



# Advanced Banking Malware Via Tor

October 29, 2015 - UBC  
Raul Alvarez

# About Me



# About Me



- Senior Security Researcher @ Fortinet
- 21 published articles in Virus Bulletin
- Regular contributor in our company blog



# Tools





- Sysinternals
  - (<https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx>)
  - Process Explorer
  - Process Monitor
  - etc
- for rootkits
  - GMER (<http://www.gmer.net/>)
  - IceSword
- PEStudio(<http://www.winitor.com/>)
  - v8.46

# Tools for Malware Analysis (Deeper View)



- OllyDbg (<http://www.ollydbg.de/>) by Oleh Yuschuk
  - 64-bit (05-Feb-2014)
- Immunity Debugger(<http://debugger.immunityinc.com/>)
- x64\_dbg(<http://x64dbg.com/>) – open source x64/x32 debugger
  - 30 December 2014 – latest version
- IDA Pro
  - ([https://www.hex-rays.com/products/ida/support/download\\_freeware.shtml](https://www.hex-rays.com/products/ida/support/download_freeware.shtml))
  - v5.0 is FREE
- volatility (<http://www.volatilityfoundation.org/>)
  - memory forensic

# Different Types of Malware



# Different Types Of Malware



- Viruses (file infectors)
- Trojans
- Botnet
- Ransomware
- POS Malware
- Banking Malware



# Agenda





- Vawtrak
  - Different features
  - Different layers
  - Multiple armoring strategies within the layers
  - **Domain Name Generator(DGA ) for its C&Cs**
  - Use of Tor2web
  
- Tor
  - Hidden Services + .onion addresses
  - Tor installation
  - **Creating your own hidden service**
  - **Personalizing your own .onion address**
  
- Can Vawtrak really use DGA to create a randomized Tor C&Cs?

