WHAT LURKS ON THE DARKWEB

Chris Patteson
Executive Director – Risk Transformation Office

Chris Patteson

Executive Director - Risk Transformation Office

in https://www.linkedin.com/in/cpat13/

Chris Patteson has over 20 years of experience as a leader, practitioner, and innovator within GRC and Integrated Risk Management (IRM) in the manufacturing/logistics, technology and logistics sectors.

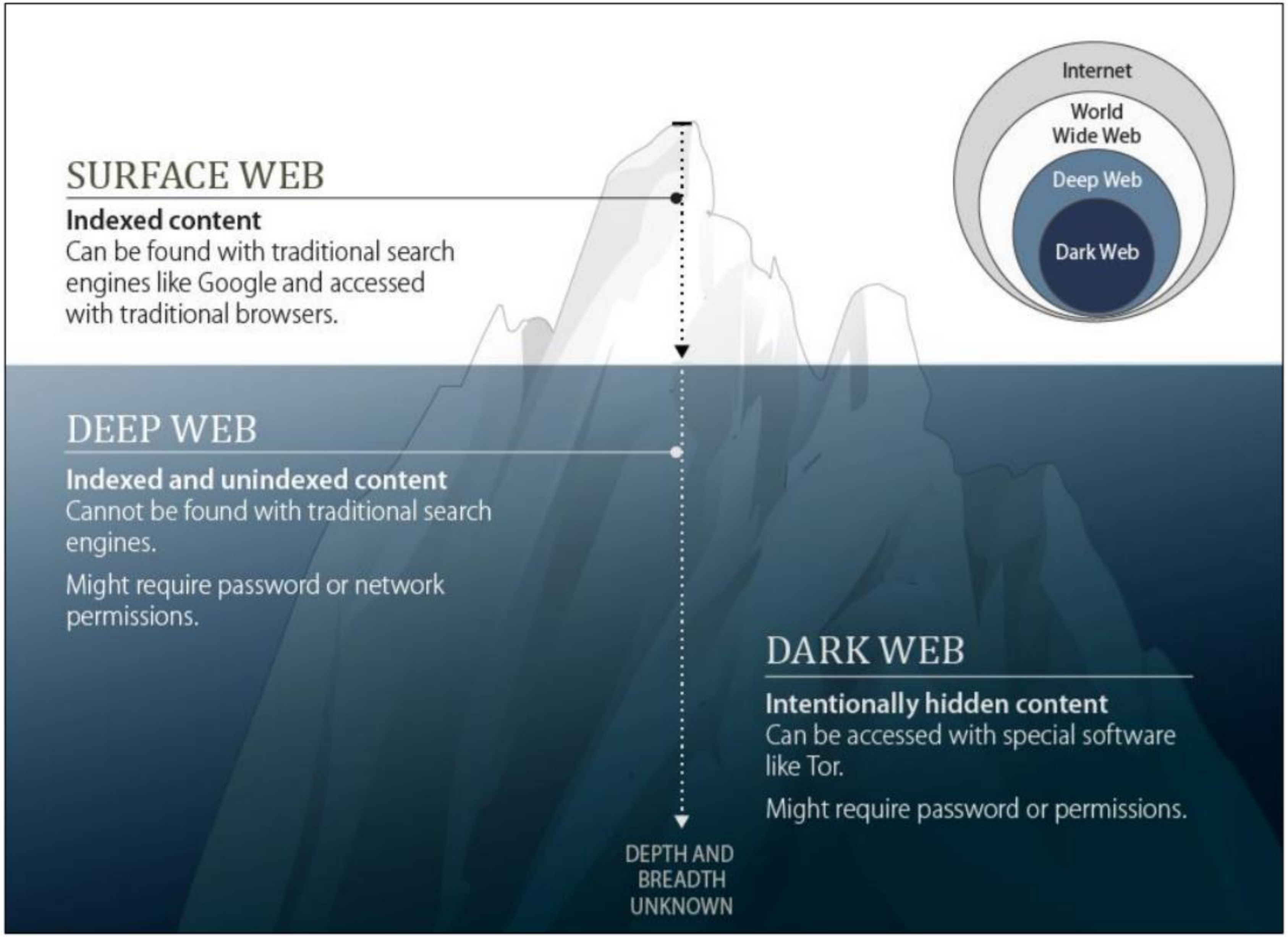
- Executive responsible for IRM with a leading global logistics corporation
- Led data sciences and automation organization in developing new models, methods and architectures in fraud management and cargo security risk
- Led global research and strategy development for emerging global transportation models
- Drove Integrated Risk Management transformation to improve adherence and reporting of compliance gaps

Chris' current research lies in security architectures related to risk systems and risk data science. His work led to a patent for Methods, Systems, and Devices for Detecting and Isolating Device Posing Security Threats.

