RSAC Studio

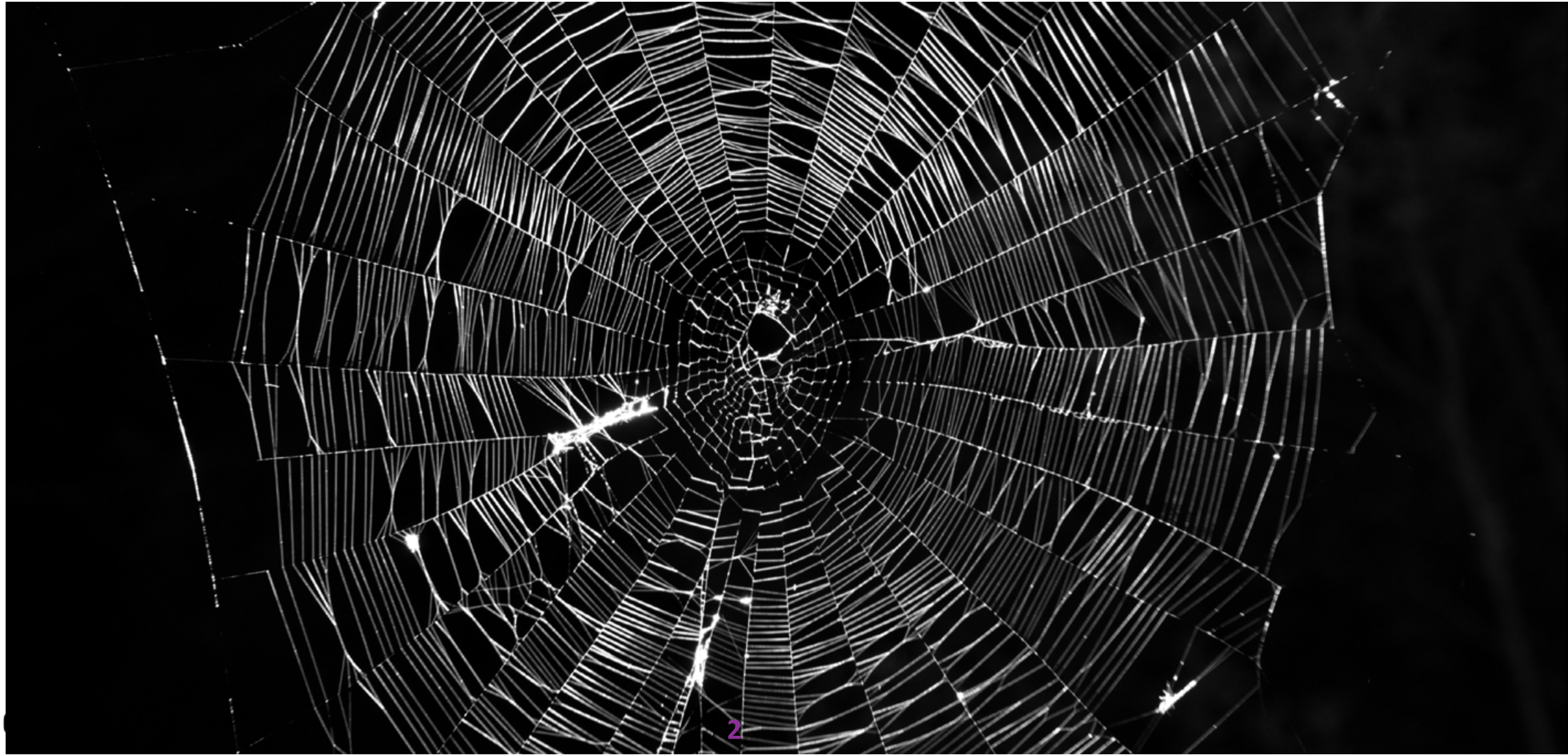
Connect to Protect

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

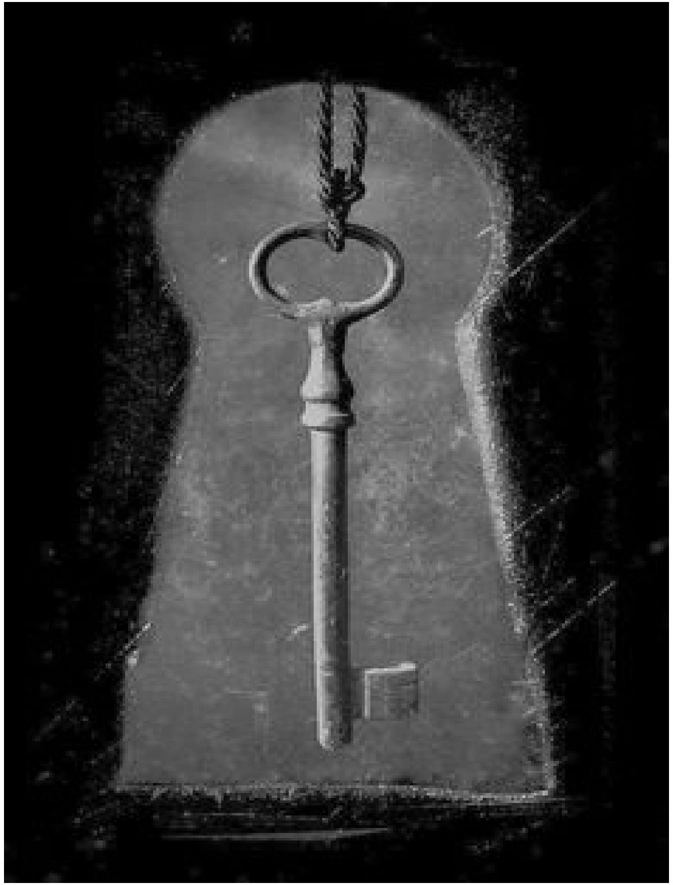
Will Gragido

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?

