

# The Dark Web

## Dark Web, Dark Net, What you need to know...

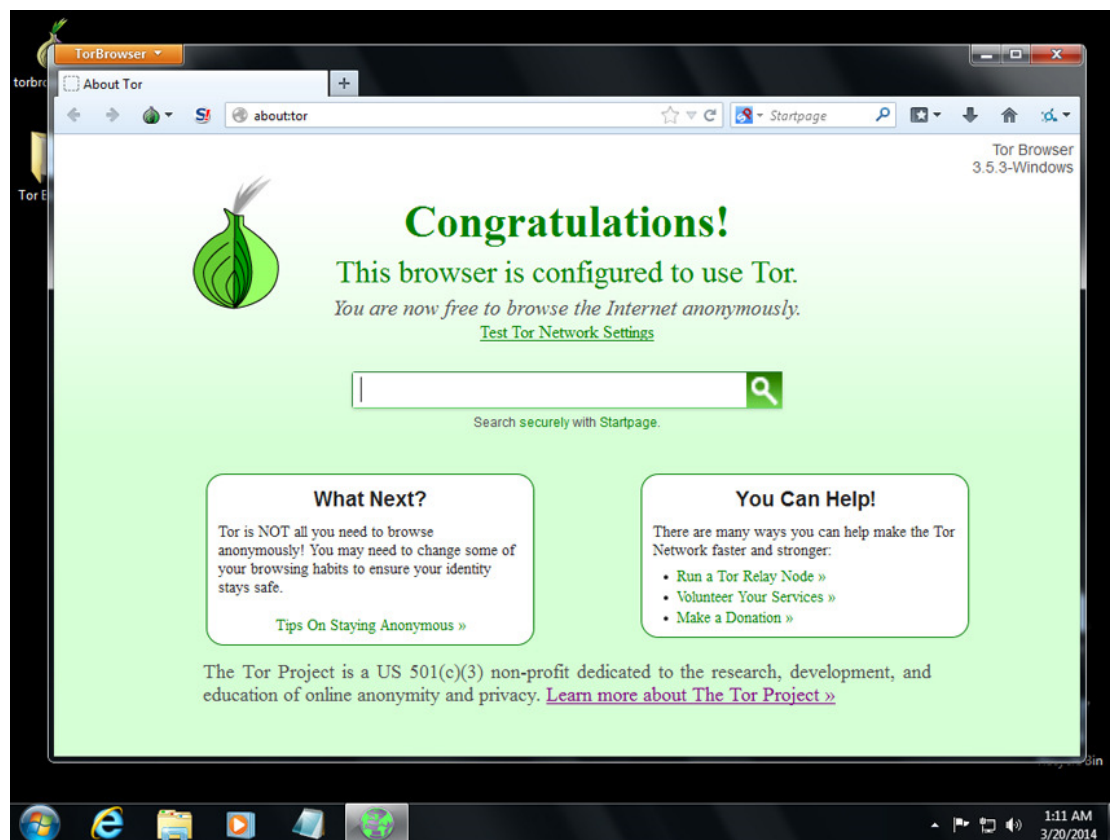
Martin Overton  
ERS Team Lead, Security Consultant, Ethical  
Hacker, Malware Specialist, Forensics, etc.  
IBM ERS, CSAR



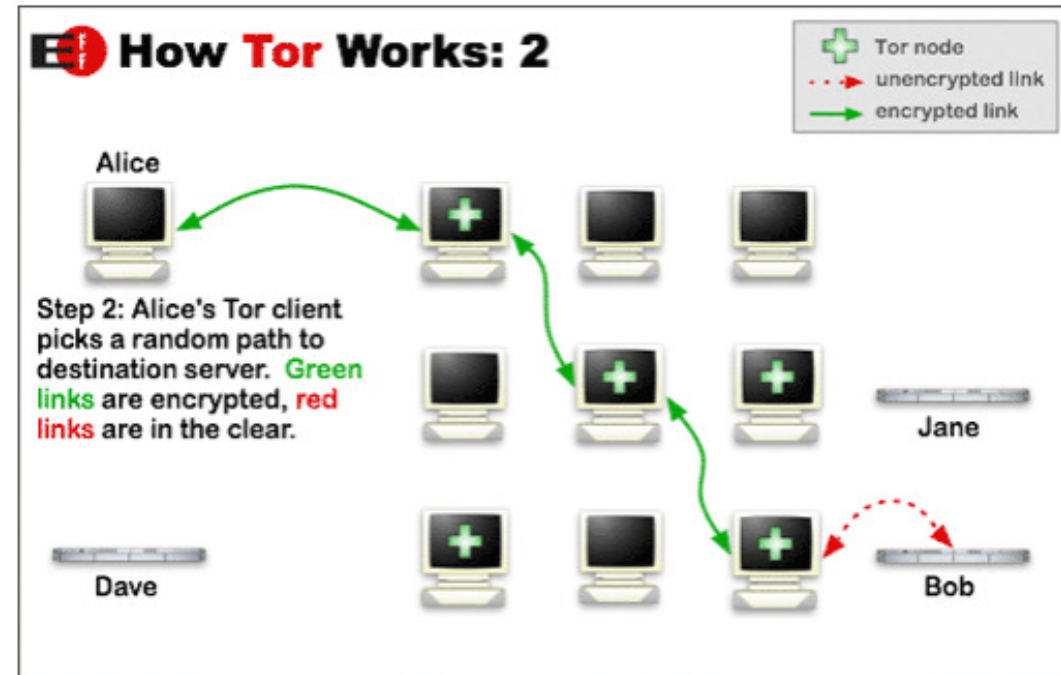
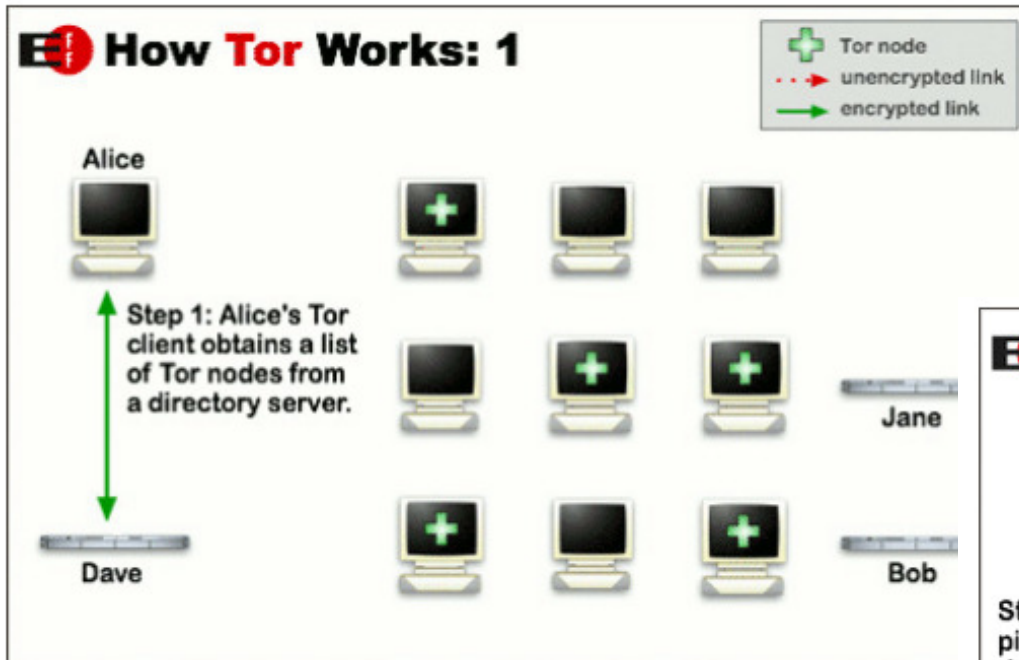
## The “Dark Net” / “Dark Web”