Chris holds a bachelor's degree in Industrial Engineering from University of Tennessee and an MBA from Christian Brothers University.

Chris leads **Industrials and Technology** for the Risk Transformation Office.

WHAT ARE WE TALKING ABOUT..



SURFACE WEB

Indexed content
Can be found with traditional search engines like Google and accessed with traditional browsers.

DEEP WEB

Indexed and unindexed content
Cannot be found with traditional search engines.

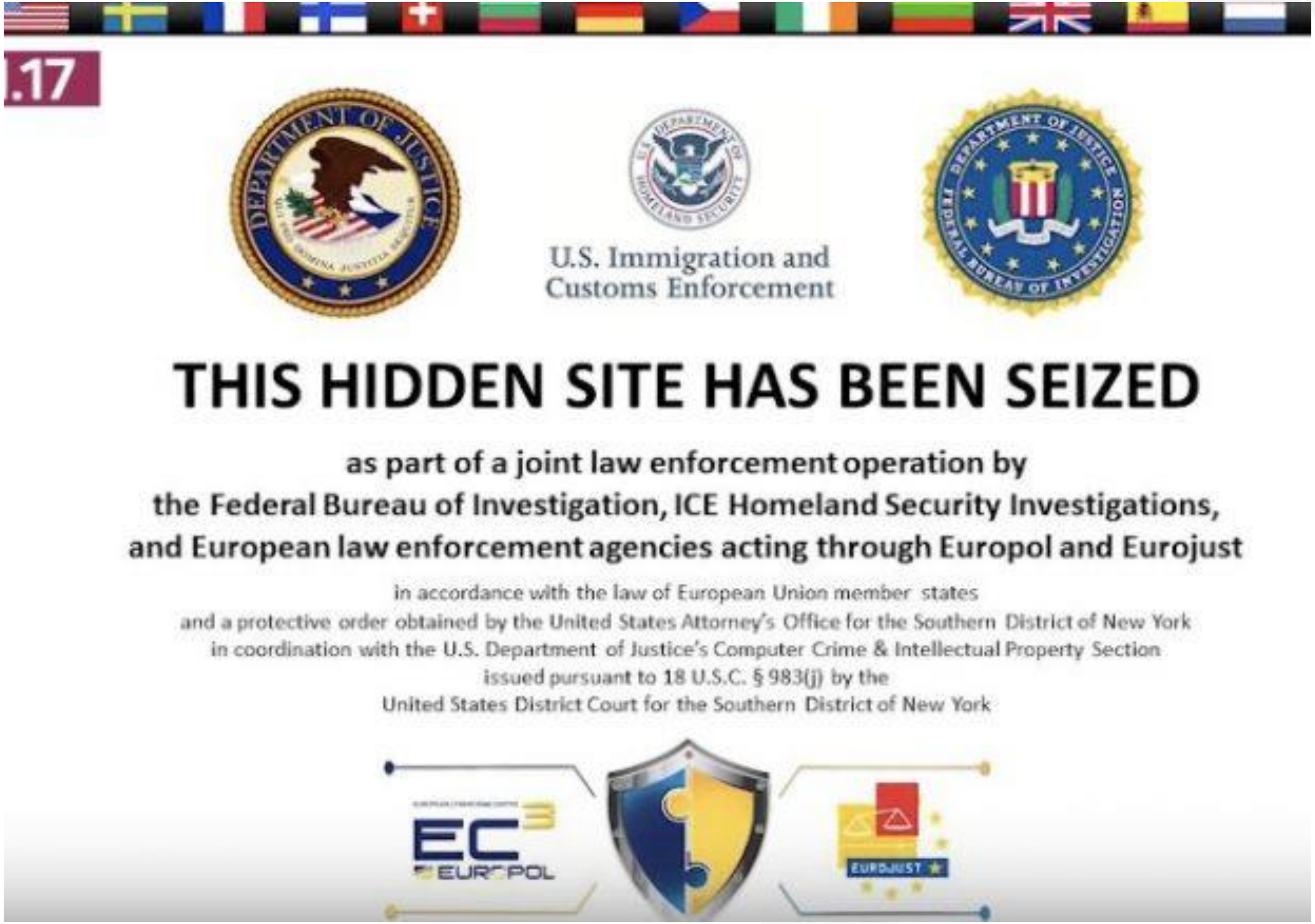
Might require password or network permissions.