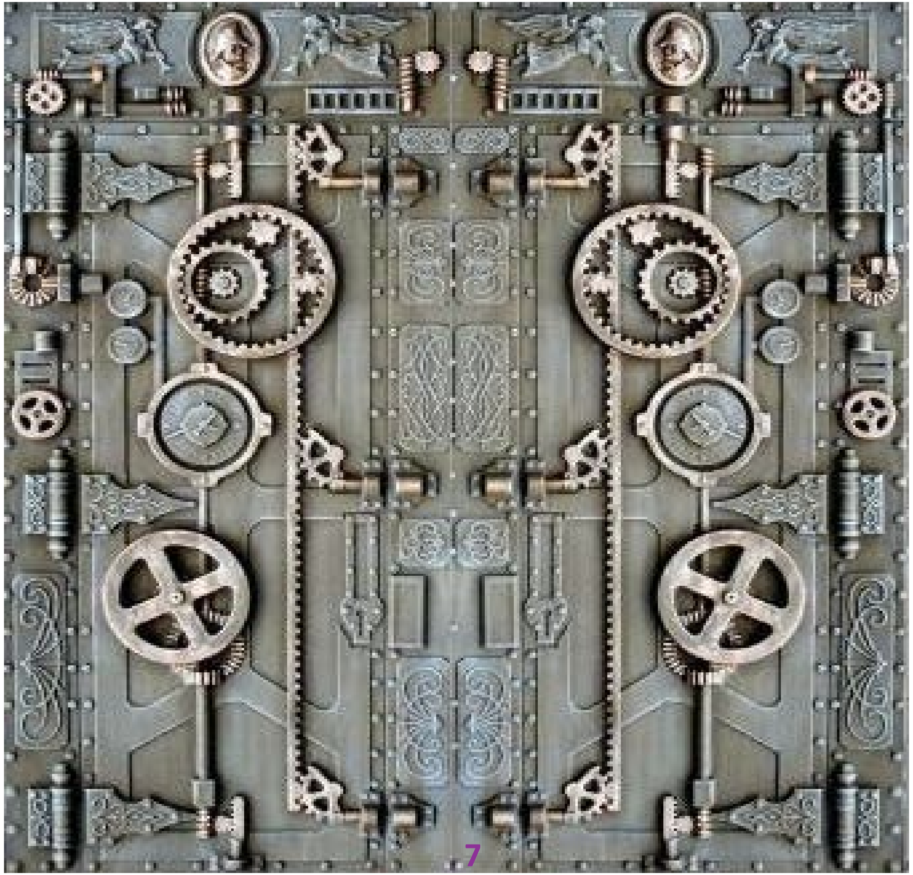
- For some, it is a vehicle and means to an end for illicit activity
- For others, it is a vital tool in their arsenal to ensure privacy and anonymity
- Global privacy and anonymity issues will ensure it continues to grow

Dangerous but worth the risk

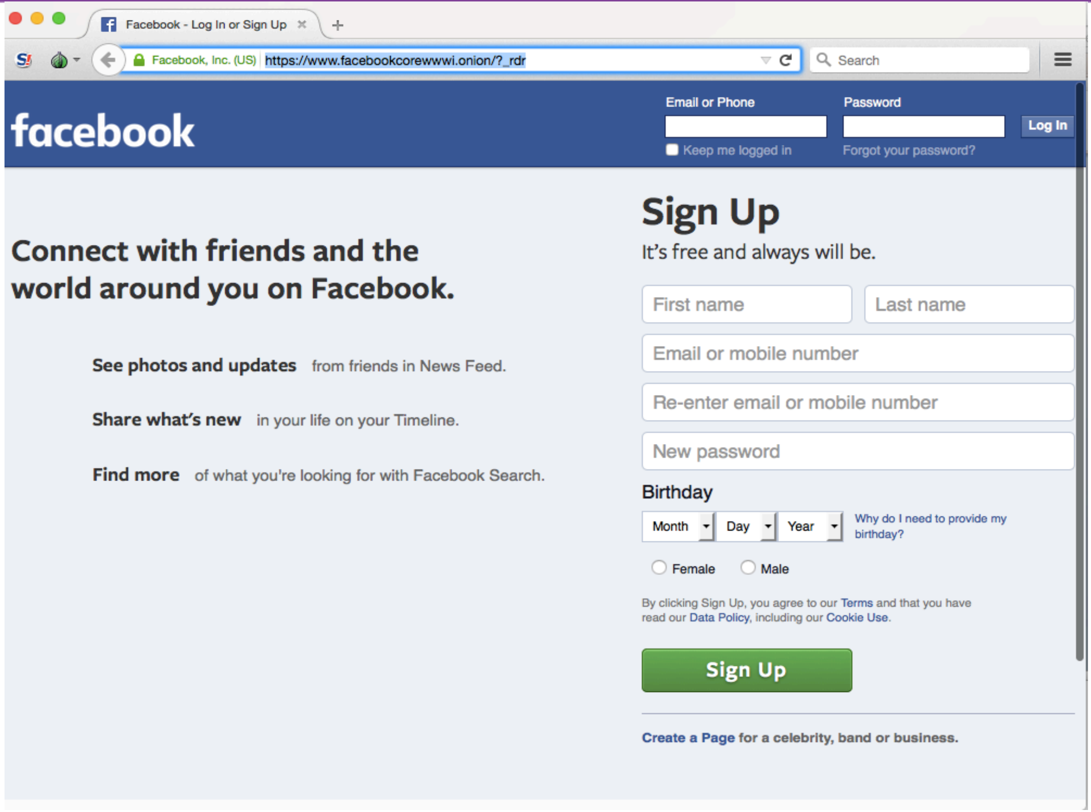
- Complexity is worth the value provided
- Why?

And so the dance begins…

But not all is as it seems…



Legitimate uses of dark web services



Facebook - Log In or Sign Up

Facebook, Inc. (US) https://www.facebookcorewwwi.onion/?_rdr

facebook

Email or Phone

Password

Log In

□ Keep me logged in

Forgot your password?

Sign Up

It's free and always will be.

Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Find more of what you're looking for with Facebook Search.

First name

Last name

Email or mobile number

Re-enter email or mobile number

New password

Birthday

Month Day Year

Why do I need to provide my birthday?

○ Female ○ Male

By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.