- Used by those working inside repressive countries/states for secure “anonymous” Internet use and communication.
- Also used by the bad guys and girls for hiding their activity and identity.
- A massive black-market now exists on TOR for guns, drugs, stolen credentials, hacked account, malicious services, identity theft, credit card accounts, etc.
- Then there are crypto-currencies, such as Bitcoin that are anonymous and effectively untraceable\* ...

\* if used properly



# The Onion Router (TOR)



# There's not just TOR!

Welcome to I2P

Epsites of Interest

- anoncoin.i2p
- Anonymous Git Hosting
- Bug Reports
- Dev Forum
- diffracker
- echelon.i2p
- Ident Microblog
- Javadocs
- jeko.i2p
- killyourtv.i2p
- Pastebin
- Planet I2P
- stats.i2p
- Technical Docs
- Trac Wiki
- Ugha's Wiki

Local Services

- Addressbook
- Configure Bandwidth
- Configure Language
- Customize Home Page
- Email
- Help

#i2p	95	[+ntlf] I2P Community & Support Channel   Current: 0.9.17   Off-topic discussions to
#salt	91	[+ntT] wiki: nacl.i2p   ontopic: anonymity, privacy, coding, meta salt   offtopic: politics, r
#i2p-chat	73	[+ntlf] I2P community off topic chatter and deep sleep chamber   I2P 0.9.17 released!
#i2p-dev	66	[+ntlf] Dev build: 0.9.17-10   http://zzz.i2p/topics/1778-toronto-i2p-meetings-summ
#irc2p	30	[+ntlf] Irc2P support. Please read the Irc2P terms and services by typing /rules or /qu
#torrents	30	[+nt] Welcome to #torrents   check out vuze.com for new I2P capability   feel free to
#freedom	30	[+nt] Freedom from all oppression, even if sanctioned by 51% mob of scared idiots. Libe
#overchan	29	[+n] https://www.youtube.com/watch?v=kKO9h-gG4Qg
#i2pd-dev	29	[+nt] Meeting will be rescheduled for a different day
#anoncoin	26	[+nt] Hard fork upgrade will be released soon; stay tuned!   UFO project is done; some
#tahoe-lafs	26	[+nt] Anonymous decentralized data store    Tahoe-LAFS for I2P v1.10.0 released: htt
#anonops	24	[+nt] Can't wait for you to fill my hole with your knowledge juice   RAWR!   #i2people
#mempo	23	[+nt]
#i2people	23	[+nt] Doing what we do every night, taking over the world. #metastasis for nom's distri
#ru	22	[+nt] Russian anonymous channel   Main charset is UTF-8   AIB: http://hiddenchan.i2p
#linux	18	[+nt] Welcome to #linux, the Windows haters club. Sacrificing fanboys (Windows and/c
#bitcoin	18	[+nt]
#coders	17	[+nt] scala: twitter.github.io/scala_School/
#Abscond	17	[+nt] https://www.reddit.com/r/TheAbscondBundle/comments/2skv61/new_release.o
#firehose	14	[+nt] Bugtraq - Ars Technica - r/netsec - LinuxToday - xkcd - explosm - Wired - Futility
#torrent-flood	14	[+nt] Feeds of tracker2.postman.i2p and diffracker.i2p; suggestions for other feeds wel
#tor	13	[+nt] Tor community on i2p   Questions? Highlight a ChanOp   https://blog.torproject.c

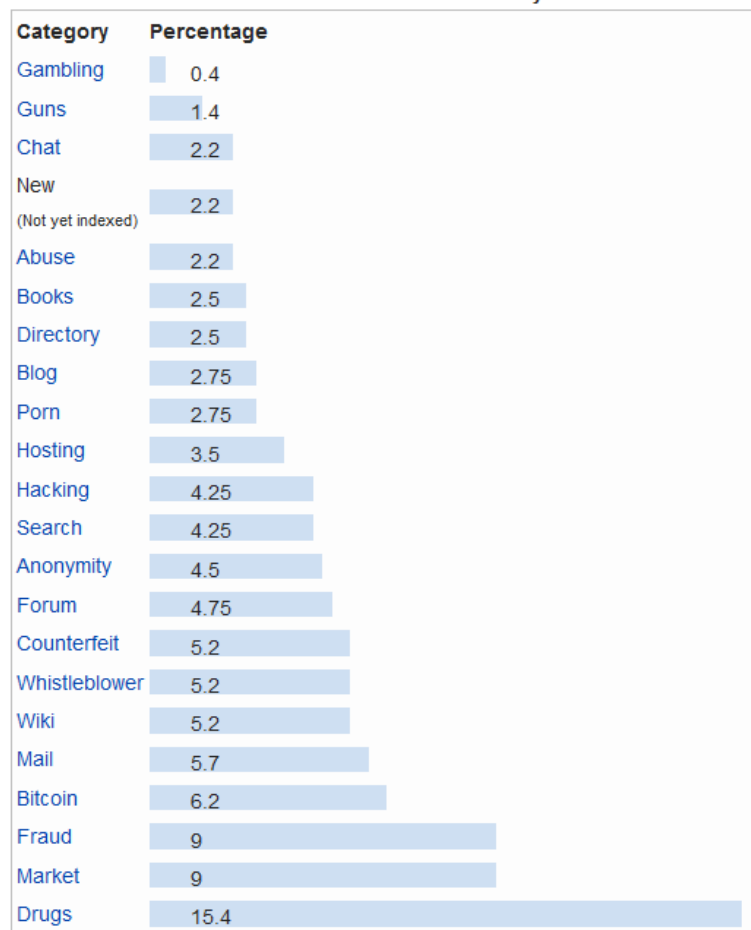
# What can you find on the “Dark Web”?

