Illuminating the Deep Dark Web with drugs, exploits, and zero-days

CLE-R09

Jack Chan

Security Strategist
FortiGuard Advanced Labs, Fortinet
@FortiGuardLabs
WARNING

- Presentation contains real world attacker methods and demos
- Some material is not suitable to all audiences
- Use common sense and ethical guidelines
- Don’t be Homer Simpson
Who are we...

Aamir Lakhani
Researcher / Consultant
Ninja / Pirate / Hacker

Jack Chan
Security Strategist, consultant

Time Magazine’s Person of the Year 2006...
And so were...
“There are only two types of companies: those that have been hacked, and those that will be.”

Robert Mueller
FBI Director, 2012
Fortinet Advantage – FortiGuard Labs Threat Research

**The FortiGuard Minute**

**Per Minute**
- 25,000 Spam emails intercepted
- 390,000 Network Intrusion Attempts resisted
- 83,000 Malware programs neutralized
- 160,000 Malicious Website accesses blocked
- 59,000 Botnet C&C attempts thwarted
- 39 million Website categorization requests

**Per Week**
- 47 million New & updated spam rules
- 100 Intrusion prevention rules
- 2 million New & updated AV definitions
- 1.3 million New URL ratings
- 8,000 Hours of threat research globally

**Total Database**
- 170 Terabytes of threat samples
- 17,500 Intrusion Prevention rules
- 5,800 Application Control rules
- 250 million Rated websites in 78 categories
- 173 Zero-day threats discovered

Based on Q1 2015 data
Image: threatmap.FortiGuard.com
Deep Web

Invisible web

Hidden web
Dr. Jill Ellsworth used the term *Invisible Web* in 1994.

The first use of the specific term *Deep Web* occurred in Michael Bergman study in 2001.
The anonymous Internet

Daily Tor users per 100,000 Internet users

- > 200
- 100 - 200
- 50 - 100
- 25 - 50
- 10 - 25
- 5 - 10
- < 5
- no information

Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal metrics.torproject.org
World Bank data.worldbank.org

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.ox.ac.uk

Oxford Internet Institute
University of Oxford
How Tor Works

Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Source: TOR Project
.Onion

- Works like a top-level domain
- Tor Hidden Services
- Can be hosted or Peer-to-Peer
- Can be found by search engines only if they want to be
- Must be on the TOR network or use a Web-to-TOR proxy to access
- Looks like this: http://3g2upl4pq6kufc4m.onion/ - DuckDuckGo Search
- Used for legitimate sites like Facebook and human right groups
- Used for illegal services and forums for illegal activity
- We are starting to see .onion sites with SSL – but that may actually reduce anonymity
The Deep Web

• 1000X larger?

• 7Tb observed

• More than just WWW services

• Different levels of Deep Web
Why Search Engines Can’t find them

- Private web
- Unlinked content
- Dynamic content
- Limited-access content
- Non-HTML content
- Hidden source code
Playing the Levels

• Level 0: Common Web

• Level 1: Surface Web
  • Reddit
  • Digg
  • Temp Email Services

• Level 2: Bergie Web
  • Google locked results
  • Honeypots
  • 4Chan, Newsgroups, FTP, other services
  • Freehive, Bunny Tube, Streams

• Level 4: Charter Web
  • Hacking Groups
  • Shelling Networking
  • AI Theorist
  • Banned media
  • Activist communications

• Level 5:
  • Onion Sites
  • Illegal Material
  • Human Trafficking, Bounty Hunters, Rare Animal Trade
  • Exploits, Black Markets, Drugs
Deep Web Level 8

- What happened to levels 6 – 7?

I entered the 8th Level of the Deep Web and met the Archons, ask me a question

Believe it or not but I managed to enter the 8th level of the Deep Web.

How am I still alive? Well, they said they won't touch me or my family and subsequent generations because of my accomplishment.

You do not need superior hacking skills to enter the 8th Level that is... I can tell you.

- Made up, BS, Fake?
What is the Tor Browser?

The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

The Tor Browser lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained.

Do you like what we do? Please consider making a donation »
Tor Hidden Wiki – The First Place You will go to feel Dark

• Collection of hidden links and .onion sites
• How hard is it to find?
Black Markets on the Dark Web
They change .onion addresses often
Sometimes invite only
Example: Silk Roads
Nov. 6th 2013 Silk Roads shutdown
Nov. 13th 2013 Silk Road 2.0
Nov 6th 2014 Silk Roads 2.0 shutdown
Nov 14th 2014 Pablo Escobar posted Silk Roads 3.0 is coming
Feb 4th 2015 Ross Ulbricht convicted on charges
Buy malware, exploits, social engineering expertise
Social Security numbers, national identification cards
Scammers, con artists, organized crime, drugs, guns
Mind-reeling amount of information
Powerful
Secure
Free of surveillance
You can get anything
Louis Vuitton Eva Clutch

0.15633956 BTC

This stylish Louis Vuitton Eva Clutch comes with a golden chain wrist strap and a leather cross shoulder strap.