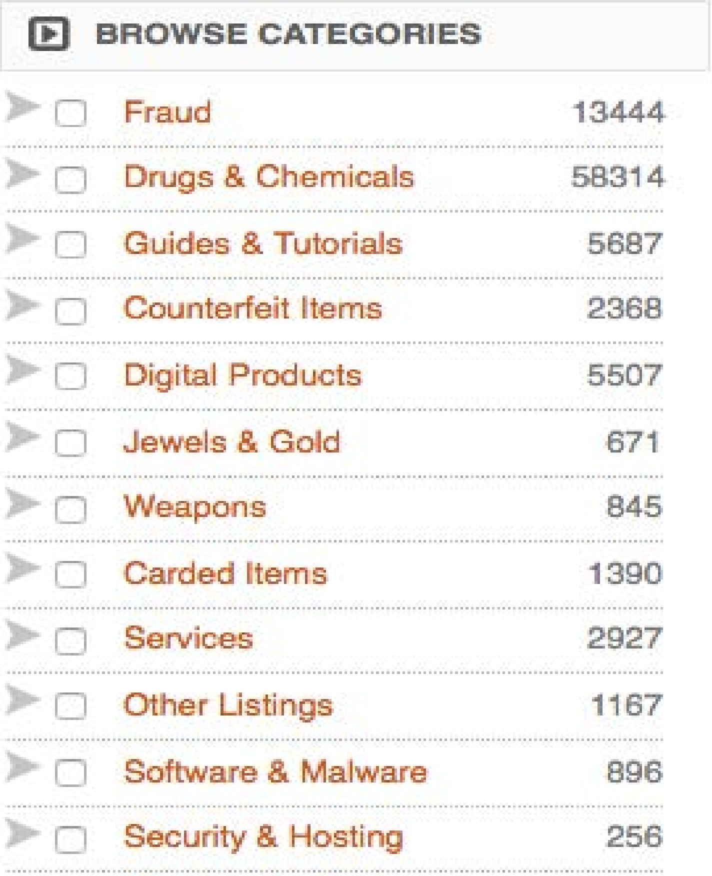
Sign Up

Create a Page for a celebrity, band or business.

https://facebookcorewwwi.onion/

Dark net markets

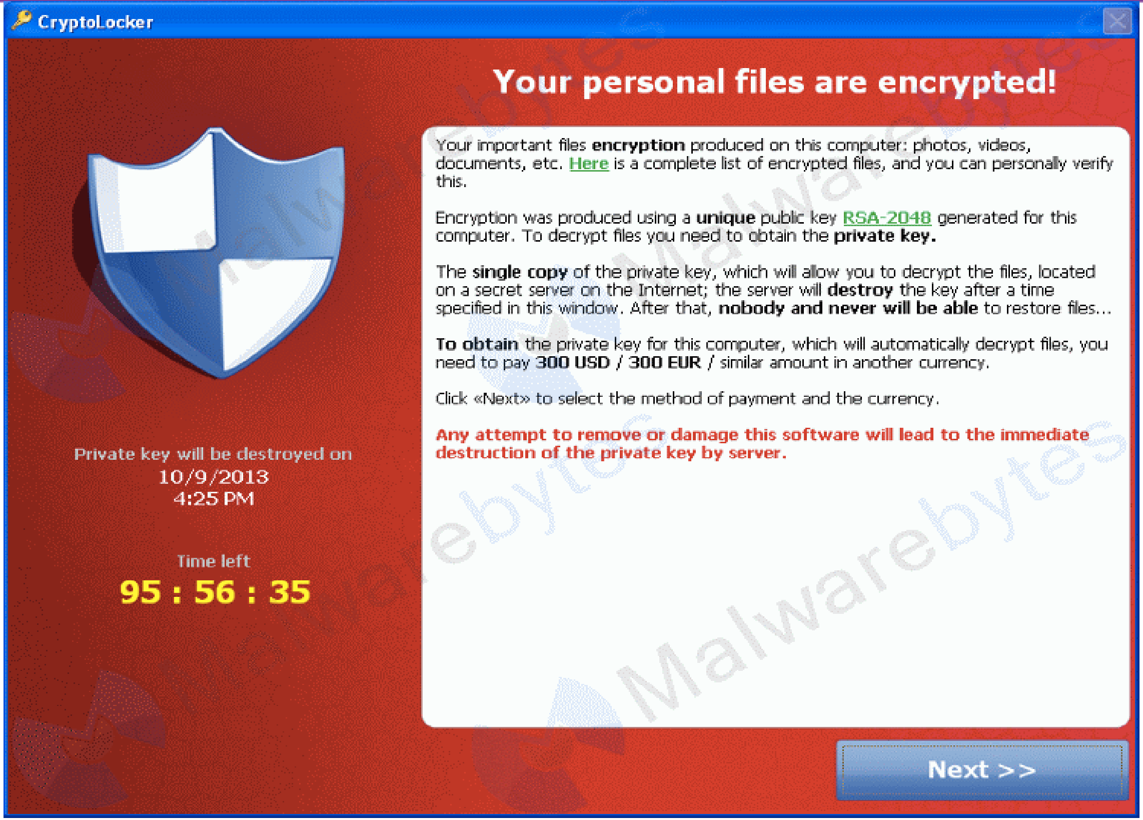
You can have anything you want, but you won’t get it for free!



BROWSE CATEGORIES

□	Fraud	13444
□	Drugs & Chemicals	58314
□	Guides & Tutorials	5687
□	Counterfeit Items	2368
□	Digital Products	5507
□	Jewels & Gold	671
□	Weapons	845
□	Carded Items	1390
□	Services	2927
□	Other Listings	1167
□	Software & Malware	896
□	Security & Hosting	256

Ransomware



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.

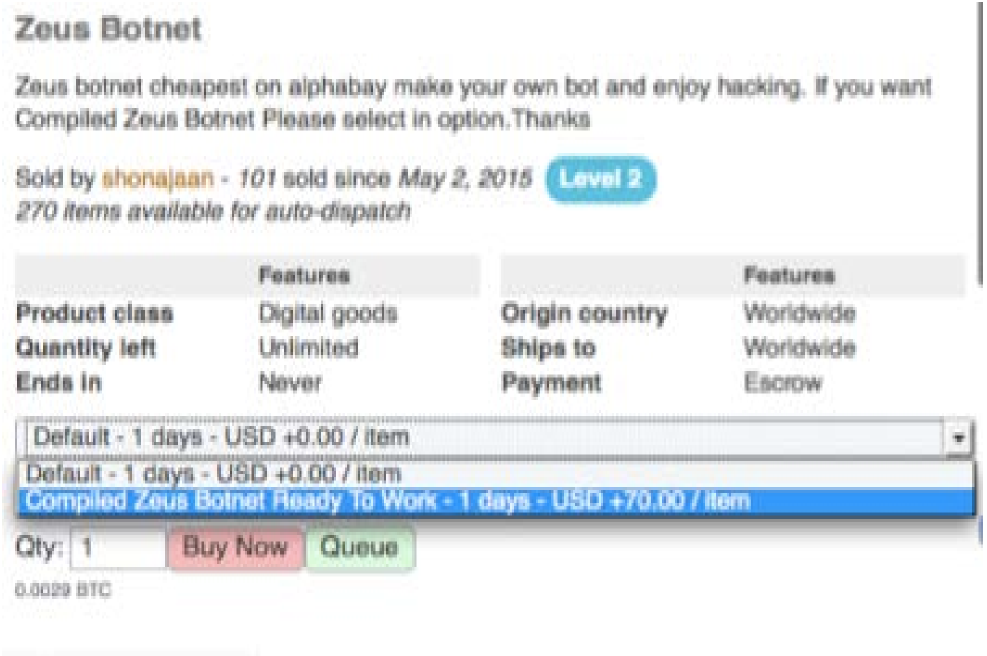
Click «Next» to select the method of payment and the currency.