## Commerce [ edit ]

See also: [Darknet market](#)

- [Assassination market](#)
- [Agora](#) (defunct)
- [Atlantis](#) (defunct)
- [AlphaBay Market](#)
- [Babylon](#), an Italian language darknet market, shut down in August 2015<sup>[17]</sup>
- [Black Market Reloaded](#) (defunct)
- [C'thulhu](#) - An assassination group that advertises a variety of services, including
- [Evolution](#) (defunct)
- [Hitman network](#), a site that claims to offer murder for hire<sup>[20]</sup>
- [The Farmer's Market](#) (defunct)
- [Sheep Marketplace](#) (defunct)
- [Silk Road](#) (defunct)
- [TheRealDeal](#)
- [Utopia](#) (defunct)

Web based Hidden Services January 2015<sup>[1]</sup>



# Risks

- External
  - Reconnaissance using TOR; pre-attack planning
  - Attacks using TOR to hide originating IPs (DDoS, C&C, Hacking – Application and Network level)
  - Infection; browsing the dark web is not safe, drive-by downloads, exploit kits, etc.
- Circumventing IT controls
  - TOR from USB or using TAILS Live CD
  - Private Proxy
- TOR Relay Hosting
  - TOR relays set up in your own network leading to potentially illegal material, non-authorised users of your network resources and the legal knock-on effects
  - Possibility of the relay host being compromised (hacked) acting as a pivot point for attackers
- BitCoin Mining
  - Data centre and other powerful systems being used without the knowledge or approval of the asset owner

# Attacks using TOR

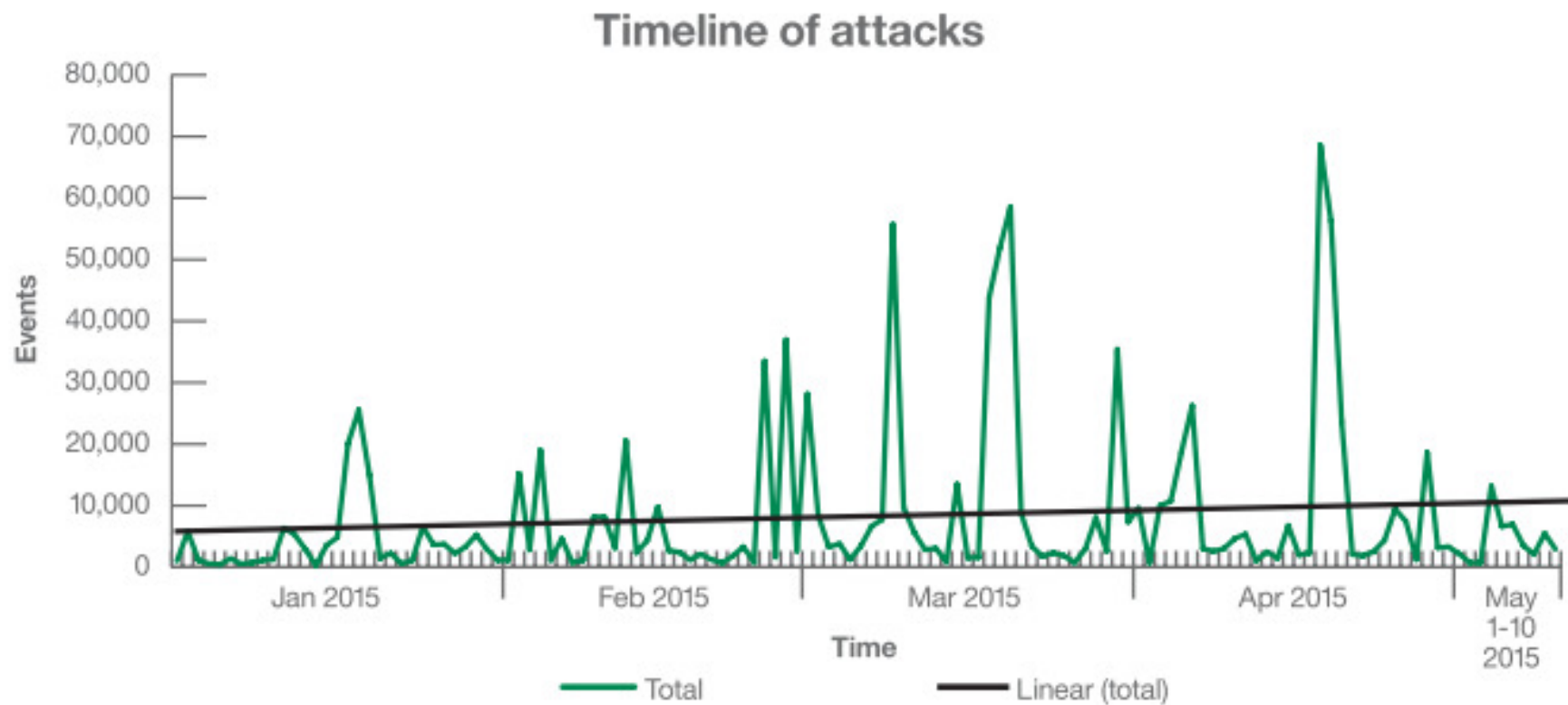


Figure 1. Malicious attacks from Tor have been on the rise since the beginning of 2015. Source: IBM MSS data.