The real ones go for $775. You can own this identical version for just $60.

Brought to you by: MagicHat [4.82/5, 300–500 deals]

From: USA
To: Worldwide

0.15633956 BTC

Feedbacks:
5/5  Terrific Vendor. Awesome product! Can't wait to order more :) Thanks MagicHat!

38 days ago  anon [~5/5, 6–10 deals]

5/5  84 days ago  anon [~5/5, 10–15 deals]

5/5  Looks just as good as my real LV. Great product...looking for more LV

122 days ago  anon [~2/5, 3–5 deals]
Crime is Thriving

THE PEOPLES DRUG STORE pride ourselves on offering the best quality products at competitive prices and making every effort to go above and beyond when it comes to customer satisfaction!

Choose a category by clicking on any of the following:

Heroin, Cocaine, Ecstasy, Speed, Cannabis Prescriptions, Bitcoins and Services

WANNA MAKE SOME FREE BTC??

Tell others about this shop, and earn 5% from every purchase they will make. Simply give them the following link: http://www.peoplesdrugstore.org/?ref=YOURUSERNAME (or the original http://newpdsusimzqazv.onion/?ref=YOURUSERNAME)
Replace YOURUSERNAME with your actual username on this site and get earnings directly to your wallet.
The Real Secret of PayPal
## Cyber Crime Sales

**ccPal Store - PayPals, CCs, CVV2s, Ebay accounts**

We get new lists every day!  
80%+ working guarantee, we will replace if more than 20% don't work!

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 PayPal accounts</td>
<td>100 USD = 0.260 $</td>
<td>1 X</td>
</tr>
<tr>
<td>Buy now</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100 Ebay accounts</td>
<td>100 USD = 0.260 $</td>
<td>1 X</td>
</tr>
<tr>
<td>Buy now</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100 CCs with CVV2</td>
<td>150 USD = 0.390 $</td>
<td>1 X</td>
</tr>
<tr>
<td>Buy now</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Welcome to Fake Documents Service - the unique producer of quality fake documents. We offer only original high-quality fake passports, driver's licenses, ID cards, stamps and other products for following countries: Australia, Belgium, Brazil, Canada, Finland, France, Germany, Italy, Netherlands, UK, USA and some others.

If you want to learn more about what kinds of documents can be found in our website please visit the sections "Services" and "Samples". You can find more details about ordering procedure and additional details visiting the sections "FAQ" and "Order".
Our notes are produced of cotton based paper. They pass the pen test without problems. UVI is incorporated, so they pass the UV test as well. They have all necessary security features to be spent at most retailers. Free shipping in the US.

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 x 50 USD BILLS</td>
<td>600 USD = 1.343 $</td>
<td>1</td>
<td>Buy now</td>
</tr>
<tr>
<td>100 x 50 USD BILLS</td>
<td>2000 USD = 4.475 $</td>
<td>1</td>
<td>Buy now</td>
</tr>
</tbody>
</table>
Click here to view Kim's Credit Report

Kimberly Noel Kardashian
SSN: [REDACTED]
DOB: 10/21/1980
Address: 25: [REDACTED]ow Rd
Hidden Hills, CA 91302
Previous Addresses:
18056 Lake Encino Dr Encino, CA 91316
19254 Romar St Northridge, CA 91324
19254 Romar St Canoga Park, CA 91304
118 S CLARK DR APT 206 WEST HOLLYWOOD, CA 90048
5210 PREMIERE HILLS CIR APT 230 WOODLAND HILLS, CA 91364

Return to Exposed Homepage
Credit Cards!

ALL CREDIT CARD PIN CODES IN THE WORLD LEAKED ...
pastebin.com/2qbRRk3R
Sep 10, 2012 ... ALL CREDIT CARD PIN CODES IN THE WORLD LEAKED. 0000 0001 0002 0003 0004 0005 0006 0007 0008 0009. 0010 0011 0012 0013 ...

[2015] Credit card - Pastebin.com
pastebin.com/x85aGIKf
Jan 30, 2015 ... BANK BUKOPIN | Indonesia[ID] | VISA | CLASSIC | CREDIT CARD | LO:120 LA:- 5 [ResellerPanel]Live=> | 4211670101485875|07/2017|844 ...

Credit Card DUMP [Working] - Pastebin.com
pastebin.com/0suJUk7f
Feb 10, 2015 ... Want a free creditcard? Dump below of working cards as of 10/02/2015. 4427919903011599 0817 257. 4427910007028860 1115 553.

#OpUSA 10000 credit card leak - Pastebin.com
pastebin.com/8QB5018R
May 7, 2013 ... Credit card: American Express, 373276618282003. Expiration date: 8 2007. Cardholders Name: Nicole George. Credit card verification ...