# Banking Malware





- Binary updates/enhancements

- Operational commands

- Storage of stolen banking credentials

- Latest configuration



- Binary armoring to avoid detection

- Continuous monitoring of AV detection

- Using DGA to minimize takedowns

- Hiding its C&C via Tor

Vawtrak



# What is Vawtrak?



- Also known as Neverquest

- A banking trojan

- Uses layering techniques similar to a Matryoshka doll

- Uses multiple armoring strategies

- Uses DGA

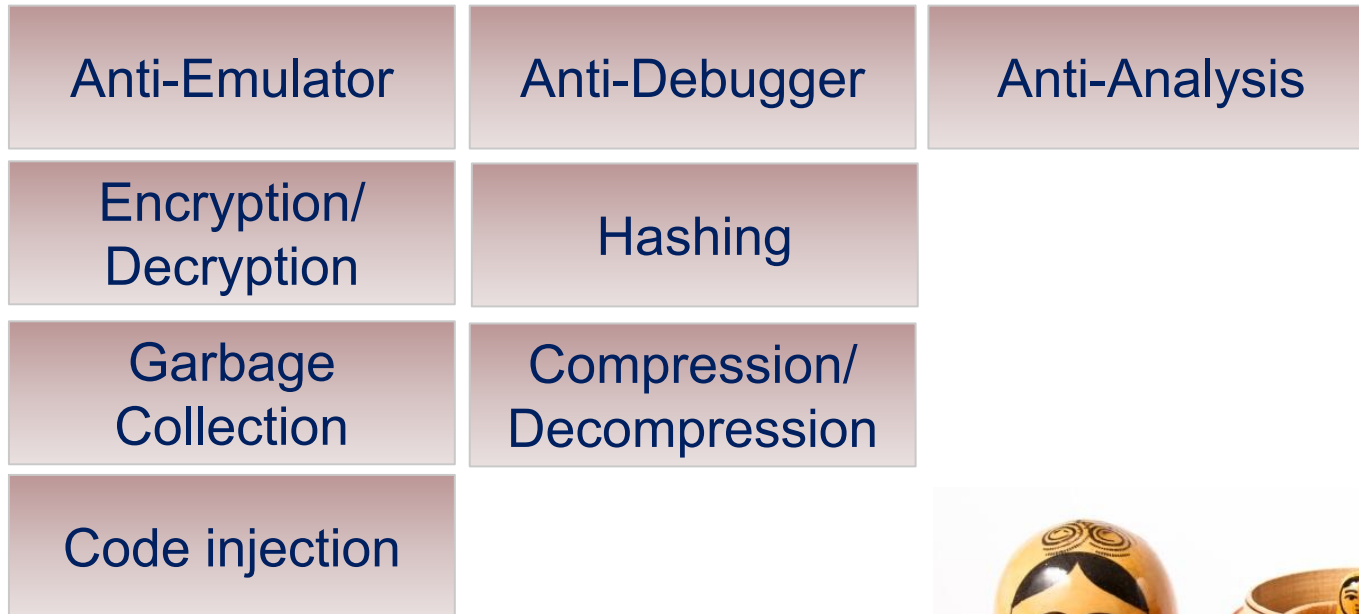
- Uses Tor2web

# Layers Of Vawtrak

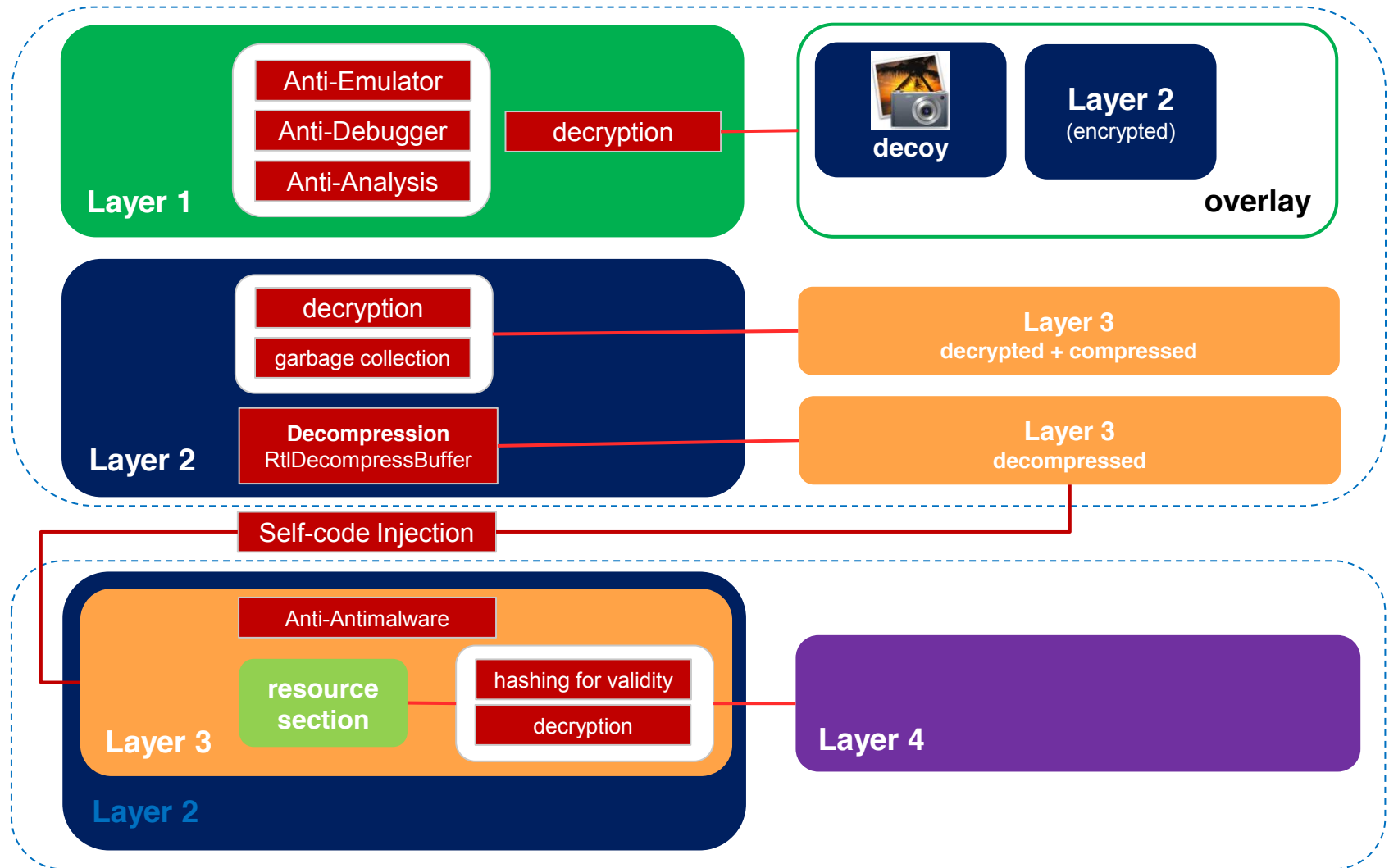




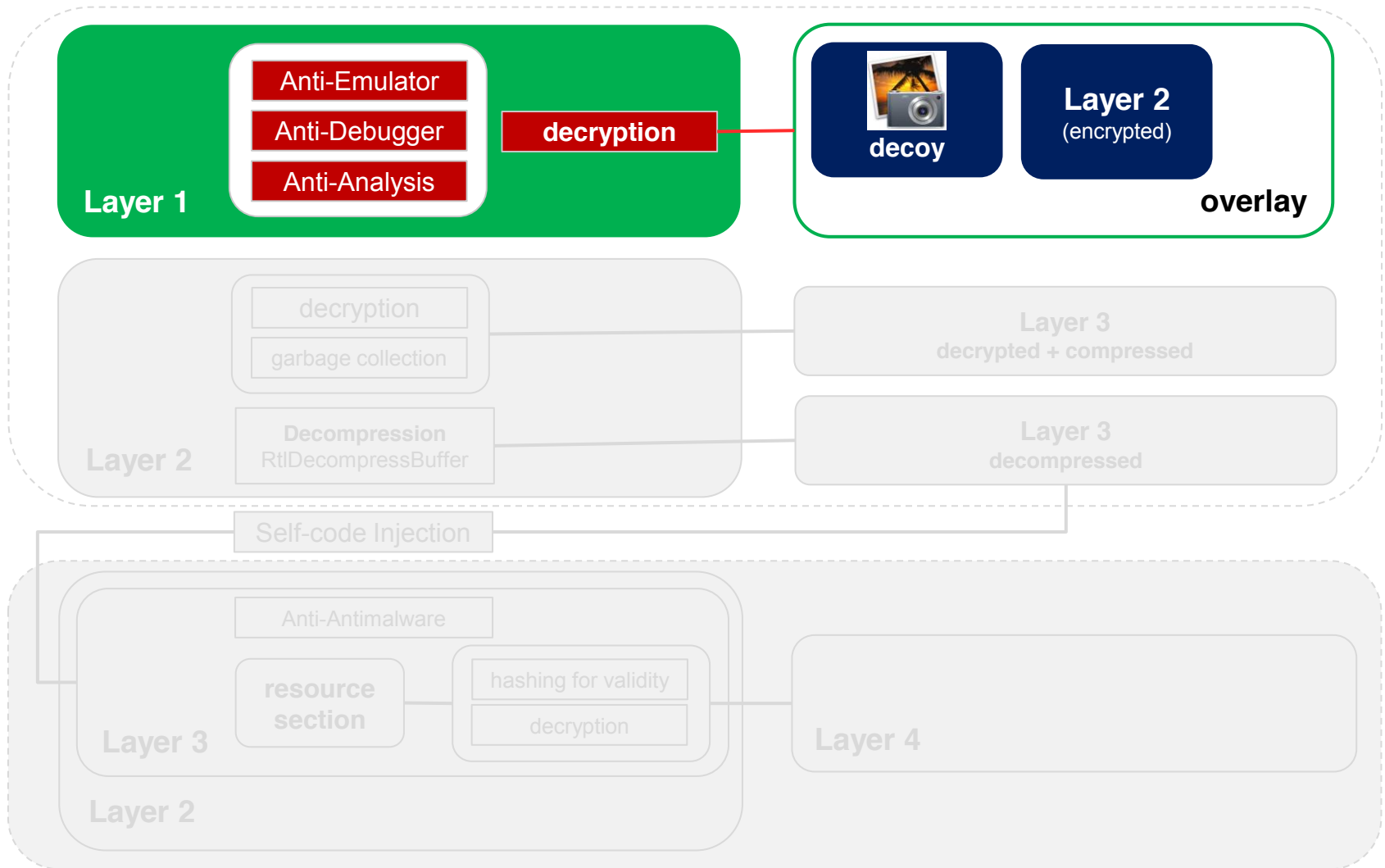
# Armoring Strategies Within The Layers



# Layers of Vawtrak



# Layer 1



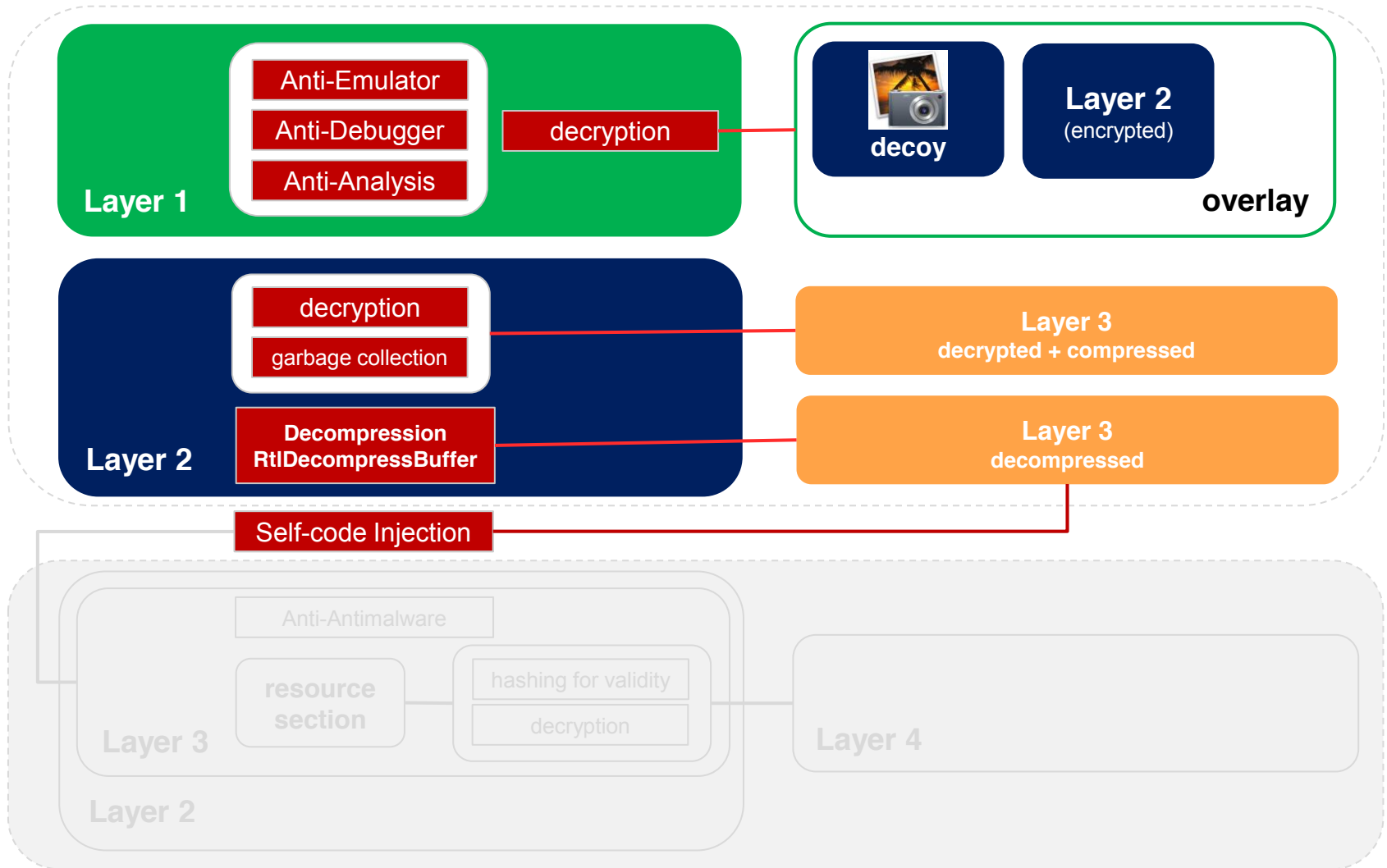


<b>Anti-Emulator</b>	Uses hundreds of instruction 0x00 ADD BYTE PTR DS:[eax],al
<b>Anti-Debugger</b>	Parses the PEB to check for BeingDebugged Flag PEB – Process Environment Block
<b>Anti-Analysis</b>	Uses RETN instruction to call the API Pushes all parameters in stack memory including the API address (to hide the actual API call)
<b>Encryption/ Decryption</b>	Decrypts the encrypted 2 <sup>nd</sup> layer Decrypts the decoy file