# Attacks using TOR

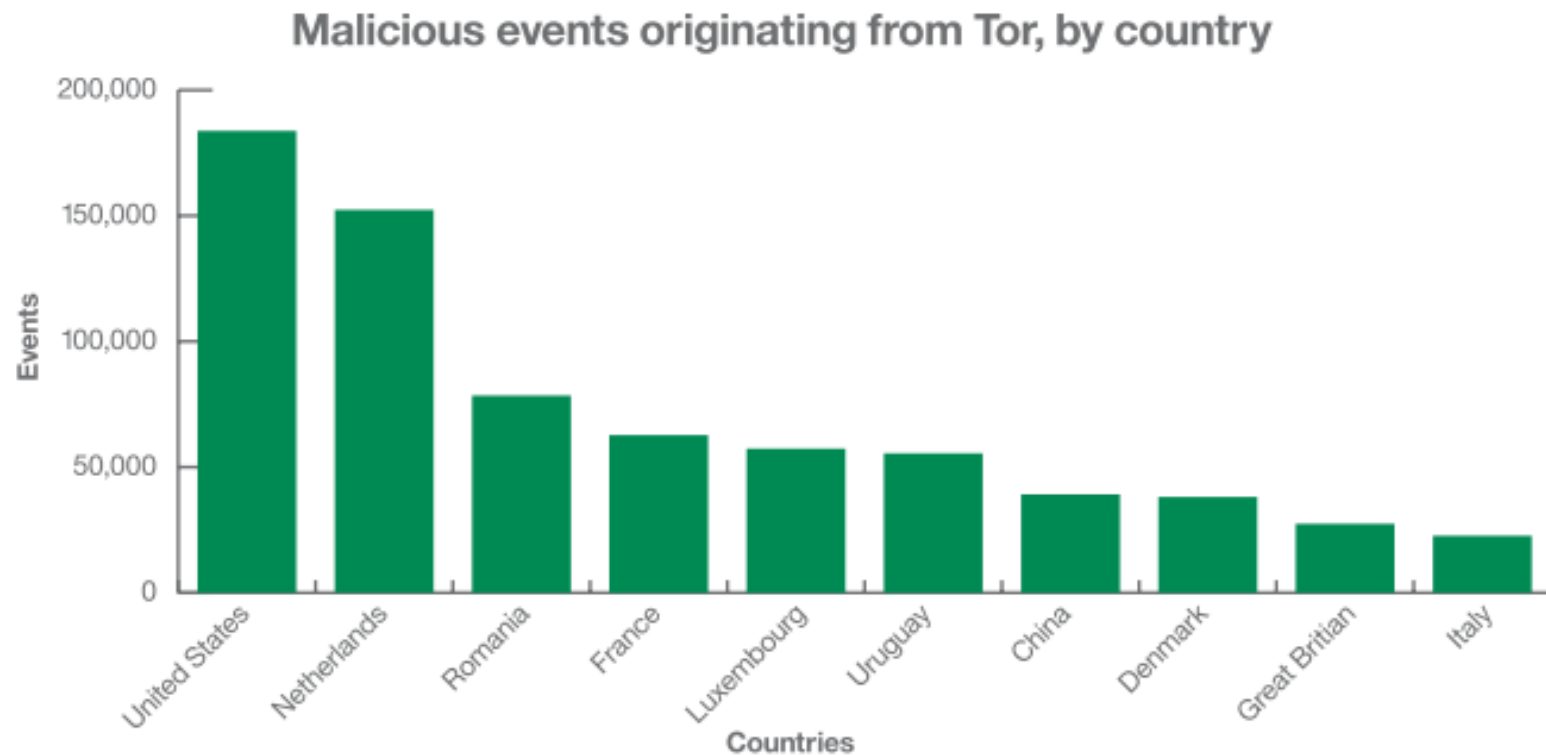


Figure 3. Malicious traffic volumes sourcing from Tor exit nodes, by country. Source: IBM MSS data (Jan 1, 2015 - May 10, 2015).



## Industries Under Fire...

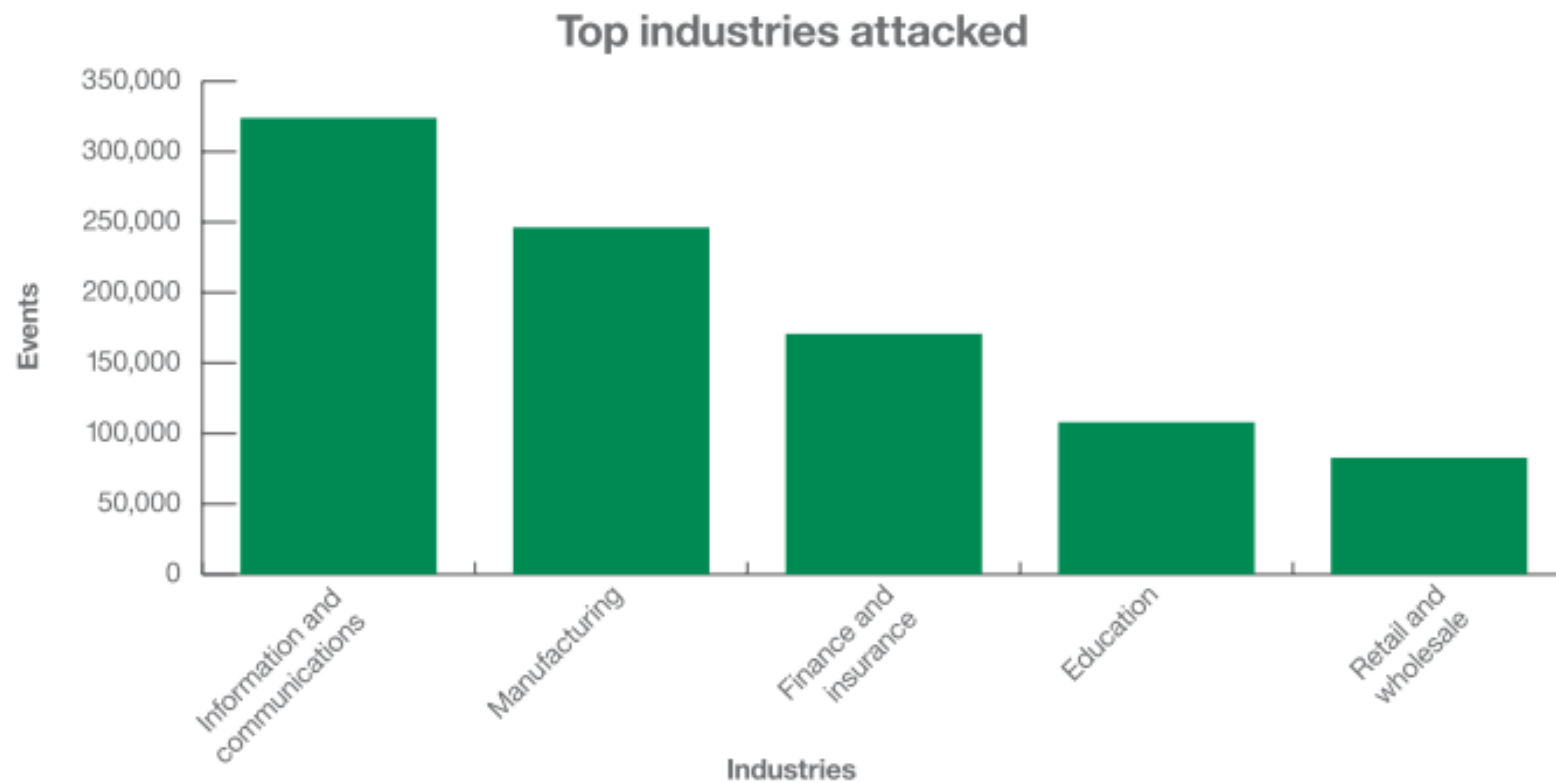
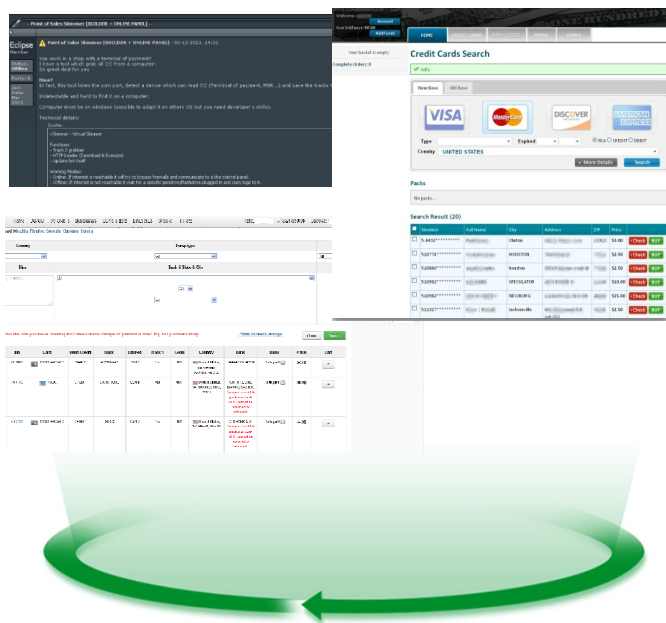