DARK WEB

Intentionally hidden content
Can be accessed with special software like Tor.

Might require password or permissions.

Congressional Research Service – www.crs.gov

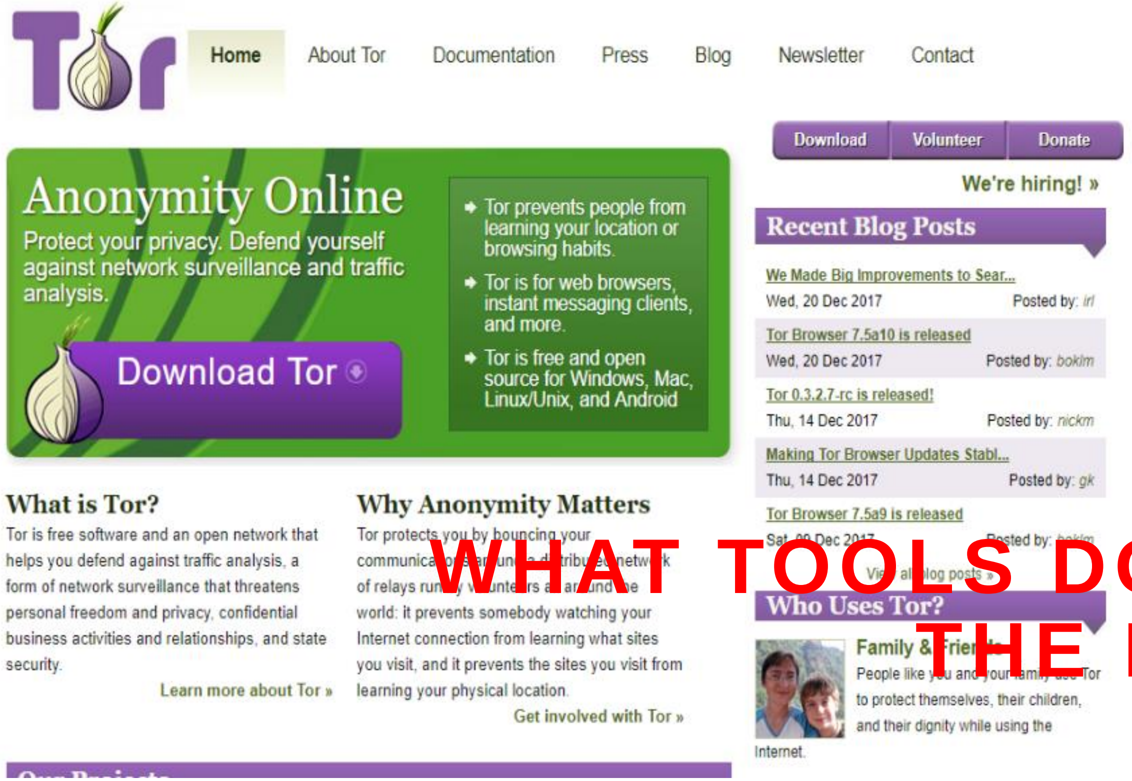


THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

WHAT TOOLS DO I NEED TO EXPLORE THE DARK WEB?



Home | About Tor | Documentation | Press | Blog | Newsletter | Contact

Download | Volunteer | Donate

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

We're hiring! »

Recent Blog Posts

We Made Big Improvements to Sear...
Wed, 20 Dec 2017 Posted by: irl

Tor Browser 7.5a10 is released
Wed, 20 Dec 2017 Posted by: boklm

Tor 0.3.2.7-rc is released!
Thu, 14 Dec 2017 Posted by: nickm

Making Tor Browser Updates Stabl...
Thu, 14 Dec 2017 Posted by: gk

Tor Browser 7.5a9 is released
Sat, 09 Dec 2017 Posted by: boklm

View all blog posts »

What is Tor?