# Decoy File



# Layer 2

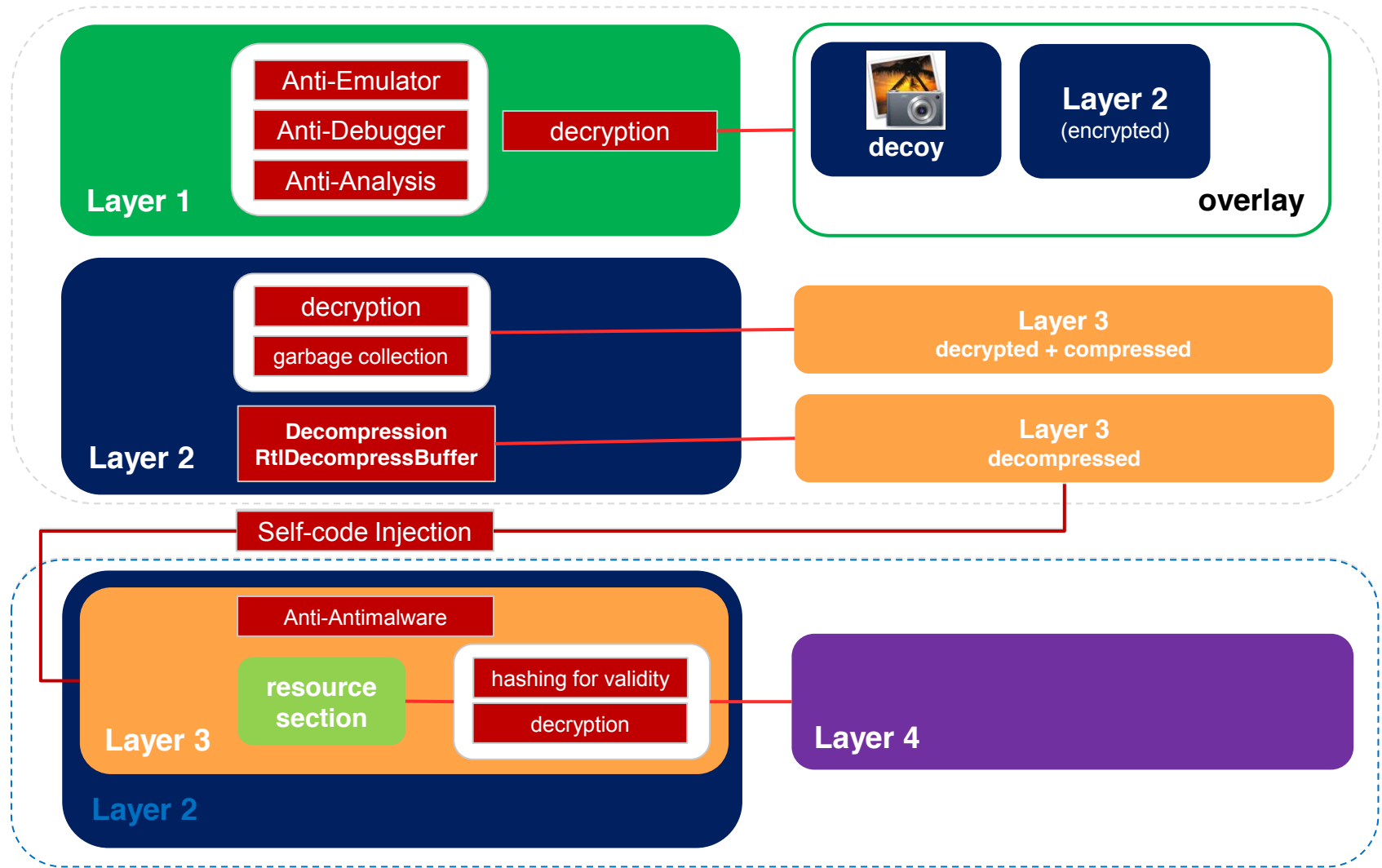


# Layer 2



<b>Encryption/ Decryption</b>	Decrypts the encrypted-compressed 3 <sup>rd</sup> layer Decryption algorithm is embedded with the garbage code
<b>Garbage Collection</b>	Contains instructions/code that is not relevant to the malware
<b>Compression/ Decompression</b>	Uses RtlDecompressBuffer API to decompress the 3 <sup>rd</sup> layer
<b>Self-Code Injection</b>	Injects the decompressed 3 <sup>rd</sup> layer at the location of the 2 <sup>nd</sup> layer

# Layer 3





# Layer 3



<b>Anti- antimalware</b>	Disables the installed antimalware/antivirus/security applications in the system
<b>Hashing</b>	Checks the hash of the encrypted layer 4
<b>Encryption/ Decryption</b>	Decrypts the 4 <sup>th</sup> layer 4 <sup>th</sup> layer is the payload executable

# DGA – Hiding is not enough





- DGA – Domain name Generation Algorithm
- Also called PrDGA (Pseudo-random DGA)
- Generates a binary seed
  - Can be a constant value
  - Can be generated from the current time and date
- Generates a string of random alpha-numeric characters
- Adds a variation of TLDs, such as com, org, info



- Normal Domains
  - yahoo.com
  - google.com
  - youtube.com
  
- DGA
  - zxrryy1223.ru
  - stslkflkjf.com
  - oiojlkmdlkjklj.org

# How DGA works



- Client-side and Server-side uses the same algorithm
- The server-side registers one or more generated domain names
- The client-side tries all possible combination of generated domain names
- The client-side establishes connection to the server-side
- The server-side un-registers the registered domain to avoid detection

C&C





- Not a fixed string

- Derived from a DWORD value

- Controlled by 40-byte XOR key

- Different variants, different domains

# Vawtrak's DGA



seed

```
MOV ESI,DWORD PTR SS:[EBP-0C]  
MOV EAX,DWORD PTR DS:[EDI+EBX+212]  
XOR EDI,EDI  
MOV DWORD PTR SS:[EBP-10],EAX  
LEA EAX,[EBP-10]  
PUSH EAX  
CALL byte_gen  
POP ECX  
MOV ECX,DWORD PTR DS:[16E2144]  
ADD ECX,EBX  
XOR AL,BYTE PTR DS:[EDI+ECX+216]  
MOV BYTE PTR DS:[ESI+EDI],AL  
INC EDI  
CMP EDI,40  
JB SHORT 016BD7FC
```

byte generator

```
PUSH EBP  
MOV EBP,ESP  
CMP DWORD PTR SS:[EBP+8],0  
JE SHORT 016C0D1D  
PUSH 4  
POP EAX  
IMUL EAX,EAX,0  
MOV ECX,DWORD PTR SS:[EBP+8]  
IMUL EAX,DWORD PTR DS:[EAX+ECX],343FD  
ADD EAX,269EC3  
PUSH 4  
POP ECX  
IMUL ECX,ECX,0  
MOV EDX,DWORD PTR SS:[EBP+8]  
MOV DWORD PTR DS:[ECX+EDX],EAX  
PUSH 4  
POP EAX  
IMUL EAX,EAX,0  
MOV ECX,DWORD PTR SS:[EBP+8]  
MOV EAX,DWORD PTR DS:[EAX+ECX]  
SHR EAX,10  
AND EAX,00007FFF  
JMP SHORT 016C0D51
```

alphanumeric generator



# Different variants, different domains



No.	Time	Source	Destination	Protocol	Info
41982	6		30	4.2	DNS Standard query A su... izehereclick.net
42009	8		30	4.2	DNS Standard query A go... neonthehere.org
42013	8		30	4.2	DNS Standard query A br... lowload23now1.su
43156	8		30	4.2	DNS Standard query A fa... eandlike.com
43184	1		30	4.2	DNS Standard query A ch... id-gde.su
43303	1		30	4.2	DNS Standard query A up... ndmegohits.ru
43386	1		30	4.2	DNS Standard query A su... izehereclick.net
43424	1		30	4.2	DNS Standard query A go... neonthehere.org
43428	1		30	4.2	DNS Standard query A br... lowload23now1.su
43435	2		30	4.2	DNS Standard query A fa... eandlike.com

sample #1

# Different variants, different domains



No.	Time	Source	Destination	Protocol	Info
465	7		40	04.2	DNS Standard query A wo... laref.ru
483	7		40	04.2	DNS Standard query A fy... nsed.ru
493	7		40	04.2	DNS Standard query A zdi... vuyfm.com
497	8		40	04.2	DNS Standard query A nav... y.com
504	8		40	04.2	DNS Standard query A der... y.com
562	9		40	04.2	DNS Standard query A un... rheg.ru
577	1		40	04.2	DNS Standard query A ro... asmuch.ru
581	1		40	04.2	DNS Standard query A ge... tantin.ru
585	1		40	04.2	DNS Standard query A wa... hep.ru
586	1		40	04.2	DNS Standard query A wa... hep.ru
587	1		40	04.2	DNS Standard query A wa... hep.ru
588	1		40	04.2	DNS Standard query A wa... hep.ru
590	1		40	04.2	DNS Standard query A wa... hep.ru

sample #2

# Different variants, different domains



No.	Source	Destination	Protocol	Info
66	50	4.2	DNS	standard query A ro talo.com
104	50	4.2	DNS	Standard query A be ek.net
148	50	4.2	DNS	Standard query A my rground.ru
152	50	4.2	DNS	Standard query A ma el.biz
166	50	4.2	DNS	Standard query A ab rozmaslalo.info
171	50	4.2	DNS	Standard query A go neonthehere.org
175	50	4.2	DNS	Standard query A wo fborjomi.net
180	50	4.2	DNS	Standard query A el golfclub.com
218	50	4.2	DNS	Standard query A ma e2016.com
232	50	4.2	DNS	Standard query A bi higherthanyou.com
246	50	4.2	DNS	Standard query A we thechampionsmyfrriends.com
275	50	4.2	DNS	Standard query A be ek.net
288	50	4.2	DNS	Standard query A ma el.biz
300	50	4.2	DNS	Standard query A ab rozmaslalo.info
305	50	4.2	DNS	Standard query A wo fborjomi.net