Figure 5. Comparison of malicious traffic from the Netherlands and the United States. Source: IBM MSS data. (Jan 1, 2015 - May 10, 2015)

# The emergence of a mature black market has made profiting from data theft easy

## A Global Black Market Dealing in Credit Card Data



- **Readily available black market sites** are now utilized to provide actual stolen credit card data and services to support the theft as well as the utilization of stolen data
- **Literally hundreds of these sites** are currently in operation selling cards from virtually every bank
- **Sites often include information on stores** like zip codes and store names where cards were stolen in order to help fraudsters make same state purchases
- **Credit card data is sold in bulk** and can be as cheap as \$5 per credit card
- **Specialized malware** like Dexter malware is available for purchase to infect PoS systems

**Malware as a Service (MaaS), Hacking as a Service (HaaS), DDoS as a Service (DaaS), Ransomware as a Service (RaaS), etc.**

## Incident Costs (Per Record)



Per-record data breach costs vary widely across industries, with a significant year-to-year increase for retail.



7

Currencies converted to US dollars

© 2015 IBM Corporation

## ERS – Retail Company

### ■ Business challenge:

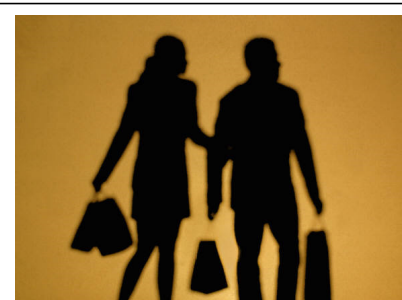
- The customer contacted IBM as it was suspected that the customer's website credential store (user ID and passwords) had been compromised and that hackers were stealing accounts with large loyalty card balances and selling these stolen accounts via a dark web site only available over TOR.
- TOR (The Onion Router Project) allows users to remain anonymous by bouncing communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection.

### ■ Solution:

- IBM confirmed that the integrity of the server had not been compromised.
- IBM confirmed that the account credentials misused were most likely due to a third party being compromised (shared passwords) or them being guessed.
- IBM confirmed that the web servers were not as secure as they could be and that credentials could easily be enumerated or guessed, allowing the hackers to seize accounts with large loyalty card balances and re-sell them.

### ■ Benefits:

- IBM performed a thorough assessment of the security posture of the servers, providing the customer with a list of critical areas/issues that should be reviewed/addressed including seriously improving the login and account management functions to make them more resilient to attack and misuse.
- The final report also included a set of medium and longer term recommendations on remediating migration procedures and security best practices that needed to be implemented to reduce the attack surface.
- Recommendations included the use of data analytics, such as SIEM and fraud detection solutions, such as i2 to help identify future attacks faster.



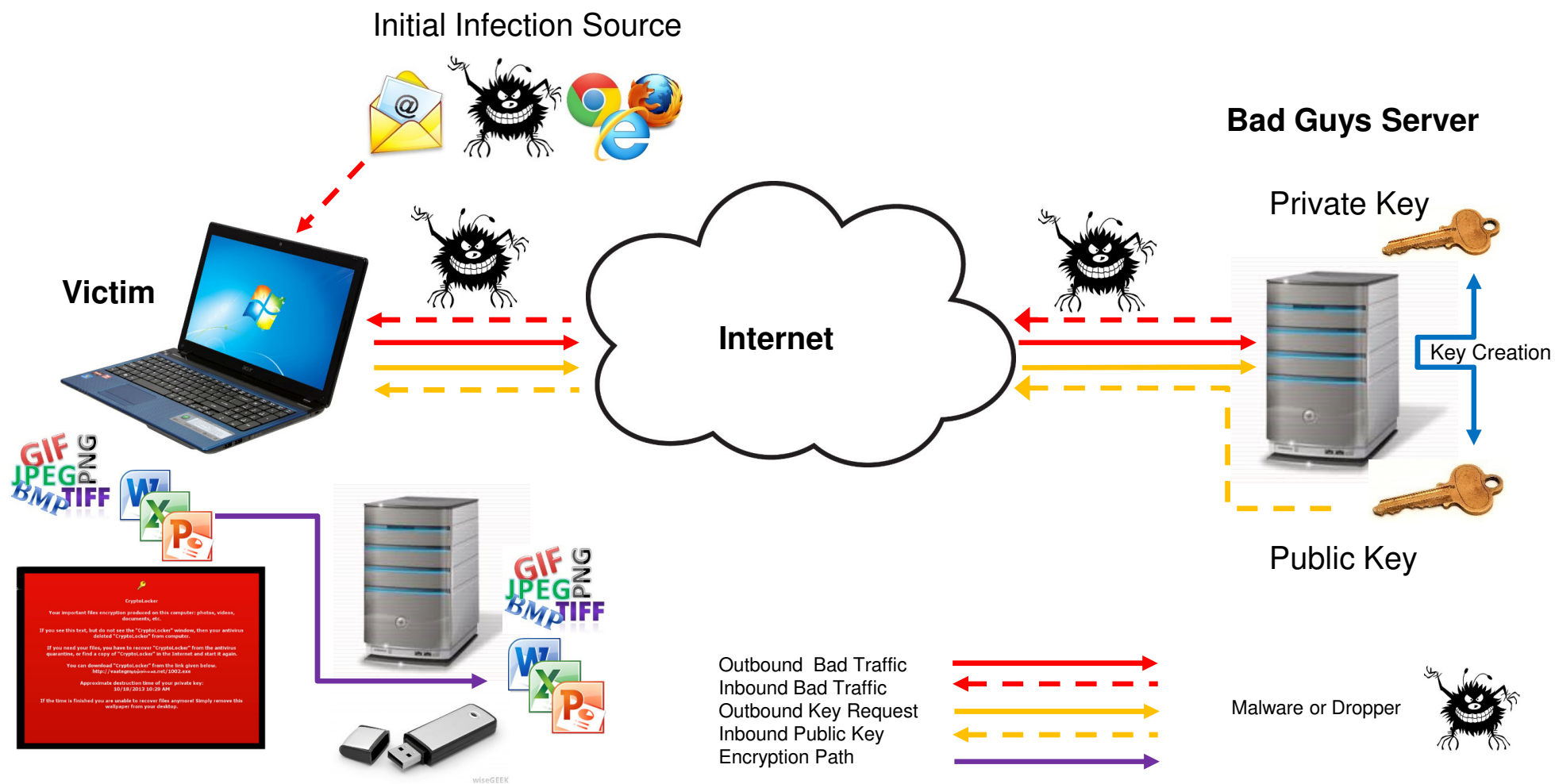
User accounts that had large loyalty card balances were being compromised and re-sold by cyber-thieves.