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

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

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

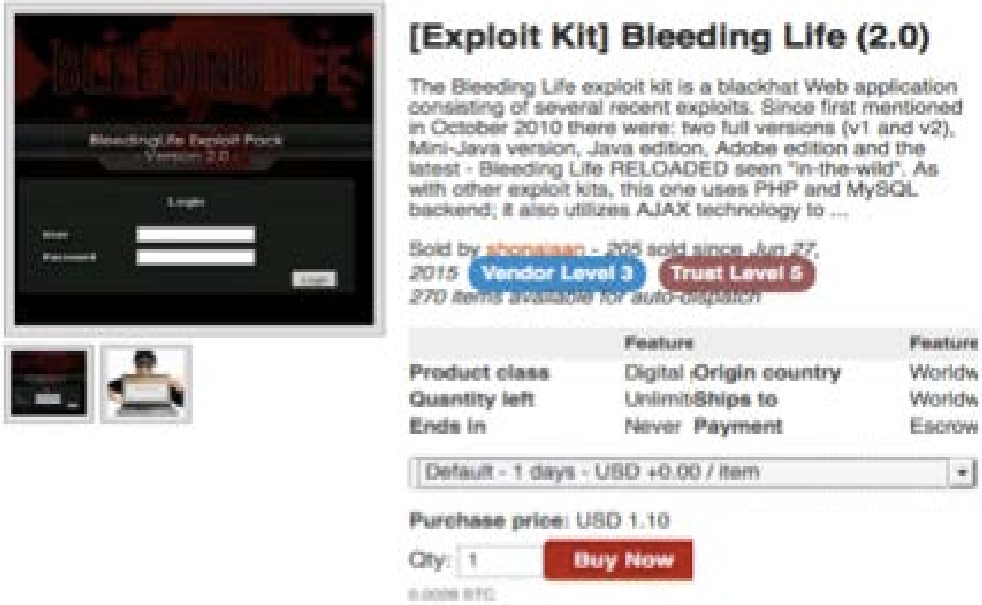
	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

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 to ...

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

	Feature		Feature
Product class	Digital	Origin country	Worldw
Quantity left	Unlimit	Ships to	Worldw
Ends in	Never	Payment	Escrow

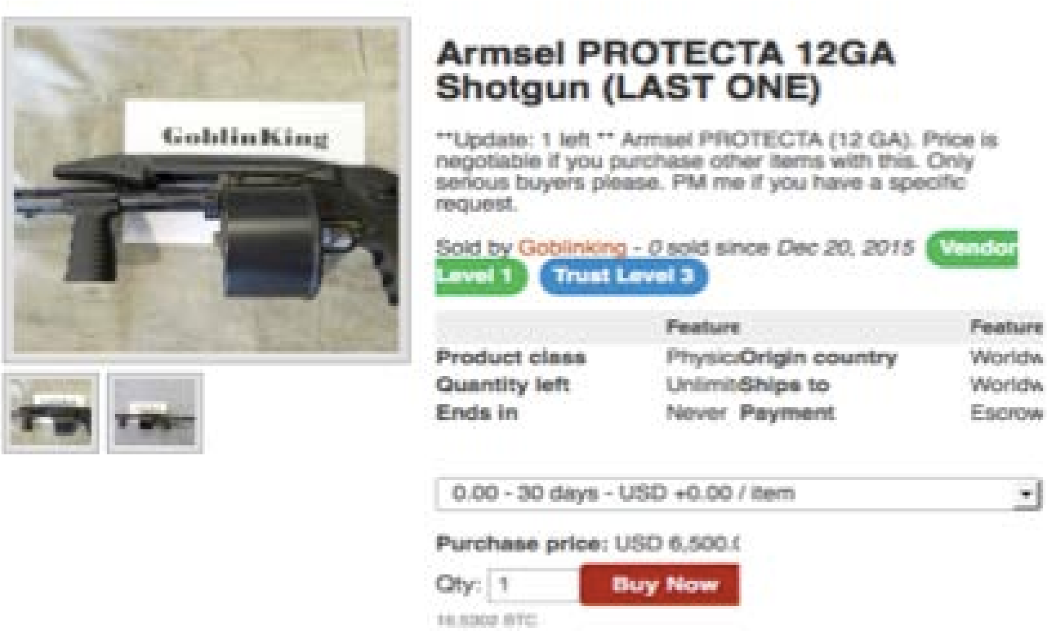
Default - 1 days - USD +0.00 / item ▾

Purchase price: USD 1.10

Qty: 1 Buy Now

0.0026 BTC

Weapons



Armsel PROTECTA 12GA Shotgun (LAST ONE)

**Update: 1 left ** Armsel 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 Vendor Level 1 Trust Level 3

	Feature		Feature
Product class	Physica	**Origin country**	Worldw
Quantity left	Unlimit	**Ships to**	Worldw
Ends in	Never	**Payment**	Escrow

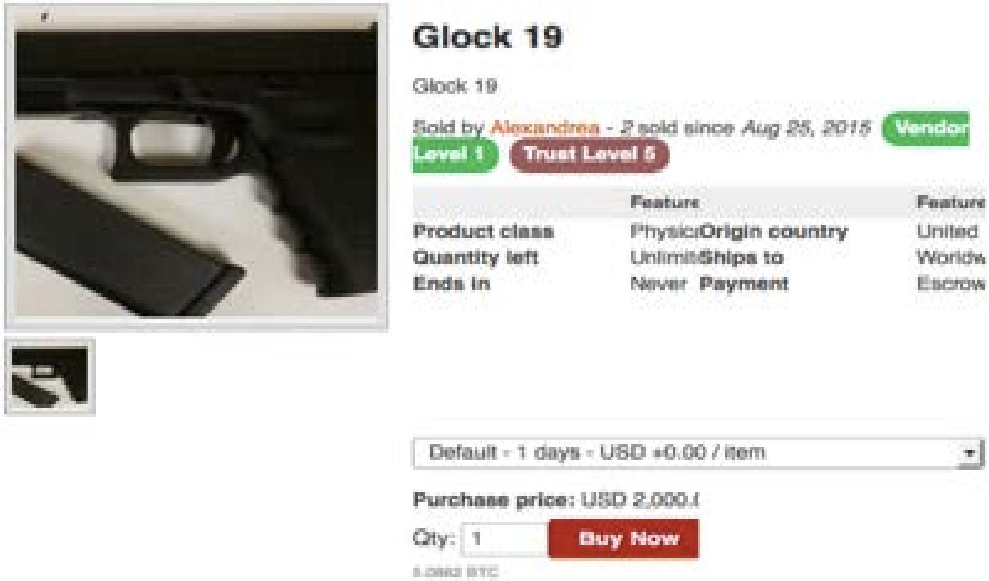
0.00 - 30 days - USD +0.00 / item

Purchase price: USD 6,500.(

Qty: 1 Buy Now

16.5302 BTC

Weapons, continued



Glock 19

Glock 19

Sold by Alexandrea - *2 sold since Aug 25, 2015* Vendor Level 1 Trust Level 5

	Feature		Feature
Product class	Physic	**Origin country**	United
Quantity left	Unlimit	**Ships to**	Worldw
Ends in	Never	**Payment**	Escrow

