In The Dark: An Introduction to the Hidden World of the Dark Web

Will Gragido
Head of Threat Intelligence
Digital Shadows
The dark web...
Where is it?

- Not accessible via traditional browsers
- Exists somewhere amongst the Surface and Deep webs
- For most people it is the stuff of legend; like monsters under the bed
Oh what a wicked web we weave...or is it?

- For some, it is a vehicle and means to an end for illicit activity.
- For others, it is a vital tool in their arsenal to ensure privacy and anonymity.
- Global privacy and anonymity issues will ensure it continues to grow.
Dangerous but worth the risk

- Complexity is worth the value provided

- Why?

digital shadows
And so the dance begins...
But not all is as it seems...
Legitimate uses of dark web services

https://facebookcorewwwi.onion/
Dark net markets
You can have anything you want, but you won’t get it for free!
Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet: the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Botnet

Zeus Botnet

Zeus botnet cheapest on alphabay make your own bot and enjoy hacking. If you want Compiled Zeus Botnet Please select in option. Thanks

Sold by shonajaan - 101 sold since May 2, 2015 Level 2
270 items available for auto-dispatch

<table>
<thead>
<tr>
<th>Features</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product class</td>
<td>Origin country</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Ships to</td>
</tr>
<tr>
<td>Ends in</td>
<td>Worldwide</td>
</tr>
<tr>
<td></td>
<td>Worldwide</td>
</tr>
<tr>
<td></td>
<td>Escrow</td>
</tr>
</tbody>
</table>

- Default - 1 days - USD +0.00 / item
- Default - 1 days - USD +0.00 / item
- Compiled Zeus Botnet Ready To Work - 1 days - USD +70.00 / item

Qty: 1 | Buy Now | Queue

0.0029 BTC
Exploit kit

[Exploit Kit] Bleeding Life (2.0)

The Bleeding Life exploit kit is a blackhat Web application consisting of several recent exploits. Since first mentioned in October 2010 there were: two full versions (v1 and v2), Mini-Java version, Java edition, Adobe edition and the latest - Bleeding Life RELOADED seen "in-the-wild". As with other exploit kits, this one uses PHP and MySQL backend; it also utilizes AJAX technology too ...

Sold by sh00t: 205 sold since Jun 27, 2015
Vendor Level 3 Trust Level 5
270 items available for auto-dispatch

<table>
<thead>
<tr>
<th>Feature</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product class</td>
<td>Digital Origin country</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Unlimited Ships to</td>
</tr>
<tr>
<td>Ends in</td>
<td>Never Payment</td>
</tr>
</tbody>
</table>

Default - 1 days - USD +0.00 / item
Purchase price: USD 1.10
Qty: 1
Buy Now

0.0008 BTC
Weapons

Armsgel PROTECTA 12GA Shotgun (LAST ONE)

**Update: 1 left** Armsgel PROTECTA (12 GA). Price is negotiable if you purchase other items with this. Only serious buyers please. PM me if you have a specific request.

Sold by Goblinking - 0 sold since Dec 20, 2015

<table>
<thead>
<tr>
<th>Level</th>
<th>Trust Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physics Origin country</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Unlimited Ships to</td>
</tr>
<tr>
<td>Ends in</td>
<td>Never Payment</td>
</tr>
</tbody>
</table>

Purchase price: USD 6,500

Qty: 1  Buy Now

digital shadows
Weapons, continued

Glock 19

Sold by Alexandria - 2 sold since Aug 25, 2015

Level 1 Trust Level 5

<table>
<thead>
<tr>
<th>Feature</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product class</td>
<td>PhysicalOrigin country</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Ships to</td>
</tr>
<tr>
<td>Ends in</td>
<td>Never Payment</td>
</tr>
</tbody>
</table>

Default - 1 days - USD +0.00 / item

Purchase price: USD 2,000.1

Qty: 1

Buy Now
Drugs

1 GRAM STRAIGHT DROP CRACK COCAINE

This straight drop crack that I offer is the best on the streets, so I know it's the best on the net by far. We offer this 1988 butter cooked straight from the pearly fish scale cocaine that we offer. So you must know this this the best thing ever. If you where a big crack smoker in the 80-90's and you missed the potency look no more, you just found it. We don't stretch our crack with...

Sold by EL HEFE - 82 sold since Sep 15, 2015

<table>
<thead>
<tr>
<th>Level 3</th>
<th>Trust Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Feature</td>
</tr>
<tr>
<td>Product class</td>
<td>Physici</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Unlimit</td>
</tr>
<tr>
<td>Ends In</td>
<td>Never</td>
</tr>
<tr>
<td>Payment</td>
<td>Escrow</td>
</tr>
</tbody>
</table>

PRIORITY OVERNIGHT - 1 days - USD +30.00 / order

Purchase price: USD 145.00
Qty: 1

Buy Now
Credit cards

USA HIGH LEVEL CC - Check store for more!

