Measuring popularity of darknet sites

 $\label{lem:degree} \textit{Degree programme: BSc in Computer Science} \mid \textit{Specialisation: IT Security}$

Thesis advisor: Prof. Dr. Emmanuel Benoist

Expert: Dr. Igor Metz (GLUE Software Engineering AG)

The Tor network is used to hide trafic to website. Moreover websites are hidden within the Tor network. We call them hidden services. Our goal is to find the most visited hidden services over a two-month period. To achieve this, we create an infrastructure of six hidden service directories in the Tor network. These servers receive encrypted requests from Tor users that we decrypt. Thereby, we know which hidden services are visited and by how many clients.

Introduction:

There are tens of thousands of sites on the darknet. In the Tor network, these sites are called hidden services. Tor encrypts traffic and makes users anonymous by changing their IP addresses. As a result, the main sites are drug markets, forums and images hosting services. Our goal is to collect clients encrypted requests and compile a list of the most visited hidden services.

Concept:

When a client wants to contact a hidden service, they only need to type the onion address of this site. The encrypted request reaches a server called Hidden Service Directory (HSDir), which transfers a descriptor to the client. This descriptor is also encrypted and contains all the information to contact the requested hidden service. The idea was to create some HSDir on the Tor network to host information from hidden services. On average, an HSDir contains about 1300 descriptors. A hidden service is randomly assigned to a limited number of HSDir. This relationship changes over time. So, when a client requests access to a site

to which our servers are assigned, we pass on the descriptor in question. Thus, the HSDir can log that request. Then we decrypt the descriptor and store the name of the hidden service in a database. Finally, we aggregate all our data for the final statistics.

Architecture:

To achieve our goal, we have divided it into several steps:

- Adapt a crawler to get a maximum of sites URL on the darknet
- Modify Tor's source code to retrieve encrypted data that says customers visited sites
- Decrypt this data with the list of recovered sites (dictionary attack)
- Store the results in a database

Results:

In the final list of the most visited sites from April to May, the first two are drug markets, the others are mainly forums and image hosting sites. This list is not



Liviu Grozea
liviu.grozea15@gmail.com



Arthur Louis Simonin arthur.simonin@gmail.com

Site	Requests	
BlackSprut	381'022	
Tor2Door	148'782	
Mega Market	99'356	
HDDoro	20'441	
Amorzinho	14'285	
Easy Image Upload	10'498	
Brave	10'330	
imghost	9220	
Darkhost	6392	
The Resistance	5980	
TorDex	4546	
The Pirate Bay	4079	



mike@zanella.io

2dcor Market	Become a Orders Vendor	Help ▼ Messages ▼ Wallet	• 🛕 🦲 MODS2022
Categories	Q Quick Search		₩ MY CART
Fraud 1501			
Drugs & Chemics 8 67	We currently offer vendor bond	waiver to all established vendors, A	pply here.
Digital Products 2931	Featured Products		
Counterfeit Items 108			
Jewels & Gold 11			
Services 92	1 177	ATTENDED TO	
02		AVABORATE	
Software & Hosting 68			
Others 217	Xanax Bars Sample	1g Cocaine WASHE	Black Tar Heroin, pu.
	\$35	\$132.22	\$44.13
	* * * * (0 reviews)	* * * * * (0 reviews)	* * * * * (1 review)
Exchange Rates	Seller:	Seller: CokeMano	Seller:
BTC XMR	GulfCoastPharma		GermanDrugScout
USD \$44,793.22			
EUR €40,598.15			
GBP £33,875.32	· 2000年	The same of the sa	
CADCA\$56,099.02			1 1
AUD AU\$59,535.2	Same Carrier		~ N
 JPY JP¥5,437,054 	STEAR F	the state of	
CNY ¥284,724		and the second second	
XAR R648,941	6IX6INE 320mg - ora \$3.75	UK IMPORT SCORPI	14g Half - Crystal Cl. \$200
C TRY \$664,381	\$3.75 (0 reviews)	\$0 * * * * * (0 reviews)	\$200 * * * * * (1 review)
DUDD4554.004	= = = = (0 reviews)	= = = = (0 reviews)	RRR RR R (I revi