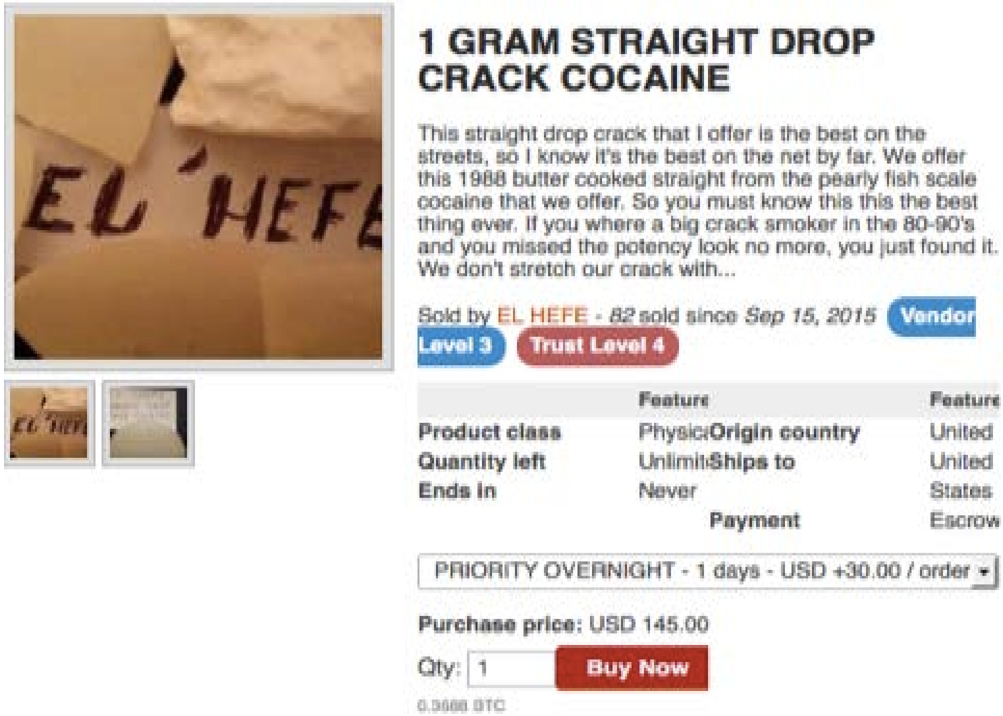
Default - 1 days - USD +0.00 / item

Purchase price: USD 2,000 /

Qty: 1 Buy Now

[illegible] BTC

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* Vendor Level 3 Trust Level 4

	Featur		Featur
Product class	Physic	**Origin country**	United
Quantity left	Unlimit	**Ships to**	United
Ends in	Never		States
		Payment	Escrow

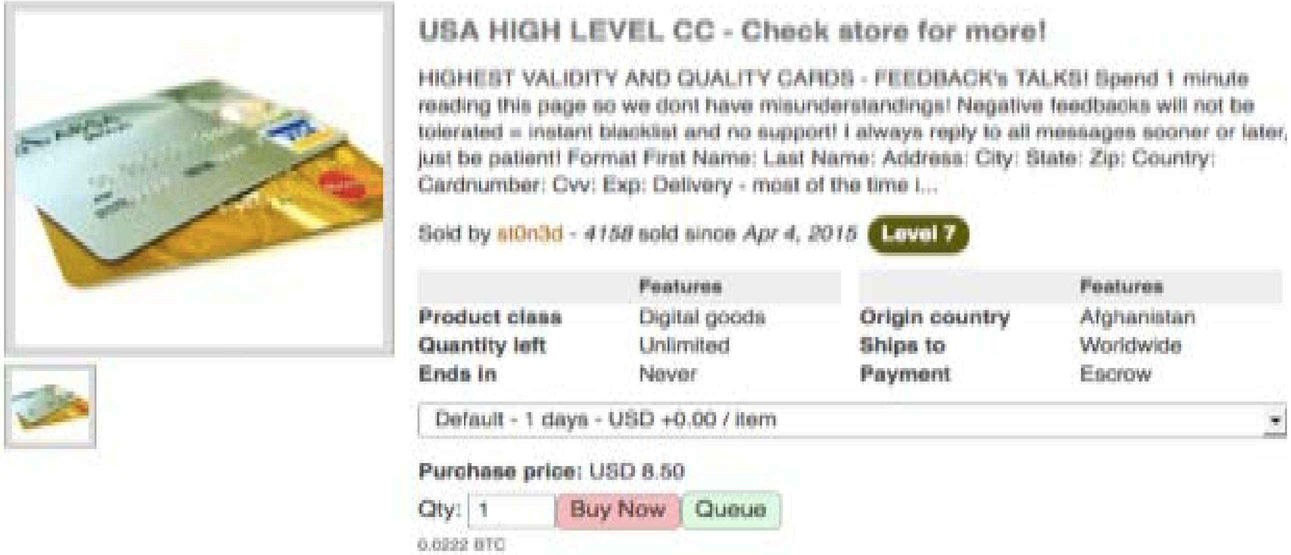
PRIORITY OVERNIGHT - 1 days - USD +30.00 / order ▾

Purchase price: USD 145.00

Qty: 1 **Buy Now**

0.3688 BTC

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 dont 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 sl0n3d - *4158* sold since *Apr 4, 2015* Level 7

	Features		Features
Product class	Digital goods	**Origin country**	Afghanistan
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