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Learn more about Tor »

Why Anonymity Matters

Tor 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, and it prevents the sites you visit from learning your physical location.

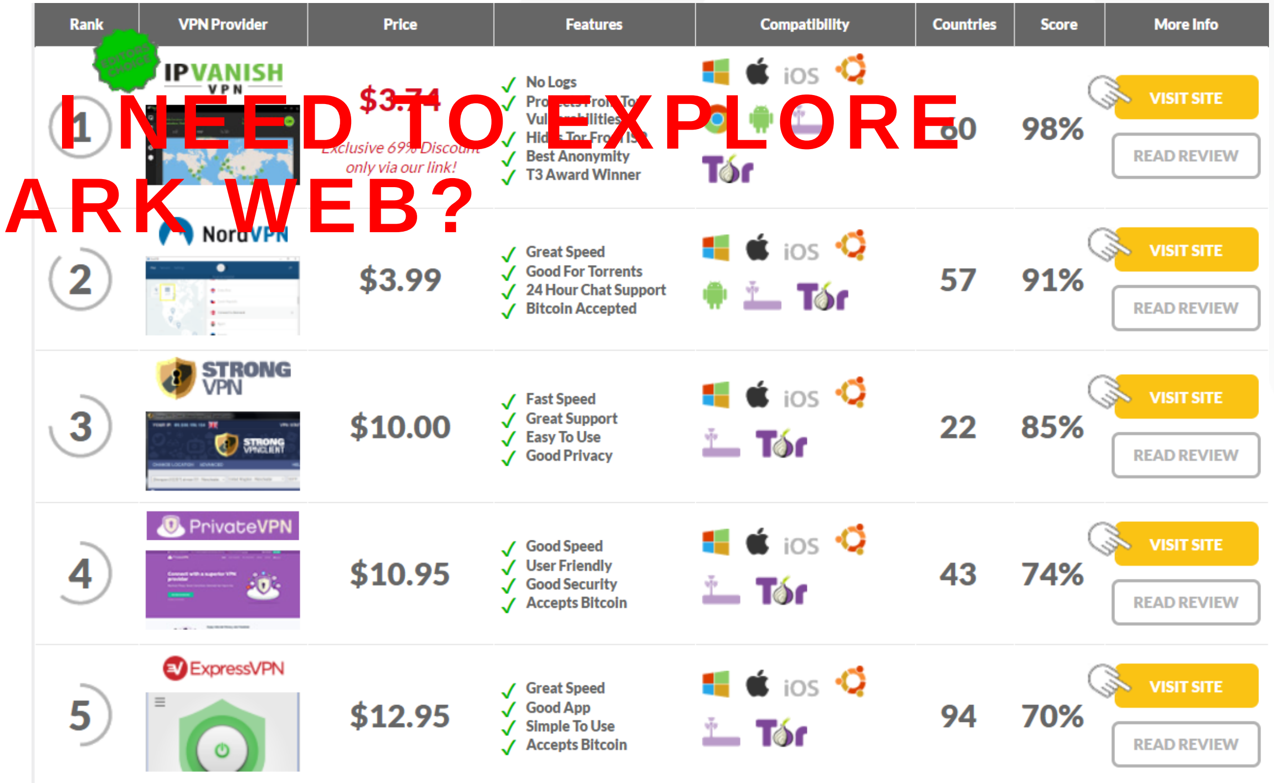
Get involved with Tor »

Who Uses Tor?

Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.