sample #3

# Different variants, different domains



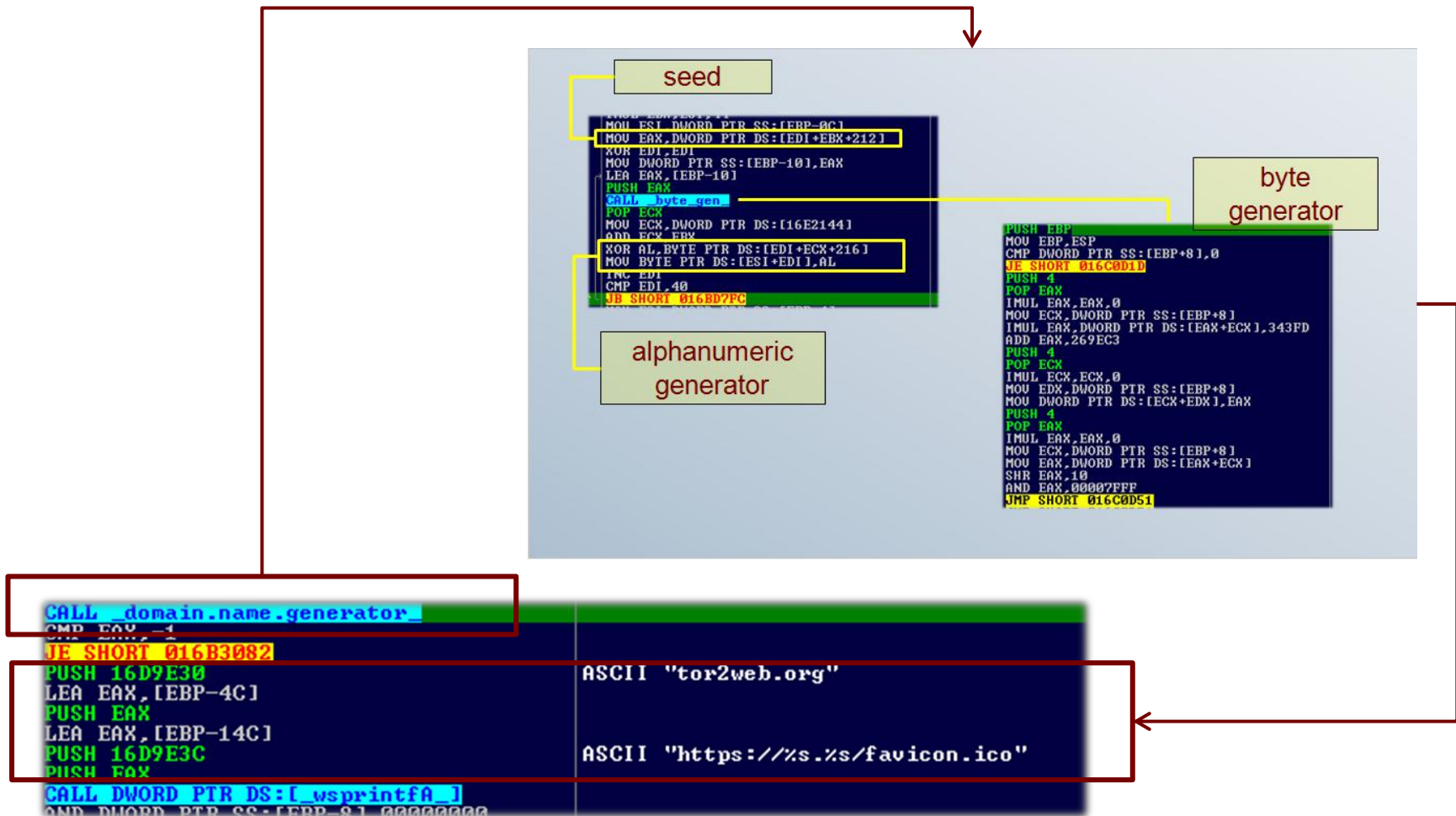
No.	Time	Source	Destination	Protocol	Info
42914	53		192.168.1.2	DNS	Standard query A w...ercrow.com
42929	53		192.168.1.2	DNS	Standard query A q...tenatel.com
42936	53		192.168.1.2	DNS	Standard query A m...erstargon.ru
42937	53		192.168.1.2	DNS	Standard query A m...erstargon.ru
42938	53		192.168.1.2	DNS	Standard query A m...erstargon.ru
42939	53		192.168.1.2	DNS	Standard query A m...erstargon.ru
42949	53		192.168.1.2	DNS	Standard query A l...rowler.ru
42950	53		192.168.1.2	DNS	Standard query A l...rowler.ru
42951	53		192.168.1.2	DNS	Standard query A l...rowler.ru
43153	63		192.168.1.2	DNS	Standard query A o...rda.ru
43197	63		192.168.1.2	DNS	Standard query A y...yalam.ru
43210	63		192.168.1.2	DNS	Standard query A a...to.ru
43217	63		192.168.1.2	DNS	Standard query A b...ime.ru
43227	63		192.168.1.2	DNS	Standard query A i...han.com
43261	63		192.168.1.2	DNS	Standard query A k...shi.com
43276	63		192.168.1.2	DNS	Standard query A u...tus.com
43298	63		192.168.1.2	DNS	Standard query A c...dhisjohn.com
43302	63		192.168.1.2	DNS	Standard query A i...entehed.com
43312	63		192.168.1.2	DNS	Standard query A r...eugrigh.com
43319	63		192.168.1.2	DNS	Standard query A o...rsforrep.com
43325	63		192.168.1.2	DNS	Standard query A s...ines.com
43327	63		192.168.1.2	DNS	Standard query A s...ines.com
43328	63		192.168.1.2	DNS	Standard query A s...ines.com
43341	63		192.168.1.2	DNS	Standard query A p...ndmaheg.ru
43348	63		192.168.1.2	DNS	Standard query A p...thec.ru
43358	64		192.168.1.2	DNS	Standard query A d...onrab.ru
43365	64		192.168.1.2	DNS	Standard query A m...bet.ru
43366	64		192.168.1.2	DNS	Standard query A m...bet.ru

sample #4

# Tor2Web C&C



# Vawtrak's DGA



# Tor2Web C&C



No.	Time	Source	Destination	Protocol	Info
121		40	4.2	DNS	Standard query A ot gxbcwvrs.tor2web.org
141		40	4.2	DNS	Standard query A 4b z4e7n6gnb.tor2web.org
161		40	4.2	DNS	Standard query A bc f4m3lnw4o.tor2web.org
245		40	4.2	DNS	Standard query A ot gxbcwvrs.tor2web.org
265		40	4.2	DNS	Standard query A 4b z4e7n6gnb.tor2web.org
285		40	4.2	DNS	Standard query A bc f4m3lnw4o.tor2web.org
370		40	4.2	DNS	Standard query A 4b z4e7n6gnb.tor2web.org
390		40	4.2	DNS	Standard query A bc f4m3lnw4o.tor2web.org
410		40	4.2	DNS	Standard query A ot gxbcwvrs.tor2web.org
599		40	4.2	DNS	Standard query A 4b z4e7n6gnb.tor2web.org
619		40	4.2	DNS	Standard query A bc f4m3lnw4o.tor2web.org
639		40	4.2	DNS	Standard query A ot gxbcwvrs.tor2web.org

sample #2



No.	Time	Source	Destination	Protocol	Info
46171	8	1	1	2	DNS Standard query A ots gxbcwvrgs.tor2web.org
46273	9	1	1	2	DNS Standard query A 4bp z4e7n6gnb.tor2web.org
46336	9	1	1	2	DNS Standard query A bc3 f4m31nw4o.tor2web.org

sample #4



Can Vawtrak really use DGA to create a randomized Tor C&Cs?