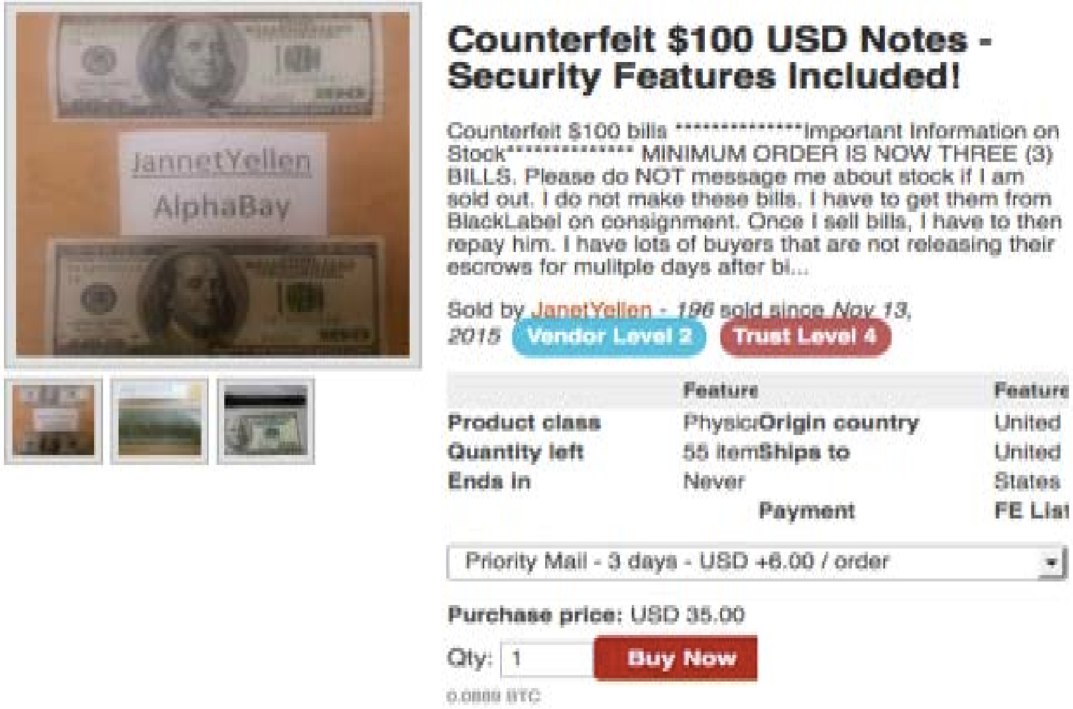
Default - 1 days - USD +0.00 / item

Purchase price: USD 8.50

Qty: 1

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 mulitple days after bi...

Sold by JanetYellen - *196 sold since Nov 13, 2015* Vendor Level 2 Trust Level 4

	Feature		Featur
Product class	Physic	**Origin country**	United
Quantity left	55 item	**Ships to**	United
Ends in	Never		States
		Payment	**FE List**

Priority Mail - 3 days - USD +6.00 / order ▾

Purchase price: USD 35.00

Qty: 1 **Buy Now**

0.0889 BTC

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

RSAC Studio

Connect to Protect

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

Will Gragido

Head of Threat Intelligence
Digital Shadows

#RSAC

RSAC Studio

Connect to Protect

A Futurist´s look at Nation-State Cyber-Espionage

Vicente Diaz

Principal Security Analyst
Kaspersky Lab
@trompi

#RSAC

The rules driving evolution

Where do we come from?

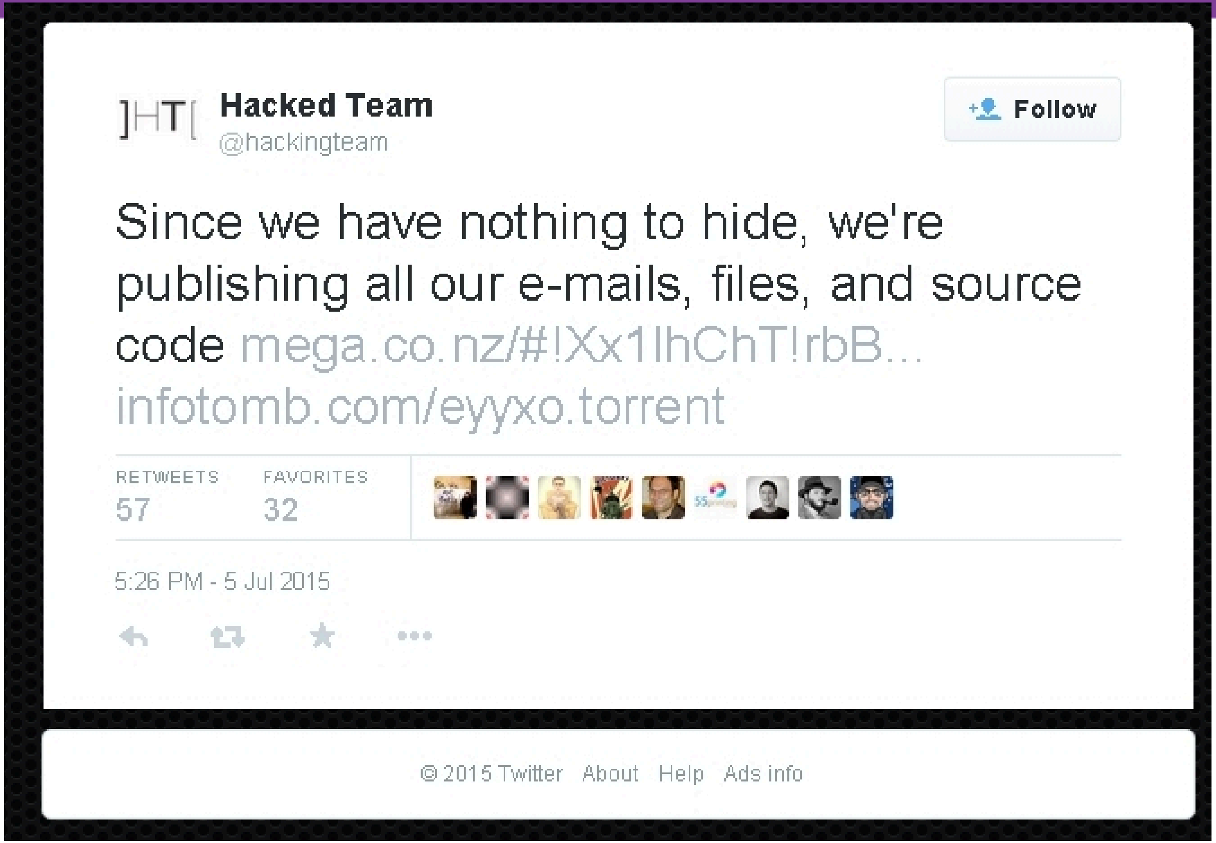
- Obviously, all countries pushed to develop their capabilities.

- According to their capabilities, we can make 3 categories.