HIGHEST VALIDITY AND QUALITY CARDS - FEEDBACK's TALKS! Spend 1 minute reading this page so we don't have misunderstandings! Negative feedbacks will not be tolerated = instant blacklist and no support! I always reply to all messages sooner or later, just be patient! Format First Name: Last Name: Address: City: State: Zip: Country:
Cardnumber: Cvv: Exp: Delivery - most of the time I...

Sold by siton3d - 4158 sold since Apr 4, 2015

<table>
<thead>
<tr>
<th>Features</th>
<th>Level 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product class</td>
<td>Digital goods</td>
</tr>
<tr>
<td>Quantity left</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Ends in</td>
<td>Never</td>
</tr>
<tr>
<td>Origin country</td>
<td>Afghanistan</td>
</tr>
<tr>
<td>Ships to</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Payment</td>
<td>Escrow</td>
</tr>
</tbody>
</table>

Default - 1 days - USD +0.00 / item

Purchase price: USD 8.50

Qty: 1  Buy Now  Queue

0.0222 BTC
Currency

Counterfeit $100 USD Notes - Security Features Included!

Counterfeit $100 bills 

*Important Information on Stock*

**MINIMUM ORDER IS NOW THREE (3) BILLS.**

Please do NOT message me about stock if I am sold out. I do not make these bills. I have to get them from BlackLabel on consignment. Once I sell bills, I have to then repay him. I have lots of buyers that are not releasing their escrows for multiple days after bi... 

Sold by **JanetYellen** - 196 sold since Nov 13, 2015

**Vendor Level 2**

**Trust Level 4**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product class</td>
<td>Physical Origin country</td>
</tr>
<tr>
<td>Quantity left</td>
<td>United</td>
</tr>
<tr>
<td>Ends In</td>
<td>55 itemShips to</td>
</tr>
<tr>
<td></td>
<td>United States</td>
</tr>
<tr>
<td>Payment</td>
<td>FE List</td>
</tr>
</tbody>
</table>

Priority Mail - 3 days - USD +6.00 / order

Purchase price: USD 35.00

Qty: 1

Buy Now
Take aways

- The Dark Web is not going away anytime soon; its popularity is growing
- We can embrace it or we can ignore it at our own risk
- Become familiar with it; its content, services, and denizens
- Use this knowledge to ensure that the noble reasons for its use continue while the illicit diminish
Contact me

- will.gragido@digitalshadows.com
- Twitter: @wgragido
- Twitter: @digitalshadows
In The Dark: An Introduction to the Hidden World of the Dark Web

Will Gragido
Head of Threat Intelligence
Digital Shadows
A Futurist’s look at Nation-State Cyber-Espionage

Vicente Diaz
Principal Security Analyst
Kaspersky Lab
@trompi
The rules driving evolution
Where do we come from?

- Obviously, all countries pushed to develop their capabilities.
- According to their capabilities, we can make 3 categories.
Category 1 - “Unlimited” resources
Category 2 - “Middle class”
Category 3 – Externalize capabilities

Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1lhChT!rbB... infotomb.com/eyyx0.torrent
What happens when you get public?

- Public level: Public scrutiny’s power depends on democracy’s health. May affect legislation and future capabilities.

- Operational level:
  - Operation burst – but maybe amortized
  - Operational changes and continue as usual
  - Do nothing

- **Diplomatic** level: Obvious consequences
Lessons learned

- Avoid attribution (but get the job done)
Where are we now?

- Top players have:
  - Legislation control
  - Infrastructure control
  - Relationships with partners/companies
Boiten argued the prime minister may try and persuade services that use end-to-end encryption, such as Apple and WhatsApp, to introduce government backdoors to give UK spies access to private communications.
Actually, where is the data now?

Undersea Fiber-Optic Cables in the Middle East
Who can do that?

- Nobody trusts other’s infrastructure → Internet Balkanization
What will we see in the future?

- Besides espionage, control of adversary’s critical systems
- “Middle class Stuxnet”

BlackEnergy Involved in Targeted Attack Against Boryspil Airport, Says Ukraine
Future cyberespionage

“Middle class” operations are enough when you control the infrastructure
Future cyberespionage

- Assume unlimited supply of 0 days

HACKERS CLAIM MILLION-DOLLAR BOUNTY FOR IOS ZERO-DAY ATTACK
Future cyberespionage

- Get control of non-controlled infrastructure attacking network devices, firmware, rogue hardware, etc. Regin and Equation as early adopters.

Either way, the malware investigators at Belgacom never got a chance to study the routers. After the infection of the Cisco routers was found, the company issued an order that no one could tamper with them. Belgacom bosses insisted that only employees from Cisco could handle the routers, which caused unease among some of the investigators.
Future cyberespionage

- Exfiltration through non monitored protocols and devices.
Future and present cold war

U.S. Charges Chinese Government Officials With Cyber Espionage
Future and present cold war

Obama: U.S. and China Reach Cyber-Espionage 'Common Understanding'
The rules of evolution

- Rule 1: Keep sophistication low to avoid attribution
- Rule 2: Infrastructure control
- Rule 3: Improve your Cyber diplomacy
- Rule 4: “IoT” infections over “computers”
A Futurist’s look at Nation-State Cyber-Espionage