These stolen accounts were then used to buy “real goods” by the purchaser of the stolen account.

Many issues were identified in the account management systems for the website that made it trivial for an attacker to take over a valid user account.

Detailed recommendations and constant consultancy was provided to customer to improve all areas of the website.

# Ransomware – How it Works...



# “FBI Says Cryptowall Cost Victims \$18 Million Since 2014”



#### What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0.  
More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA\\_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

#### What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

#### How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.  
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.  
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

#### What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.  
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. <http://www.kqonlco02.be/44444444.com/111111>
2. <http://www.kqonlco02.be/44444444.com/111111>
3. <http://www.kqonlco02.be/44444444.com/111111>
4. <http://www.kqonlco02.be/44444444.com/111111>

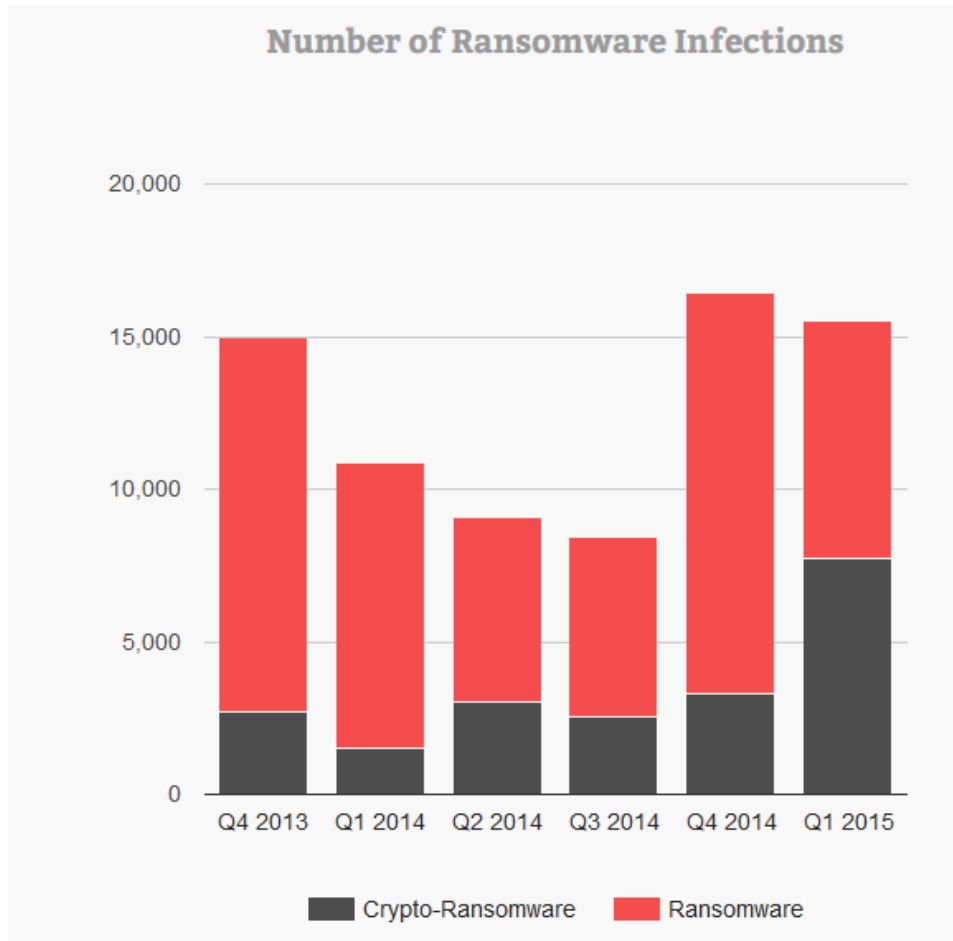
If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [www.kqonlco02.be/44444444.com/111111](http://www.kqonlco02.be/44444444.com/111111)
4. Follow the instructions on the site.

#### IMPORTANT INFORMATION:

Your Personal PAGE: <http://www.kqonlco02.be/44444444.com/111111>  
Your Personal PAGE(using TOR): [www.kqonlco02.be/44444444.com/111111](http://www.kqonlco02.be/44444444.com/111111)  
Your personal code (if you open the site (or TOR 's) directly): [111111](http://www.kqonlco02.be/44444444.com/111111)

## Growth of Ransomware



- Growth in ransomware use is massive and shows no sign of stopping
- Lots of copycats
- Little, if any risk of being caught
- Now available as a service...no coding required!

## ERS - International Bank....

### ■ Business challenge:


- The customer contacted IBM to help them with a malware outbreak that had encrypted over 500, 000 key office documents and other files.

### ■ Solution:

- IBM confirmed that the files had been encrypted.
- IBM confirmed that root cause was a new variant of CryptoWall that was using a Microsoft Word document file to bypass their security and when opened it downloaded a file (INFO.PNG) and renamed it to a random named .EXE file and finally executed it.
- This started a chain reaction, where the new EXE file contacted a web server which created a 2048 bit key pair. The PUBLIC key was downloaded to the infected system and then used to encrypt all local office documents and other files.
- Once finished on the local system, the malware started to encrypt files on remote shares and removable media.
- We managed to identify patient zero and how it bypassed their security controls.

### ■ Benefits:

- IBM performed a thorough analysis of the customer defences and identified weaknesses that needed to be fixed.
- IBM provided them with solutions that are not signature based, which would help stop a future infection, not only from new CryptoWall variant but also whole swathes of other malware (known and unknown).



**Bank staff were socially engineered into opening a booby-trapped Word document that then downloaded malware that encrypted files.**

**We identified the source and how it had bypassed their security controls and gave them “generic” methods to help stop a repeat attack.**



## So How Many Actually Pay Up?

- Recent survey carried out by the University of Kent found that a whopping 41% hit by ransomware, paid up!
- We know that the following organisations have paid to get their data back:
  - Tewksbury, Mass. police department was taken over by CryptoLocker and paid up
  - Midlothian, Ill. cops pay ransom
  - Lincoln County, Maine Sheriff's Office and four local police departments also fell victim to ransomware and paid up
  - Several Maine police agencies reported being hit by ransomware and paid up
- In some cases you can't even pay to get your data back...
  - Including backend databases powering web servers
  - Even whole disks/partitions encrypted



# Botnets

## ★ CITADEL BOTNET ★

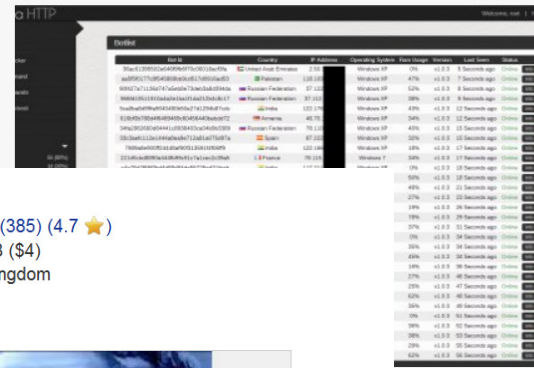
**Vendor** homodei (385) (4.7 ★)  
**Price** B0.01088 (\$4)  
**Ships from** United Kingdom  
**Escrow** Yes



### Product description

Citadel Trojan is malware created by a malicious code generating program. Citadel steal personal information, including banking and financial information, from its v Trojan, based on the Zeus source code, constructs a botnet consisting of a large computers. The attacker can execute malicious code on an infected computer, i and scareware.