# How Tor Works



# How Tor Works

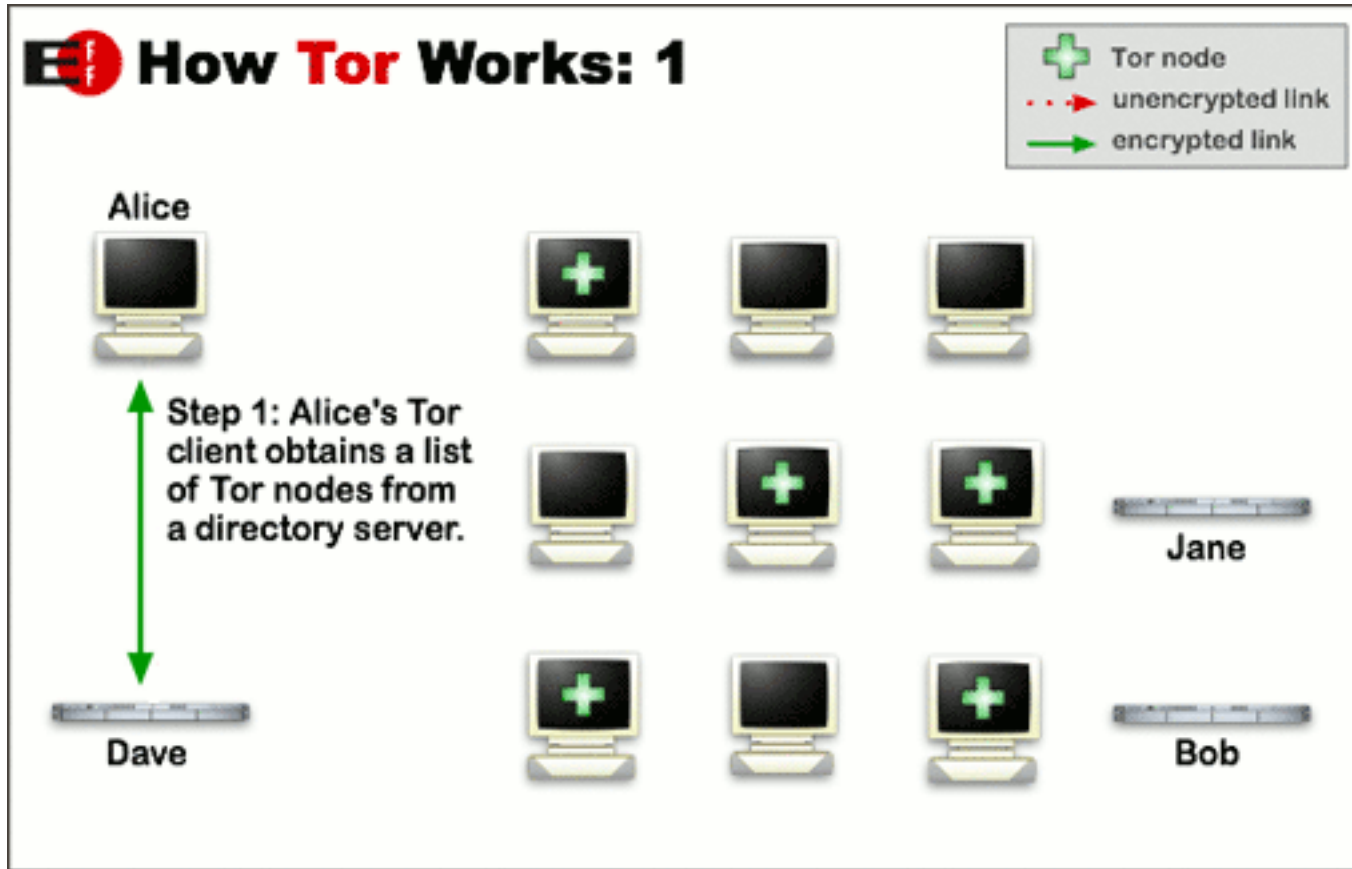


Image taken from torproject.org

# How Tor Works

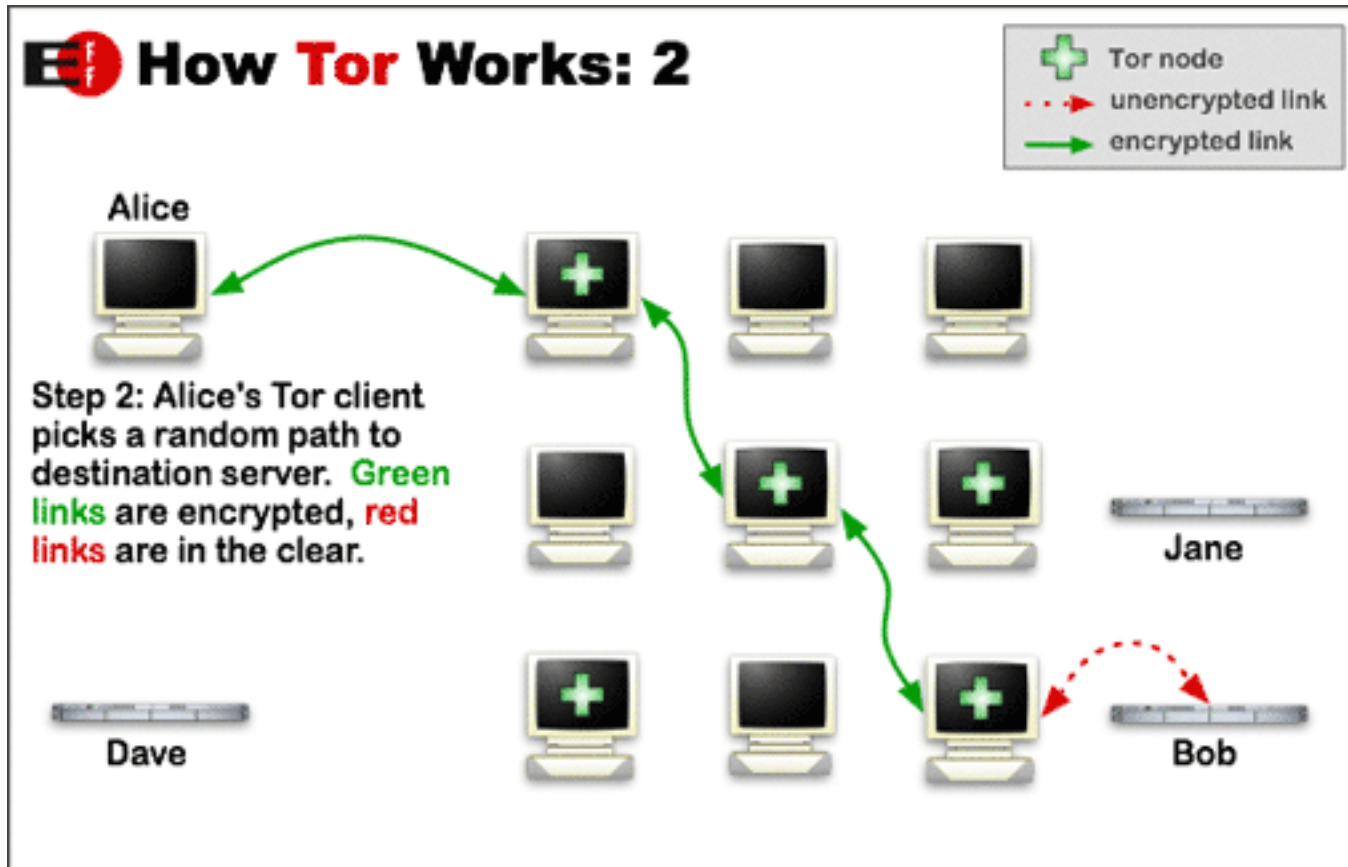


Image taken from torproject.org

# How Tor Works

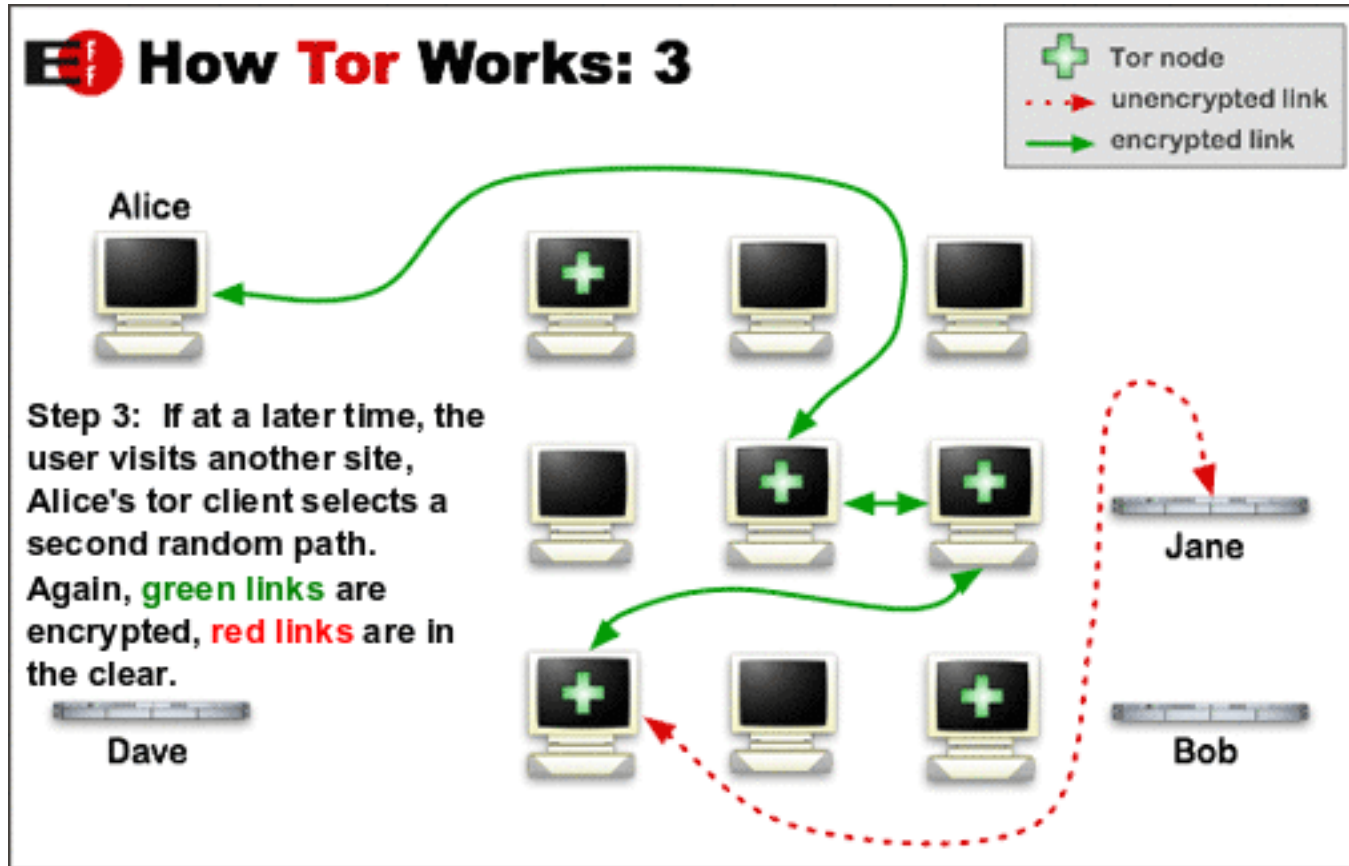


Image taken from torproject.org

# Tor and Hidden Services



# Hidden Service: **Deep Web Radio**

76q... gum7l.onion | D. deep web radio

## Deep Web Radio

Administration Server Status I2P (beta) AnonyPlayer Info

### Mount Point /AnonyJazz

M3U XSPF

Stream Title: /Anony (M3U)  
Stream Description: Anony Jazz (M3U)  
Content Type: audio/mpeg  
Bitrate: 320  
Current Listeners: 11  
Peak Listeners: 11  
Stream Genre: Jazz  
Stream URL: http://76q... gum7l.onion/AnonyJazz  
Current Song: Tony Martin - Don't Make Me Wanna Dance - [ItPepper-...]

# Hidden Service: **Electronic Store**

Browser address bar: y6.onion/index.php

Navigation: PRODUCTS, ABOUT, INFO, CONTACT

## BEST DEEPWEB ELECTRONICS STORE

BRAND NEW ELECTRONICS FOR GOOD PRICES

APPLE		
APPLE IPHONE 6 PLUS 16GB	₿1.35	ORDER
APPLE IPHONE 6 16GB	₿1.15	ORDER
APPLE IPHONE 5S 16GB	₿0.99	ORDER
APPLE IPAD AIR 2 64GB 4G	₿1.38	ORDER
APPLE IPAD MINI 3 64GB 4G	₿1.23	ORDER
APPLE MACBOOK AIR 13" 128GB	₿1.65	ORDER

SAMSUNG		
SAMSUNG GALAXY NOTE EDGE 32GB 4G	₿1.21	ORDER
SAMSUNG GALAXY NOTE 4 N910 32GB 4G	₿0.95	ORDER
SAMSUNG GALAXY S5 32GB	₿0.9	ORDER
SAMSUNG GALAXY NOTE 3 N9005 4G	₿0.78	ORDER
SAMSUNG GALAXY S5 G900FD DUAL SIM	₿0.86	ORDER
GOOGLE NEXUS 10 32GB	₿0.67	ORDER





# Hidden Service: Free Email



The screenshot shows a web browser window with the address bar containing 'sig[redacted]vw.onion'. The website has a black background with a red and blue logo of a stylized eye with red liquid dripping from it. A navigation menu includes buttons for 'home', 'login', 'signup', 'faq', 'upgrade', and 'contact us'. The main content area is a grey box with the following text:

Welcome to [redacted]

What is [redacted] [redacted] is a darknet email service that allows you to send and receive email without revealing your location or identity. We provide this service to help journalists and activists combat the dragnet surveillance that exists on the Internet today. Even if you aren't in conflict with the state or anyone in particular you as a human being deserve privacy.