[C++] USA Credit Card Leaked By XhàckerTN - Pastebin.com
pastebin.com/Ay9jvJx9
XhàckerTN ...

credit card leaked hacked - Pastebin.com
pastebin.com/KMPwvlS
Cybercrime Marketing

- Exploit FUD 0/35
- Scan Service Online
- Crypt Service Fud 0/35
- Traffic Service
- Support All Files (bots, miners bots, etc)
- Domains Included
- Hosting Included
- Lifetime Support
- Automatic Update
- All OS Compatible

---

**Packages**

- **Pack Day**
  - 1 Day
  - Unlimited Domain Names
  - 150K Traffic Limit
  - $20

- **Pack Week**
  - 1 Week
  - Unlimited Domain Names
  - 150K Traffic Limit
  - $100

- **Pack Month**
  - 1 Month
  - Unlimited Domain Names
  - 150K Traffic Limit
  - $300
Collection of Cracked Paid RATs

I'd like to present to you my list of cracked paid RATs sorted by coding language. Please PM me if any download link isn't working, I will provide a new one for you.

Format:
Language
Name (Thread Design)
Download Link

Thank you hackb0t for providing .onion links

VB.NET (.NET 2.0)
Proton RAT (http://i.imgur.com/Mq5hVKb.png)
http://sh.st/uBM0r

Diamond RAT (http://i.cubeupload.com/AfyMG2.png)
http://4zjgf5i7dkafxpdm.onion/index.php ... &q=838

LuxNET (http://i7.minus.com/ibiXfLEOy381VW.jpg)
http://4zjgf5i7dkafxpdm.onion/index.php ... &q=839

Nanocore (https://i.imgur.com/R1xLbyf.png)
http://4zjgf5i7dkafxpdm.onion/index.php ... &q=840

Plasma RAT v1.5.1 (http://i.imgur.com/O75WJNg.png)
http://ge.tt/7D7PV6x1/v/0

PHP
KazyBot (http://i.imgur.com/rnETeTb.png)
http://4zjgf5i7dkafxpdm.onion/index.php ... &q=845
Casting some light
Stopping TOR

- Application Protocols
- SSL Intercept
- IP Reputation-Based Filtering
- Sandbox Solutions
- DLP Solutions
Policies that make sense
“Oh, look ... they're reading '1984' in Ms. Smith's English class.”
“Spoiled” exit Nodes and being anonymous

- Exit nodes doing MitM
- Controlling both entry and exit nodes
- Using NON-Tor Services
Pentagon hunts for ISIS on the secret Internet

By Barbara Starr and Jamie Crawford, CNN

Updated 6:08 PM ET, Tue May 12, 2015
MEMEX Deep Web Search Engine

- Deep Web Crawlers
- Indexers
- Threat Intelligence
- US Gov’t Program
Want to play a game?

- Use a different system to test. Don’t use VMs. Use Live CDs or USBs
- Use a VPN on top of TOR (I like Private Internet Service – others? Tweet me @aamirlakhani)
- Don’t connect back to your network
- Spend time building a offline image.
- Listen, surf, and don’t participate
- Almost all newbie’s will get scammed, hacked, or in some sort of illegal trouble (e.g. .onion Twitter)
Apply Knowledge to Real World

Educate + Learn = Apply

Awareness
Technology
Risk Mitigation

DarkNET can be a valuable tool for security professionals
How to Apply what I learned

- Darknet is a valuable tool for researchers to gauge the state of their cyber security program:
  - Users need to be aware of the dark and dangerous groups of attackers.
  - Reputation and Unified Threat Management Systems can help mitigate risks.
  - Researchers need to understand traffic is not anonymous. Controlling entry and exit nodes may be able to reveal true identity of users. ISPs and law enforcement may monitor TOR and other protocols.
  - Threat Intelligence can be gained by monitoring “chatter” on your employees and your organizations.
FortiClient detected viruses on your Mac!

Processes: /Applications/Firefox.app/Contents/MacOS/firefox
Item: /Users/alakhani/Downloads/AOkDdXGe.com.part
Virus: EICAR_TEST_FILE
Status: Quarantined
‘Blastware’ Beware

Recent destructive malware in the wild

- **Disk Wipers**
  - Overwrites hard-drive and MBR
  - Triggered by logic bomb/timer
  - South Korea, March 2013
    - 3 banks, 2 media companies
    - 50,000 systems

- **Ransomware**
  - Encrypts data
  - Leaves hard drive intact
  - Forensics unhampered

New 2014 FortiGuard Labs discovery: **DorkBot**

- Erases hard drive if analysis is detected
- New variations likely to destroy other targets
Shout Out

- RSA and RSA Asia
- Fortinet and FortiGuard Labs
- Singapore
- TOR Project
- Google Image Search (or this presentation would have no pictures)
Thank You

- Jack Chan

- Fortinet Blog: blog.fortinet.com

- FortiGuard Research: www.fortiguard.com

- Twitter: @FortiGuardLabs