## ATHENA BOTNET 1.08 PANEL + BUILDER



<b>Seller</b>	133ter (4.94/5 - 463)
<b>Price</b>	6 USD
<b>FE</b>	Yes
<b>Digital item</b>	Yes
<b>Currency</b>	Bitcoin
<b>Quantity</b>	1
<a href="#">Buy It Now</a>	

## ★ ZEUS BOTNET ★

**Vendor** homodei (385) (4.7 ★)  
**Price** B0.01088 (\$4)  
**Ships from** United Kingdom  
**Escrow** Yes

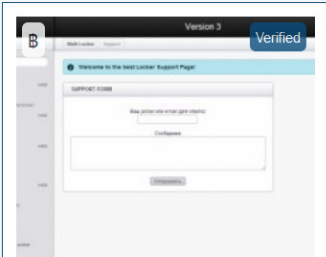


### Product description

Zeus, Zeus of Zbot is computer-malware die onder de categorie Trojaans paard (Trojan horse) valt. De trojan is gericht op computers die het Microsoft Windows-besturingssysteem gebruiken. Het is in staat om meerdere illegale taken uit te voeren en wordt meestal gebruikt om bankinformatie te stelen door middel van man-in-the-browser, keyloggers en form grabbing. Zeus wordt ook gebruikt om CryptoLocker-ransomware te installeren. Zeus wordt voornamelijk verspreid door drive-by-downloads en phishing. Het is voor het eerst geïdentificeerd in juli 2007 wanneer het gebruikt werd om informatie te stelen van het United States Department of Transportation [1] In juni 2009 ontdekte het beveiligingsbedrijf Prevx dat Zeus ondertussen meer dan 74.000 FTP-accounts op verschillende websites gecompromiteerd had.

# Ransomware & RATs

## Find item ransomware



**MULTILOCKER RANSOMWARE CUSTOMIZABLE**

17.58 USD

bluerave (4.96/5 - 514)

Digital item



**How The Russian Underground (Hacking...**

10 USD

Aracay (4.52/5 - 59)

Digital item



**Blackshades**

10 USD

DrPlatypus (4.88/5 - 104)

Digital item



\*\*\*\*Icon changer- change icon in a few...



\*\*\*\*Custom made/private keylogger \*\*\*...



**MULTILOCKER RANSOMWARE CUSTOMIZABLE -...**

## ★ Blackshades ★

**Vendor** homodei (385) (4.7 ★)

**Price** ₧0.01088 (\$4)

**Ships from** United Kingdom

**Escrow** Yes



## Product description

Blackshades is the name of a malicious trojan horse used by hackers to control computers remotely. The malware targets computers using Microsoft Windows-based operating systems. According to US officials, over 500,000 computer systems have been infected worldwide with the software.

Blackshades infects computer systems by downloading onto a victim's computer when the victim accesses a malicious webpage (sometimes downloading onto the victim's computer without the victim's knowledge, known as a drive-by download) or through external storage devices, such as USB flash drives.

Blackshades also included tools that assisted hackers in maximizing the amount of computer systems infected, such as a tool that sends infected links that masquerade as an innocuous site to other potential victims via the victim's social networking service.

Blackshades can reportedly be used remotely to access an infected computer without authorization.

# Skimmers

## BLUETOOTH GAS PUMP SKIMMER



**B5.89**

**\$2250**

Vendor  
damdev (12) (5.0 ★)

Ships from Escrow      worldwide  
Yes

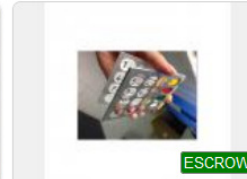
[View offer](#)



verifone offline skimmer  
software sdk and source c  
B0.1006



NCR PIN PAD PRODUCTION  
FILES 0.4FR4 PCB  
B0.272



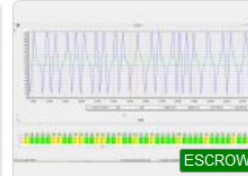
NCR SELFSEV PIN PAD STP  
FILES  
B0.1088



4x4 matrix keylogger for pin pad  
overlays product  
B0.34



VERIFONE MX850 OVERLAY  
PRODUCTION FILES STP  
AND SC  
B0.1224



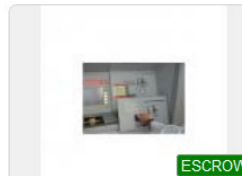
audio decode software  
mp3/wav track 2 and interupt  
B0.435



BLUETOOTH GAS PUMP  
SKIMMER  
B6.12



How to make an ATM skimmer-  
tutorial  
B0.01088



HOW TO MAKE AN ATM  
SKIMMER  
B0.00136

# Carding & Hacking

Carding service 30% 1 card for you! (USD)

**Vendor** nucleoide (46) (4.6 ★)  
**Price** ฿0.00449 (\$1)  
**Ships from** World Wide  
**Escrow** No



## Product description

--FE ONLY--

Hello, do you want a carding service? I can do that for you!

Benefits of my service:

- I use my drop address, it is safe for you
- I use my own hacked cards, you just need to worry on paying me and choose what do you want
- I am one of the few guys that can card from Amazon!!!

website Hacking services

**Vendor** apphacker (8) (5.0 ★)  
**Price** ฿1.339 (\$300)  
**Ships from** worldwide  
**Escrow** Yes



## Product description

Hacking services, depend of what you want we talk first on private message or wickr: apphacker

please order here, F.E.(finalize early) and send me specifications by chat.

the price here is for initial fee. to start working.

-----many questions about this listing so i am putting basic information here----

like lawyers, doctors, and any other professional, we charge an initial fee to check all work, make check for vulnerabilities and all the necessary steps in order to get to a conclusion. This takes a lot of patience and time depending on target. Also we do not do works against governments or any high private companies, we need to protect ourselves too.

in an exceptional case for finding information from states we do charge a very high price per service and very tight security is required between us and our client.

Hacked Paypal Accounts w/ Bank or Credit Card attached

**Vendor** nucleoide (46) (4.6 ★)  
**Price** ฿0.0359 (\$8)  
**Escrow** No



## Product description

Hello, I am a new vendor, and I am making this so cheap because I need good reviews, sure, if the sellings stay high I am sure going to keep this, PAYPAL ACCOUNTS FOR ONLY 8 DOLLARS!