Our Projects

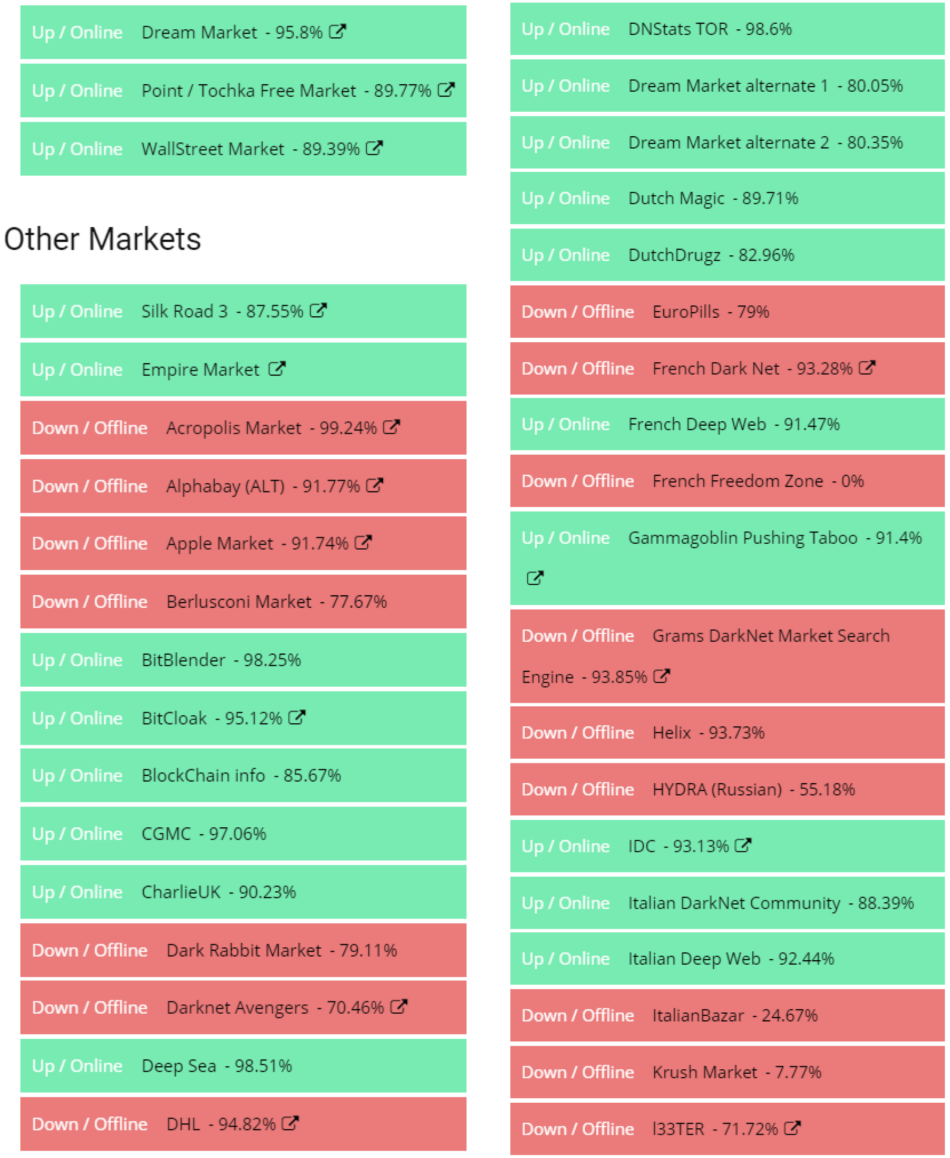


Rank	VPN Provider	Price	Features	Compatibility	Countries	Score	More Info
1	EDITORS CHOICE IPVANISH VPN	~~$3.74~~ Exclusive 69% Discount only via our link!	✓ No Logs ✓ Protects From Tor Vulnerabilities ✓ Hides Tor From ISP ✓ Best Anonymity ✓ T3 Award Winner	iOS Tor	60	98%	VISIT SITE READ REVIEW
2	NordVPN	$3.99	✓ Great Speed ✓ Good For Torrents ✓ 24 Hour Chat Support ✓ Bitcoin Accepted	iOS Tor	57	91%	VISIT SITE READ REVIEW
3	STRONG VPN	$10.00	✓ Fast Speed ✓ Great Support ✓ Easy To Use ✓ Good Privacy	iOS Tor	22	85%	VISIT SITE READ REVIEW
4	PrivateVPN	$10.95	✓ Good Speed ✓ User Friendly ✓ Good Security ✓ Accepts Bitcoin	iOS Tor	43	74%	VISIT SITE READ REVIEW
5	ExpressVPN	$12.95	✓ Great Speed ✓ Good App ✓ Simple To Use ✓ Accepts Bitcoin	iOS Tor	94	70%	VISIT SITE READ REVIEW