Why should you trust us? You don't have to trust us, in fact we recommend you don't! When you send email using our webportal we recommend you encrypt your messages using PGP.

Are there any rules to using this thing? Generally we are pretty chill, all we ask is that you don't use our FREE service to:

- Spam people
- Threaten people
- Harm people

Everything else is cool with us.

**SIGN UP**

\*\*\*\* Over 64,000 served and even faster storage! \*\*\*\*

# Hidden Service: File Storage



torsafe[REDACTED].onion/accounts/login/

Log In Sign Up

My Home Groups Shares Contacts

## Welcome to TorSafe !

TorSafe is able to host your files online in a secure way:

- File Sharing** you can organize your files in library and share them between users and group of users
- Anonymous** we use the tor network, we are compatible with TorBrowser and are compliant with the best practices of Tor
- Secure** strong encryption (AES256) is used to encrypt your files, only the owner of the key (password) can read the files, even not through the network
- Collaboration** exchange messages, files, discussions, conversations in a collaborative way with the other members
- Wiki** create your own wiki page in a WYSIWYG editor. You can keep personal notes or share pages
- Versioning of your files** you can keep multiple of versions of your files and come back to a previous versions in case of disaster

**Log In**

Email

Password

**Signup**  
Free ! No engagement

torsafe[REDACTED].onion/accounts/login/

### Pricing Plan

	Copper	Bronze	Silver	Gold	Platinum
<b>Pro Hosting in datacenter</b>	Yes	Yes	Yes	Yes	Yes
<b>Storage</b>	10MB	1GB	5GB	125GB	For large organizations that need a dedicated infrastructure. Contact us - service on demand
<b>Number of users</b>	1	1	5	50	
<b>Number of groups</b>	Unlimited	Unlimited	Unlimited	Unlimited	
<b>Monthly bandwidth</b>	1GB/month	10GB/month	Unlimited	Unlimited	
<b>Internal Backup (of encrypted data)</b>	No	No	Yes	Yes	
<b>Activation fee</b>	No	No	No	No	
<b>Price</b>	Free	Free for early adopters !	25€/month 33\$/month equivalent in bc	100€/month 137\$/month equivalent in bc	
<b>Comment</b>	Limited account, intended for test purpose	For independant ! Signup now it's free for early adopters !	For a small team	For a medium team	

We accept bitcoins [ 1PPJWAKJ[REDACTED]bdTQ3Xg ] ! Contact torsafe@bitmessage.ch for an order or for any questions

### Our key points

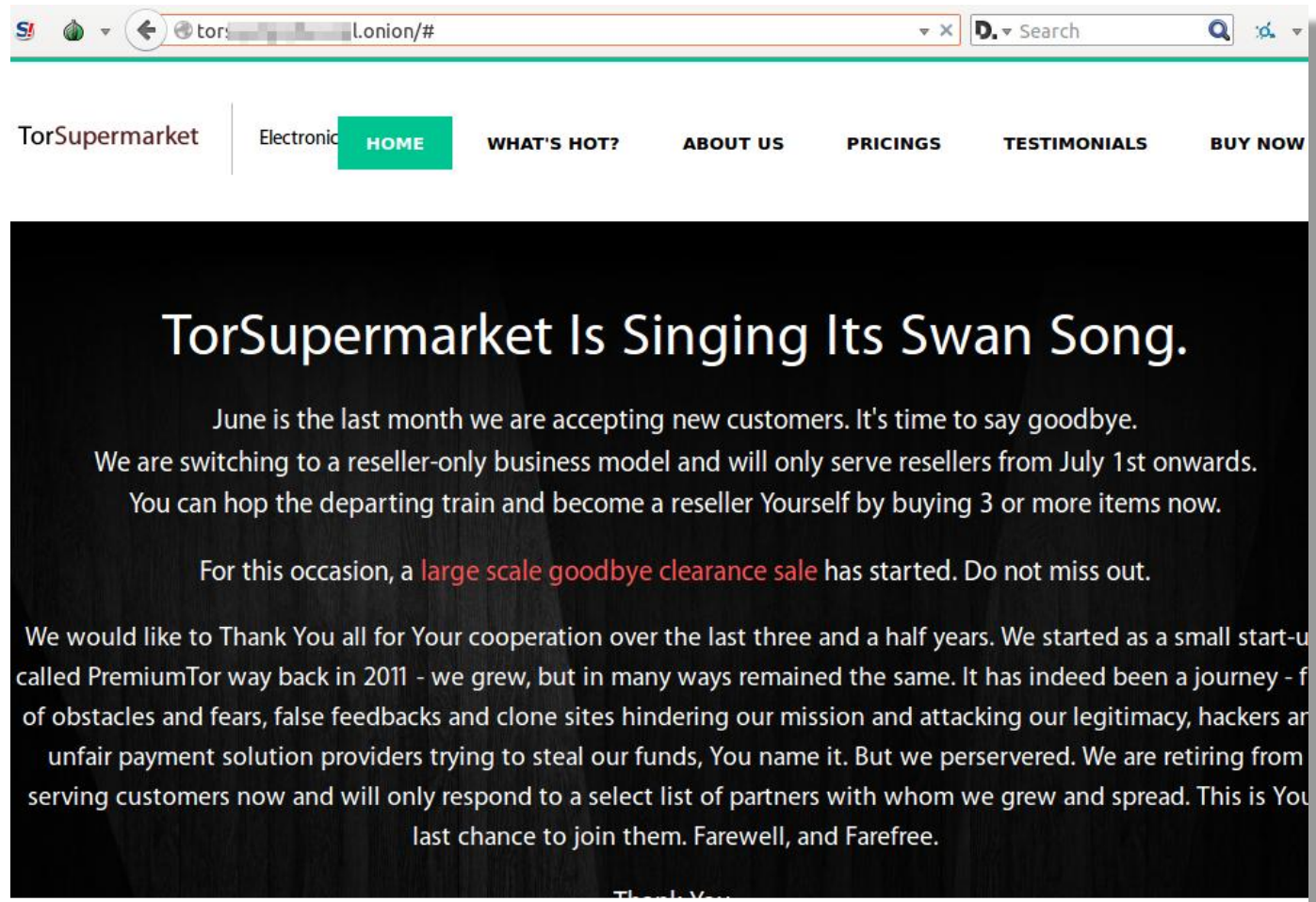
**ANONYMOUS**

is compliant with the Tor guidelines: Source: <https://www.torproject.org/download/download#warning>

use the Tor Browser™ You can use the Tor Browser to surf on TorSafe. Tor Browser is a customized version to protect your privacy and your anonymity

don't enable or install browser plugins™ You don't need any plugins that can break your anonymity such as Flash, RealPlayer, Quicktime

# Hidden Service: Tor Supermarket



The screenshot shows a web browser window with the address bar containing a Tor hidden service URL. The website header includes the name 'TorSupermarket' and a navigation menu with items like 'Electronic', 'HOME', 'WHAT'S HOT?', 'ABOUT US', 'PRICINGS', 'TESTIMONIALS', and 'BUY NOW'. The main content area features a large black background with white text announcing the site's closure.