ALERT, DO NOT BUY MORE THAN 4 UNITS, I HAVE LOW STOCK, AS THE DEMAND GROWS I BUY MORE AND UPDATE THIS, BUY LESS THAN 4 PP ACCOUNTS, YOU ARE ADVISED!

The accounts are all good, balance is 0, but they do work, I checked them by myself and they do work.

# Bank Accounts & Fullz

*pnc bank login details + info*

**Vendor** smoothhydra (2) (3.0 ★)  
**Price** B0.0314 (\$7)  
**Ships from** Worldwide  
**Escrow** No



## Product description

I have a number of USA pnc bank login details for sale. Low and medium balance. for a custom listing based on balance you need.

## UK Identity Set ( Passport+Bill+Statment+CC+NI) Cu



## ULTRA High Quality UNITED KINGDOM Fullz

**Vendor** JamrockFille (169) (4.9 ★) ✓  
**Price** B0.003868 (£1)  
**Ships to** Worldwide, Worldwide  
**Ships from** Kingston  
**Escrow** No



## Product description

IN STOCK NOW  
ALL CARDS ARE FRESH, NEVER RESOLD  
SAME PREMIUM QUALITY  
FORMAT WILL DEPEND ON SUPPLIER (ALWAYS QUALITY TESTED)  
-----

**B0.0136**

**\$5**

**Vendor** Kingscan (64) (5.0 ★) (📞 38/0/1)  
(👤 150, 5/5) (📧 44/1/0)

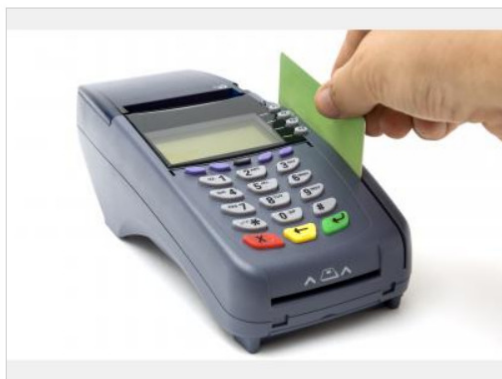
**Ships to** Worldwide, Worldwide  
**Ships from** Internet  
**Escrow** Yes

[View offer](#)

# Others, and then there's drugs, guns, porn, etc.

5 ATM hacks, cashout ALL ATM MACHINES, earn money

**Vendor** nucleoide (46) (4.6 ★)  
**Price** B0.01348 (\$3)  
**Escrow** No



## Product description

In this method you will learn 5 ATM hacks, learn how to go to any ATM machine and get all the money inside it discretely, fast and easy.

Great information is not free, this method is tested and working!  
 Cashout an ATM in less than 2 minutes!

Custom Physical Employee Cards / Any Company / Alte

**Vendor** Kingscan (64) (5.0 ★) (📅 38/0/1) (👤 150, 5/5)  
 (@ 44/1/0)  
**Price** B0.204 (\$75)  
**Ships to** Worldwide, Worldwide  
**Ships from** WW  
**Escrow** Yes



## Product description

This Listing for Physical Employee ID Card / Access Card / or any such PVC Card.

Please provide the below information:

Employee Number:  
 Employee Name:  
 Employee Position/Title:  
 Expiry:

Company Name/Logo: Optional

50000 bitcoin private keys

**Vendor** nucleoide (298) (4.7 ★) 🛡️  
**Price** B0.0562 (\$21.5)  
**Escrow** Yes



## Product description

Bitcoin private key is another meaning of password to bitcoin wallet, I took these keys from database, just like lotto, i can't guarantee what inside and how much you will find, All i can guarantee is that they all fresh and I did not used them! All orders are final!

Good luck!

Also take a look at our guide on how to recover those bitcoin keys check our guide:

<http://txocqh4nwkofil.onion/viewProduct?offer=151879.60928>

## Conclusions and Recommendations – Dark Web

- Monitor all network traffic for outbound TOR connections
  - Including TOR proxies
  - This will allow you to identify staff using TOR on your network and may be indicative of a ransomware attack
- Block TOR exit nodes
  - There are public lists available for these, so null-route (blackhole) them or use proxy/url filtering/reputational analysis to monitor or block them.
- Understand what the “Dark Web” might contain and how this may affect your company, brand(s), products, services, etc.
  - Especially important that you check to see if accounts for your organisation or services you offer are being sold (either stolen accounts or fresh accounts/digital products, etc.
- Education, education, education!
  - Backed up with policies clearly stating that TOR and other P2P software is not approved for use, same with BitCoin mining!



## Conclusions and Recommendations - Ransomware

- There is NO 100% solution, no Silver Bullet!
- However there are things you can do to help minimise a repeat:
  - Train staff (and regularly test them)
  - Use software restriction policies, or AppLocker
  - Improve URL and email filtering (anti-spam, reputational checks, blacklists, etc.) as well as checking to see if the Message-ID has a valid FULL domain name
  - Use multiple AV engines to scan all e-mail and web content
  - Set up a dedicated reporting email address and monitor it
  - Harden systems, reduce rights, disable macros (unless signed or on a whitelist)
  - Make your security policy and internet usage policy clearer and enforce it...
  - Take regular backups (not to network connected servers or cloud) – Off-site/Off-line is best.
- Things NOT to do – Pay up, as it validates the bad guys business model...Don't join the 41% that do pay up!



## Conclusions and Recommendations – DDoS & DDoS Ransom

- There is NO 100% solution, no Silver Bullet!
- However there are things you can do to help ride the storm:
  - Use a CDN (Content Delivery Network) that offers DDoS protection
  - Use a Scrubbing service (when under attack) to help reduce the impact
  - Use a Web Application Firewall to help protect against application level (Layer 7) attacks
  - Harden systems against floods, especially SYN
  - Drop Internet packets for services you are not using or expecting (NTP, DNS, UPnP, PingBack/TrackBack, SNMP, etc.) These are often used for reflection attacks
- Things NOT to do – Pay up, as you will be more likely to be targeted again and it validates the bad guys business model...



**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

# THANK YOU

[www.ibm.com/security](http://www.ibm.com/security)



## IBM Security

Intelligence. Integration. Expertise.

© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

## IBM Research Links

- Dangers of the deep, dark web
  - <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&htmlfid=SEL03035USEN&attachment=SEL03035USEN.PDF>
- What surfaces from the deep, dark web
  - <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&htmlfid=SEL03043USEN&attachment=SEL03043USEN.PDF>



## Contact Information

### **Martin Overton**

IBM CSIRT

(Office) +44 (0)2392 563442

(Mobile) +44 (0)7764 666939

[overtonm@uk.ibm.com](mailto:overtonm@uk.ibm.com)

Twitter @martin\_sec, also on LinkedIn, Xing, etc.

**ERS 24x7 Hotline : UK: +44 (0)203 6844872**



**The (cyber)storm is coming. ARE YOU READY?**

Emergency? Call: (US) +1.888.241.9812 | (WW) +1.312.212.8034  
Or get started with a [penetration test](#) & [incident response planning](#)