VPN Tips

- Must have high grade encryption
- Hides logs

WHAT IS YOUR DESTINATION



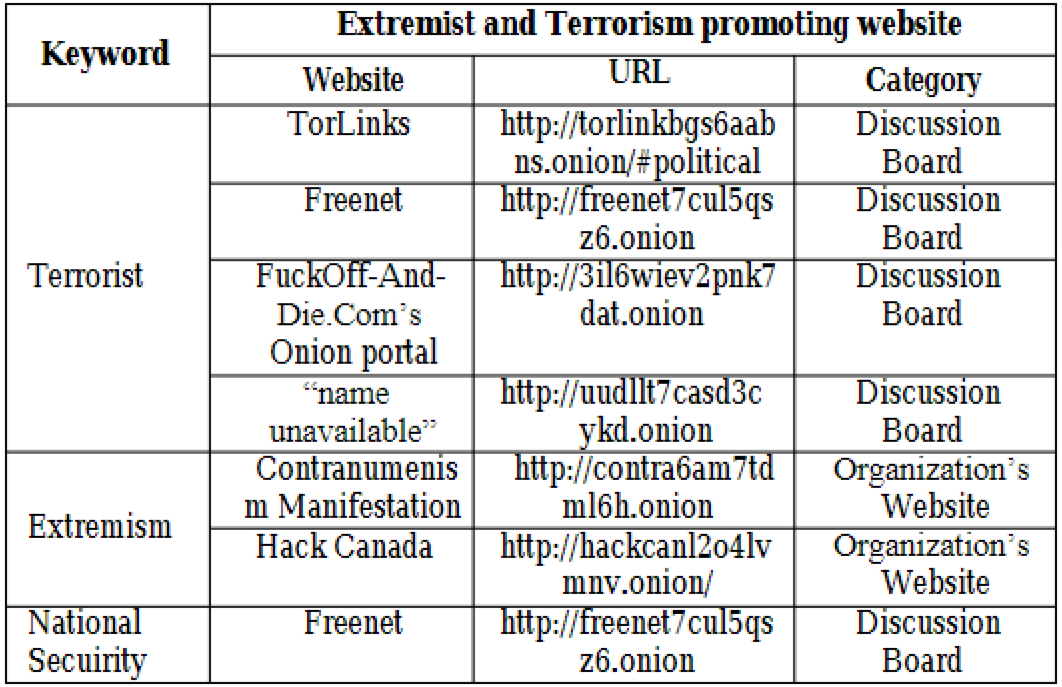
Top Markets

Up / Online	Dream Market - 95.8%
Up / Online	Point / Tochka Free Market - 89.77%
Up / Online	WallStreet Market - 89.39%