## TorSupermarket Is Singing Its Swan Song.

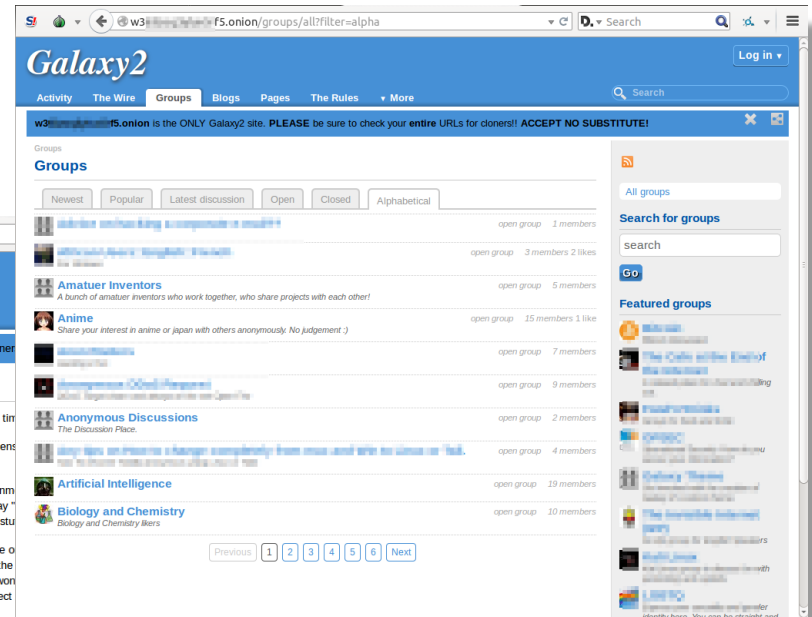
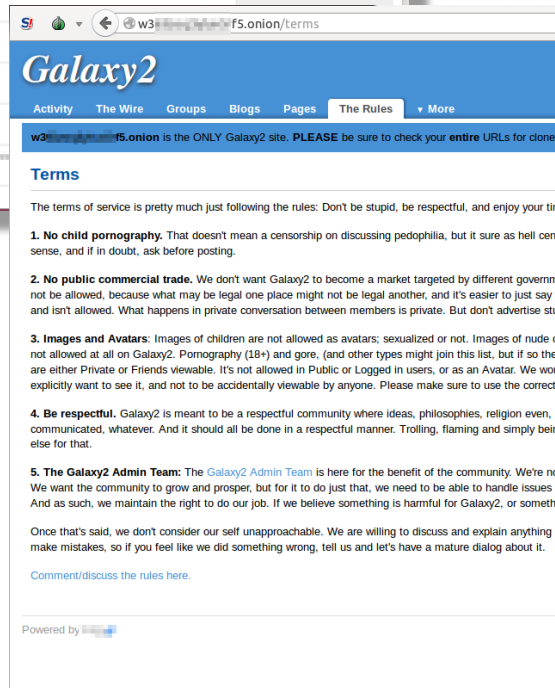
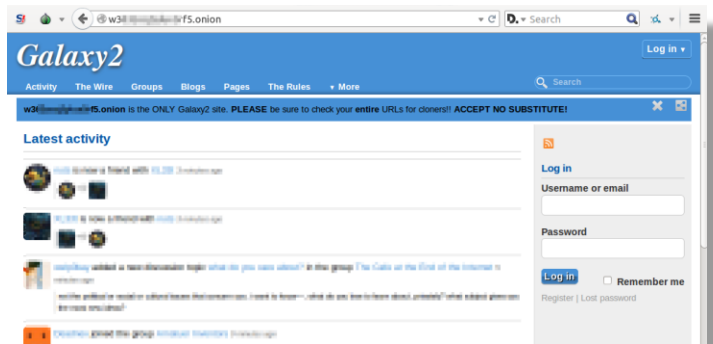
June is the last month we are accepting new customers. It's time to say goodbye. We are switching to a reseller-only business model and will only serve resellers from July 1st onwards. You can hop the departing train and become a reseller Yourself by buying 3 or more items now.

For this occasion, a **large scale goodbye clearance sale** has started. Do not miss out.

We would like to Thank You all for Your cooperation over the last three and a half years. We started as a small start-up called PremiumTor way back in 2011 - we grew, but in many ways remained the same. It has indeed been a journey - full of obstacles and fears, false feedbacks and clone sites hindering our mission and attacking our legitimacy, hackers and unfair payment solution providers trying to steal our funds, You name it. But we persevered. We are retiring from serving customers now and will only respond to a select list of partners with whom we grew and spread. This is Your last chance to join them. Farewell, and Farefree.

Thank You

# Hidden Service: Chat Rooms



# Hidden Service: The Hidden Wiki



The screenshot shows a web browser window displaying the main page of 'The Hidden Wiki'. The browser's address bar shows the URL 'zq[redacted]6ri.onion/wiki/index.php/Main\_Page'. The page features a navigation menu with links for 'page', 'discussion', 'view source', and 'history'. The main content area is titled 'Main Page' and includes a welcome message, 'Editor's picks' (a list of four articles), 'Volunteer' (a list of five tasks), and 'Introduction Points' (a list of various hidden services and their descriptions). The left sidebar contains sections for 'navigation', 'search', and 'tools'.

**The Hidden Wiki**

navigation

- Main page
- Recent changes
- Random page
- Rules of the site

search

Search

Go Search

tools

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

**Main Page**

Welcome to **The Hidden Wiki** New hidden wiki url 2015 [http://zq\[redacted\]6ri.onion](http://zq[redacted]6ri.onion) Add it to bookmarks and spread it!!!

**Editor's picks**

Bored? Pick a random page from the article index and replace one of these slots with it.

1. [The Matrix](#) - Very nice to read.
2. [How to Exit the Matrix](#) - Learn how to Protect yourself and your rights, online and off.
3. [Verifying PGP signatures](#) - A short and simple how-to guide.
4. [In Praise Of Hawala](#) - Anonymous informal value transfer system.

**Volunteer**

Here are five different things that you can help us out with.

1. Plunder other hidden service lists for links and place them here!
2. File the [SnapBBSIndex](#) links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
4. Care to start recording onionland's history? Check out [Onionland's Museum](#)
5. Perform Dead Services Duties.

**Introduction Points**

- [Alotus 1.0](#) - Open source search engine for Tor Hidden Services (allows you to add new sites to its database).
- [Clearnet Search](#) - A hidden Service that searches the clearnet.
- [Clearnet Index](#) - Open source anonymization taken seriously.
- [Hidden Wiki](#) - Tor Service Engine. Claims to index around 1.1 Million pages.
- [Hidden Wiki](#) - Directory for onion sites, moderated.
- [Clearnet](#) - Search (Hidden) Markets and more.
- [Hidden Wiki](#) - The hidden Wiki more orderly and updated!
- [Hidden Wiki](#) - A mirror of the Hidden Wiki. 2 days old users can edit the main page.
- [Hidden Wiki](#) - A hidden engine which only indexes hidden services on Tor.
- [Hidden Wiki](#) - Spider robot finding known .Onion sites. It does not list onions which are down.
- [Hidden Wiki](#) - A community editable wiki that welcomes all users. Allows a variety of uses. Now recruiting Admins. **[Down 2015/6]**



## And so much more ...



- Email/Messaging
- Books
- Financial
- Audio/Music
- Domain/Hosting
- Security
- Blogs
- Social networks
- Forums
- And so much more ...

# Creating Your Own Tor hidden Service





Warning!



WeKnowMemes

<http://weknowmemes.com/wp-content/uploads/2011/12/dont-try-what-youre-about-to-see-at-home-mythbusters.jpg>

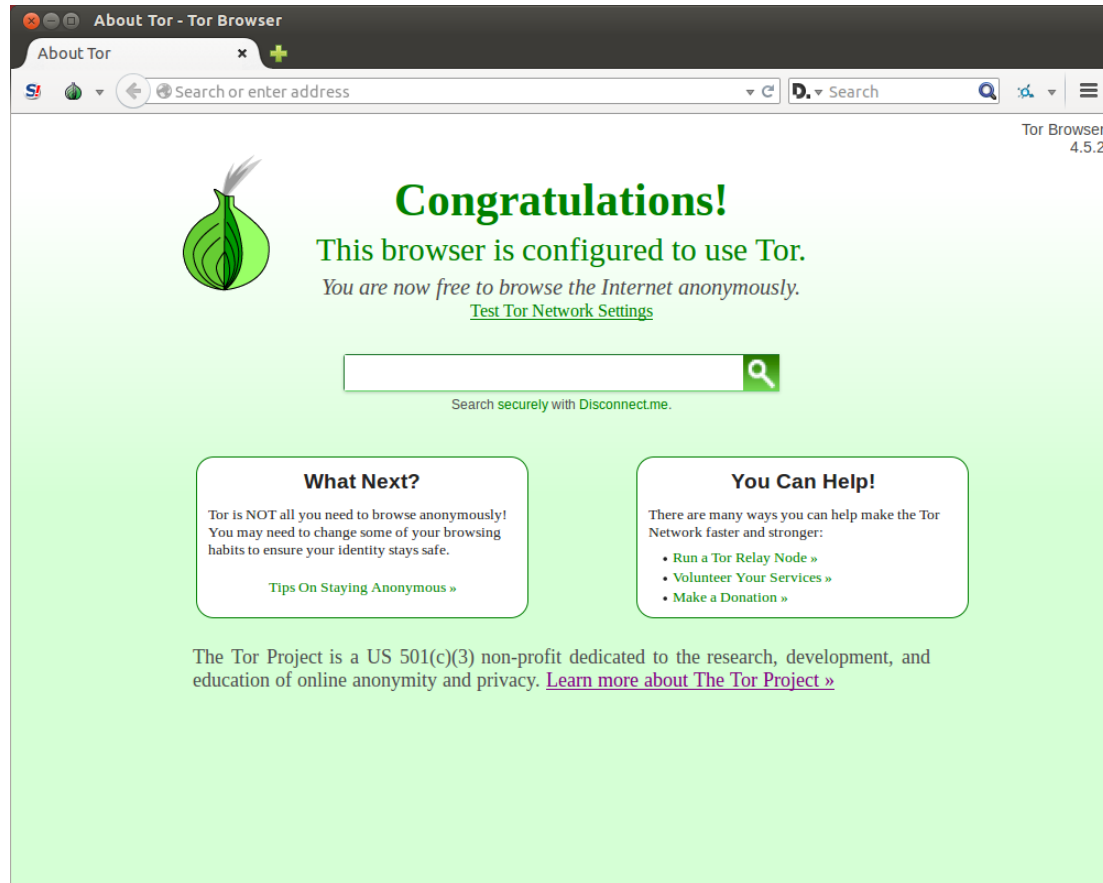
# Tor Setup

- Download Tor from the official website





## ➤ Tor browser



# Hidden Service



- Install Apache HTTP Server
- Create a simple html file

# .onion Address



- .onion is a Pseudo-TLD(top level domain)
- 16-character hashes
- consisting of letters and numbers



# Personalized .onion address



## ➤ Install Shallot

The image displays two overlapping browser windows. The background window shows the GitHub repository page for 'katmagic / Shallot'. The repository description states: 'Shallot allows you to create customized .onion addresses for your hidden service. (p.s. I didn't write Shallot)'. It lists 31 commits, 1 branch, 5 releases, and 2 contributors. The file list includes 'src', '.gitignore', 'CHANGELOG', 'LICENSE', 'Makefile', 'README.asciidoc', and 'configure'. The foreground window shows the README content for 'Shallot'. It includes an 'About' section, an 'Installation' section with terminal commands, and a 'Usage' section with a terminal example.