Category 1 - “Unlimited” resources

Category 2 - “Middle class”

Category 3 – Externalize capabilities



]HT[**Hacked Team**
@hackingteam

Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1lhChT!rbB... infotomb.com/eyyxo.torrent

RETWEETS 57 FAVORITES 32

5:26 PM - 5 Jul 2015

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

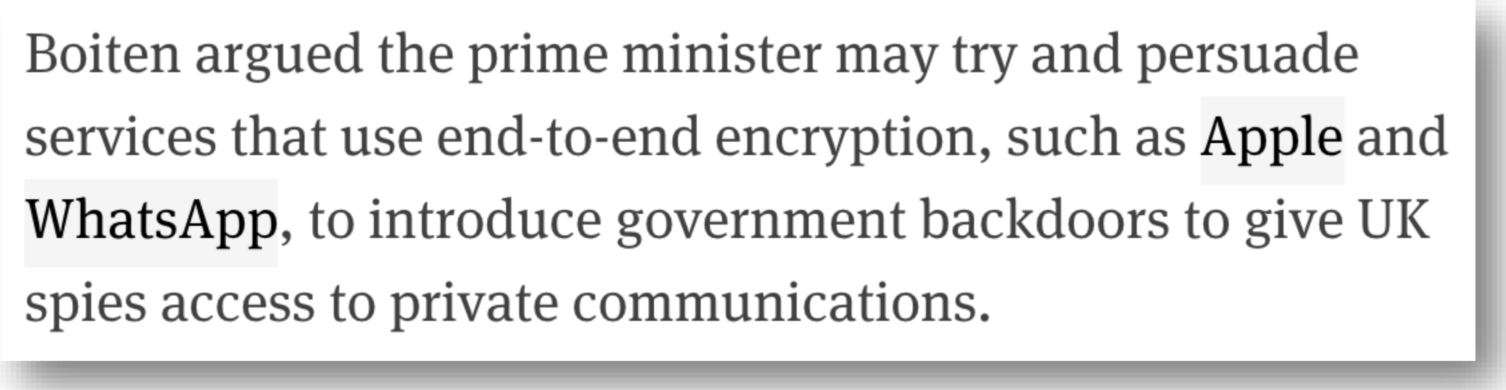
Lessons learned

- Avoid attribution (but get the job done)

Where are we now?

- Top players have:
  - Legislation control
  - Infrastructure control
  - Relationships with partners/companies

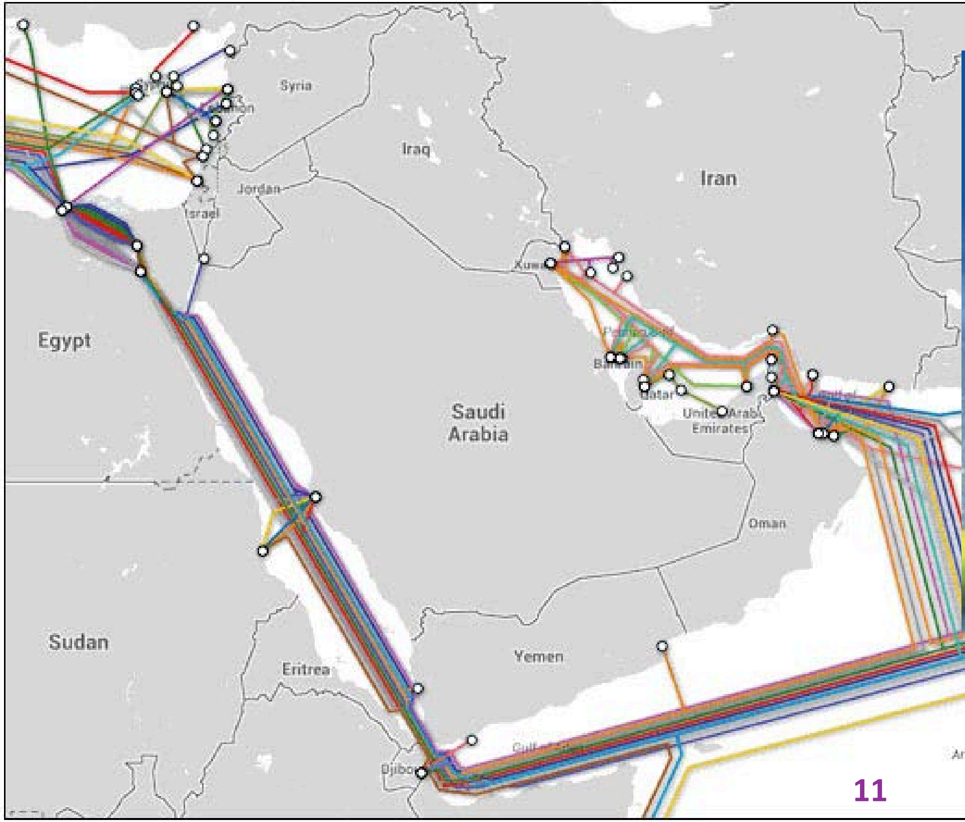
Only one barrier left

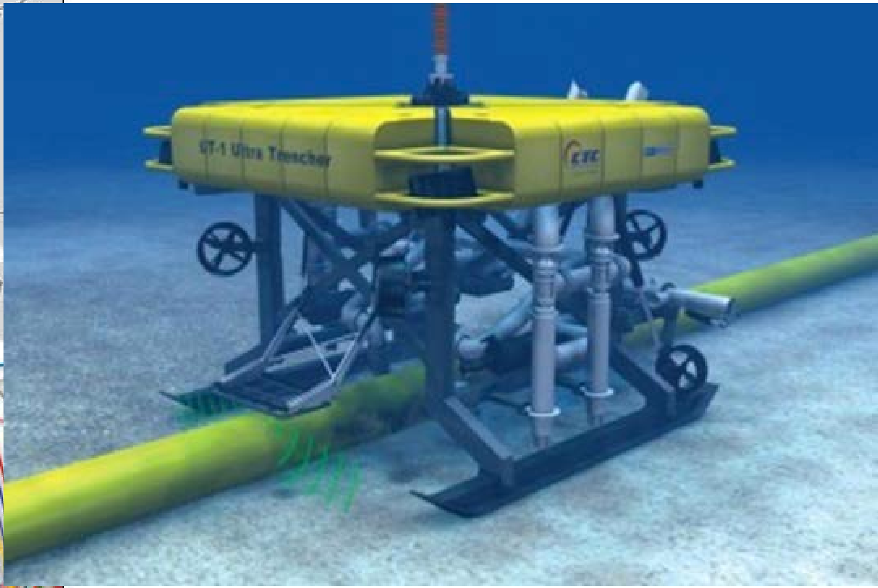


Boiten argued the prime minister may try and persuade services that use end-to-end encryption, such as Apple and WhatsApp, to introduce government backdoors to give UK spies access to private communications.

