımlar

- Network
- Web
- SYSAdmin
- Reverse
- Malware
- Forensic

Bug Bounty

- Hackerone
- Bugcrowd
- Private Bug Bounty

CTF

- ctftime.org
- vulnhab.com
- [wargames](https://wargames.com)
- [Hackmetu](https://hackmetu.com)
- [DKHOCTF](https://dkhoctf.com)
- [ringzer0](https://ringzer0.com)

Gelecek Planlaması

- Kendi yağımızda CTF
- Ulusal CTF
- Uluslararası CTF
- Bize ait CTF

Gelecek Planlaması

- Blog
- Vulnerable VMs
- Ankara University Cyber Lab

Topluluklar/Etkinlikler

- Linux Yaz Kampı
- Akademik Bilişim Günleri
- Tubitak Yaz/Kış Kampı
- Havelsan Yaz Kampı
- NOPCON
- Hacktrick