**Shallot**

Shallot allows you to create customized .onion addresses for [Tor's hidden services](#). (By customized, it is meant that part of the address can be selected. Choosing an entire address would take far longer than the universe is believed to have been in existence.)

**Installation**

```
$ ./configure && make
$ ./shallot
```

**Usage**

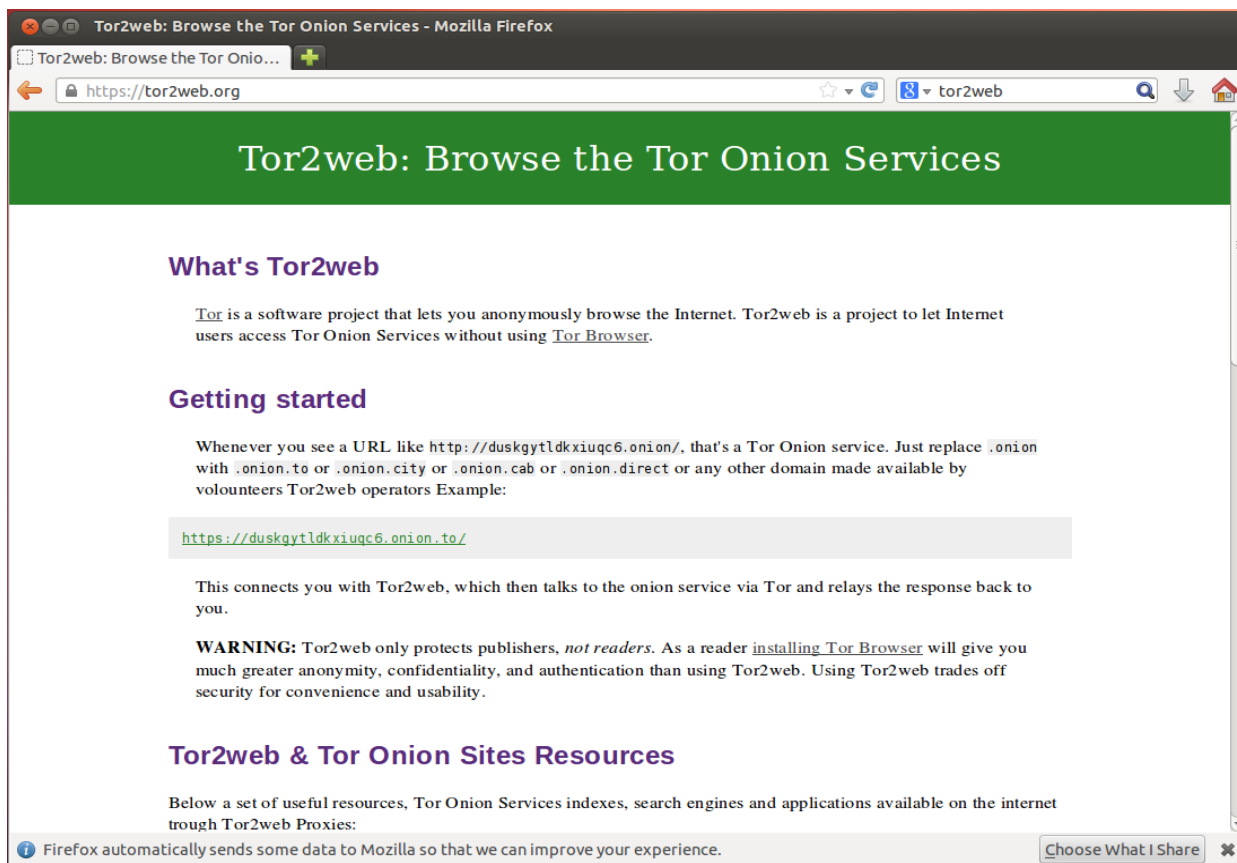
```
$ ./shallot ^test
-----
Found matching pattern after 99133 tries: testvztz3tfoiofv.onion
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAQgQC3R85mNqA1ZjaYqz1hvFIjbl4RtKdJbG8h1C9xEBkvfr/BG
8Z5vD1UzdbDtmEBuZUDanx80uGJvbXTgmczX0U1kE0g6LZ8RKpnsbKaF/EJN+Iw
T7MSXQmNcm22DeV1V7fwy+Usya12REScdVCFsPlEbVzqCum1KkEgCyFwIDBAZ7
AoGBAJSa2cGuru/XhZ3AEAIwHZdgP0num9T/srOYxUKW6afHZE0u5S4C1wb+xb/
pG0Tzn1XZfCKMf1Vdxb/f3XTCrRyB2VnBoNT0T7WfH6DksdDF4zunq1EJv19K
R+tkXmF70edrRt6wIHUmFd1E2Q9nbTHI61cdB4kR4QkYKZZAkEASM6samK7+495
```

# Tor2Web





- Browsing hidden services via a normal web browser







## ➤ Header page



**onion.to does not host this content;** we are simply a conduit connecting Internet users to content hosted inside [the Tor network](#).  
**onion.to does not provide any anonymity.** You are strongly advised to [download the Tor Browser Bundle](#) and access this content over Tor.

For more information see [our website for more details](#) and send us your [feedback](#).

[hide Tor2web header](#)

Can Vawtrak really use DGA to create a randomized Tor C&Cs?



- Pre-set .onion domains

- Pseudorandom DGA will not work

- Tor2Web C&C not so random

# Tor2Web C&C



No.	Time	Source	Destination	Protocol	Info
121		40	4.2	DNS	Standard query A ot gxbcwvrs.tor2web.org
141		40	4.2	DNS	Standard query A 4b z4e7n6gnb.tor2web.org
161		40	4.2	DNS	Standard query A bc f4m31nw4o.tor2web.org
245		40	4.2	DNS	Standard query A ot gxbcwvrs.tor2web.org
265		40	4.2	DNS	Standard query A 4b z4e7n6gnb.tor2web.org
285		40	4.2	DNS	Standard query A bc f4m31nw4o.tor2web.org
370		40	4.2	DNS	Standard query A 4b z4e7n6gnb.tor2web.org
390		40	4.2	DNS	Standard query A bc f4m31nw4o.tor2web.org
410		40	4.2	DNS	Standard query A ot gxbcwvrs.tor2web.org
599		40	4.2	DNS	Standard query A 4b z4e7n6gnb.tor2web.org
619		40	4.2	DNS	Standard query A bc f4m31nw4o.tor2web.org
639		40	4.2	DNS	Standard query A ot gxbcwvrs.tor2web.org

sample #2

# Tor2Web C&C



otsxxxxgxbcwvrrqs

4bpxxxxz4e7n6gnb

bc3xxxxf4m3lnw4o

Dump - 016B0000..0172DFFF

Address	Hex dump	ASCII
016E2A96	96 5B 10 57 28 F8 5E C9 3E 80 88 C3 7B E0 6F 81	û W<^°r>ÇêKαoü
016E2AA6	81 04 FB FF B8 A1 2A 61 7C 58 E9 B8 FC 8C 78 CF	ü♦J q í*a!X0j"îx±
016E2AB6	A6 F8 32 E5 D4 63 53 9B AD 25 64 9E 3E E8 FA 85	≈02σ lcSçizdR>è-à
016E2AC6	CD AC A0 FD 69 0E 12 23 C6 C9 AC 31 48 7D 21 5D	=%á² iJ#Hr%1H>!J
016E2AD6	5E AF 70 FE 35 4A F4 5C BD 3B 39 BC 99 88 89 05	^>>#5Jr\µ;9#0êèè
016E2AE6	F5 F9 91 3C F6 1F DC 0A DE 69 37 7B 12 D8 D7 15	J·æ<÷▼_0 li7<† IS
016E2AF6	18 8C AA 14 F8 98 C4 4A 09 83 E2 8F 99 F9 51 11	†î-9!oy-JoârRü-Q<
016E2B06	EA C1 0B EC 7A EF 24 FB 87 5B 64 ED D3 51 36 9B	Ω-8°ozñ\$Jc [dø"Q6ç
016E2B16	A5 8A C0 98 10 5B 54 0A 88 12 D3 13 12 98 41 A3	ñè-ÿ T 0è+!!!yáü
016E2B26	3A 51 CE A9 47 4A 74 96 F4 81 FC 77 48 45 B8 66	:Q!r-GJtû ñi"whE7f
016E2B36	FB 4F 49 E6 1E 3E B7 2A EB 4F 5E EB C5 AA D4 3A	J0Iµ&>π*60^δ†=:
016E2B46	08 89 78 C5 40 9C 4E 56 99 AD 0A 9C 97 80 6A 2E	Çex+0ENU0;0Eüçj.
016E2B56	07 ED C9 CD 36 90 E2 F9 60 D1 32 62 00 00 00 00	•²r-6É²θ`τ2g
016E2B66	01 00 01 00 20 20 00 00 01 00 20 00 A8 10 00 00	⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙ ⊙

No.	Time	Source	Destination	Protocol	Info
46171	8		1 1	2	DNS Standard query A otsxxxxgxbcwvrrqs.tor2web.org
46273	9		1 1	2	DNS Standard query A 4bpxxxxz4e7n6gnb.tor2web.org
46336	9		1 1	2	DNS Standard query A bc3xxxxf4m3lnw4o.tor2web.org

sample #4

**F** **RTINET**®