Actually, where is the data now?

Undersea Fiber-Optic Cables in the Middle East



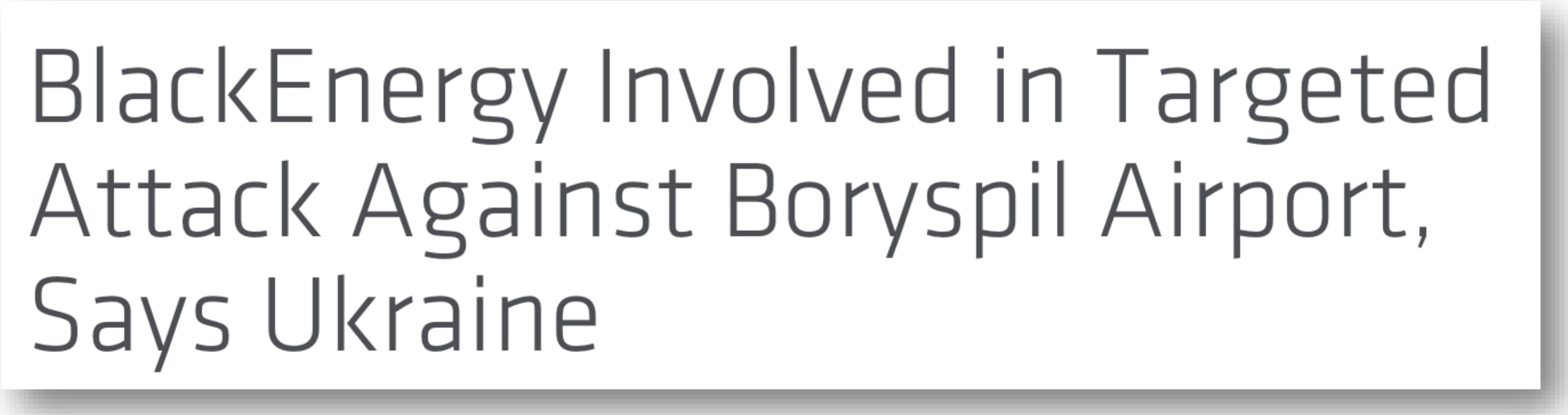


Who can do that?

- 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”



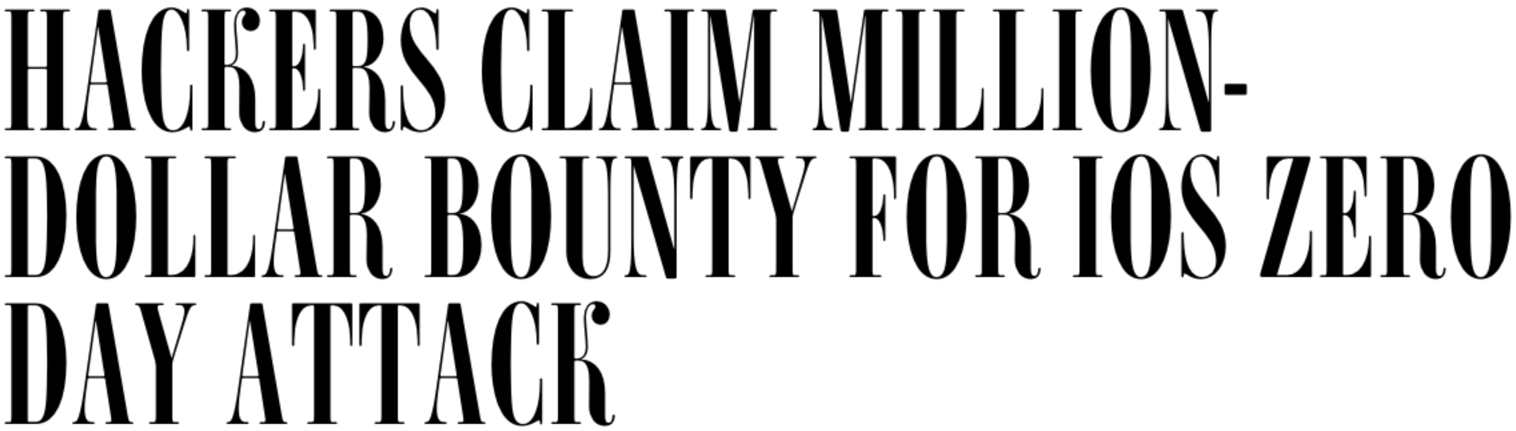
BlackEnergy Involved in Targeted Attack Against Boryspil Airport, Says Ukraine

Future cyberespionage

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

Future cyberespionage

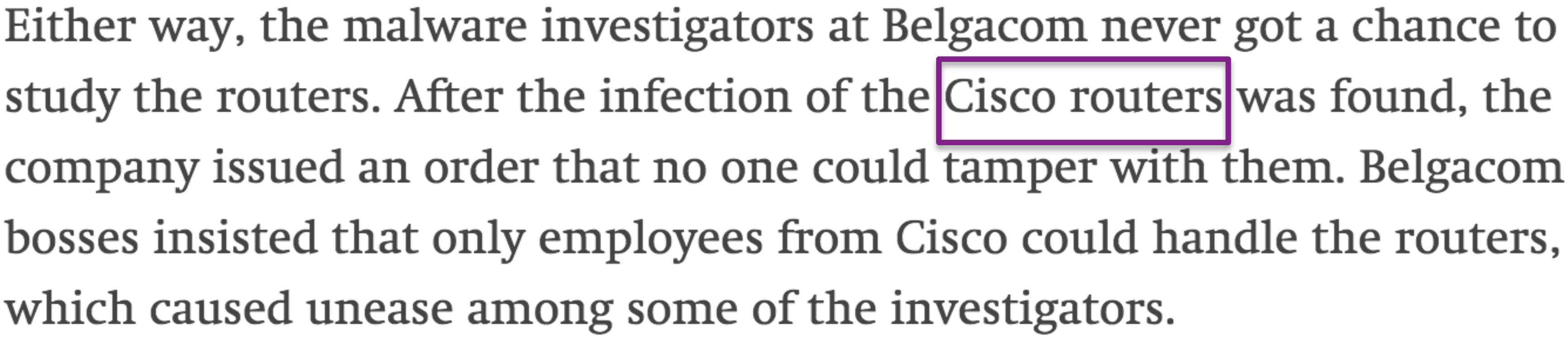
- Assume unlimited supply of 0 days



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