Other Markets

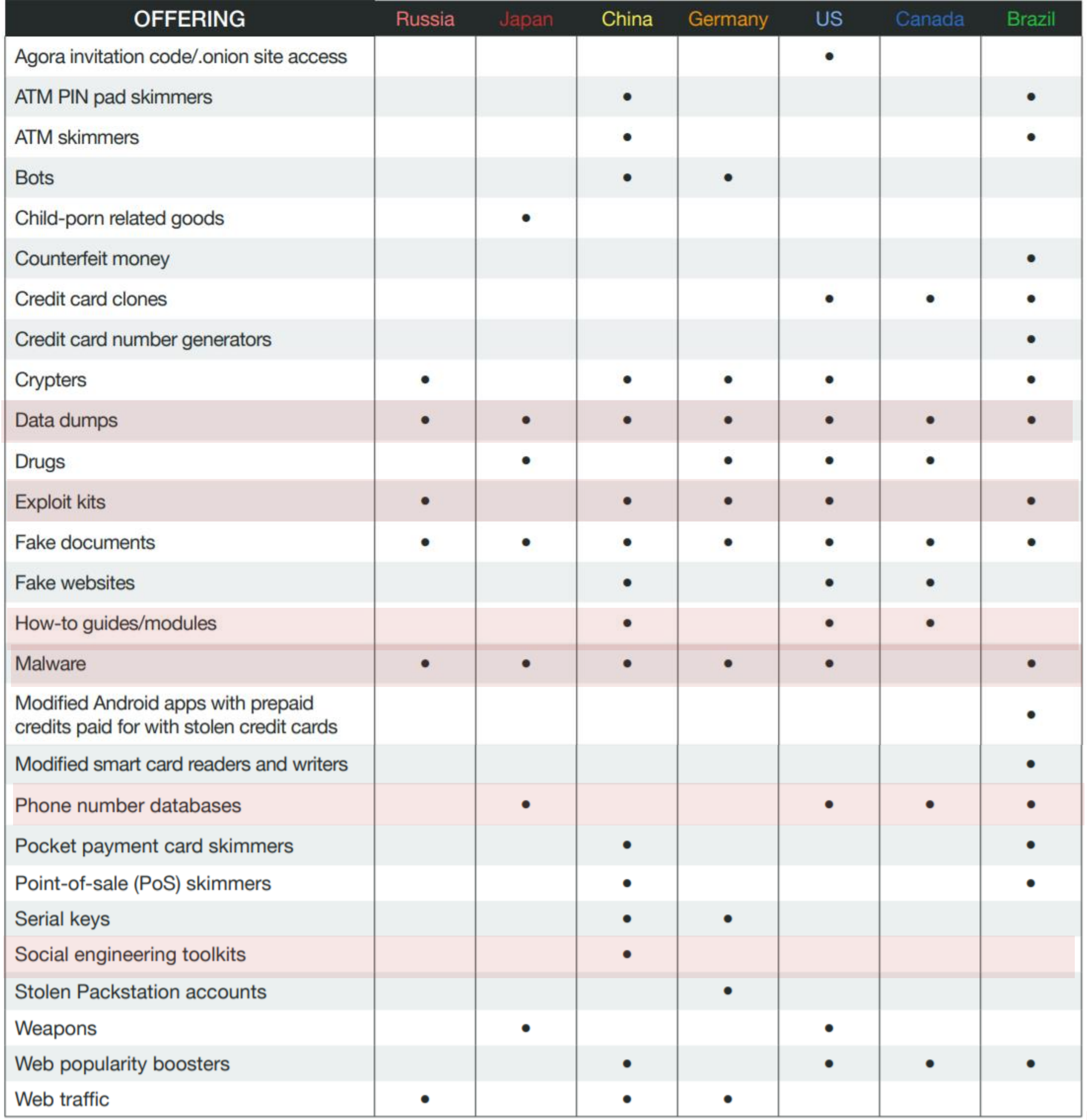
Up / Online	Silk Road 3 - 87.55%
Up / Online	Empire Market
Down / Offline	Acropolis Market - 99.24%
Down / Offline	Alphabay (ALT) - 91.77%
Down / Offline	Apple Market - 91.74%
Down / Offline	Berlusconi Market - 77.67%
Up / Online	BitBlender - 98.25%
Up / Online	BitCloak - 95.12%
Up / Online	BlockChain info - 85.67%
Up / Online	CGMC - 97.06%
Up / Online	CharlieUK - 90.23%
Down / Offline	Dark Rabbit Market - 79.11%
Down / Offline	Darknet Avengers - 70.46%
Up / Online	Deep Sea - 98.51%
Down / Offline	DHL - 94.82%
Up / Online	DNStats TOR - 98.6%
Up / Online	Dream Market alternate 1 - 80.05%
Up / Online	Dream Market alternate 2 - 80.35%
Up / Online	Dutch Magic - 89.71%
Up / Online	DutchDrugz - 82.96%
Down / Offline	EuroPills - 79%
Down / Offline	French Dark Net - 93.28%
Up / Online	French Deep Web - 91.47%
Down / Offline	French Freedom Zone - 0%
Up / Online	Gammagoblin Pushing Taboo - 91.4%
Down / Offline	Grams DarkNet Market Search Engine - 93.85%
Down / Offline	Helix - 93.73%
Down / Offline	HYDRA (Russian) - 55.18%
Up / Online	IDC - 93.13%
Up / Online	Italian DarkNet Community - 88.39%
Up / Online	Italian Deep Web - 92.44%
Down / Offline	ItalianBazar - 24.67%
Down / Offline	Krush Market - 7.77%
Down / Offline	I33TER - 71.72%

Darkwebnews.com

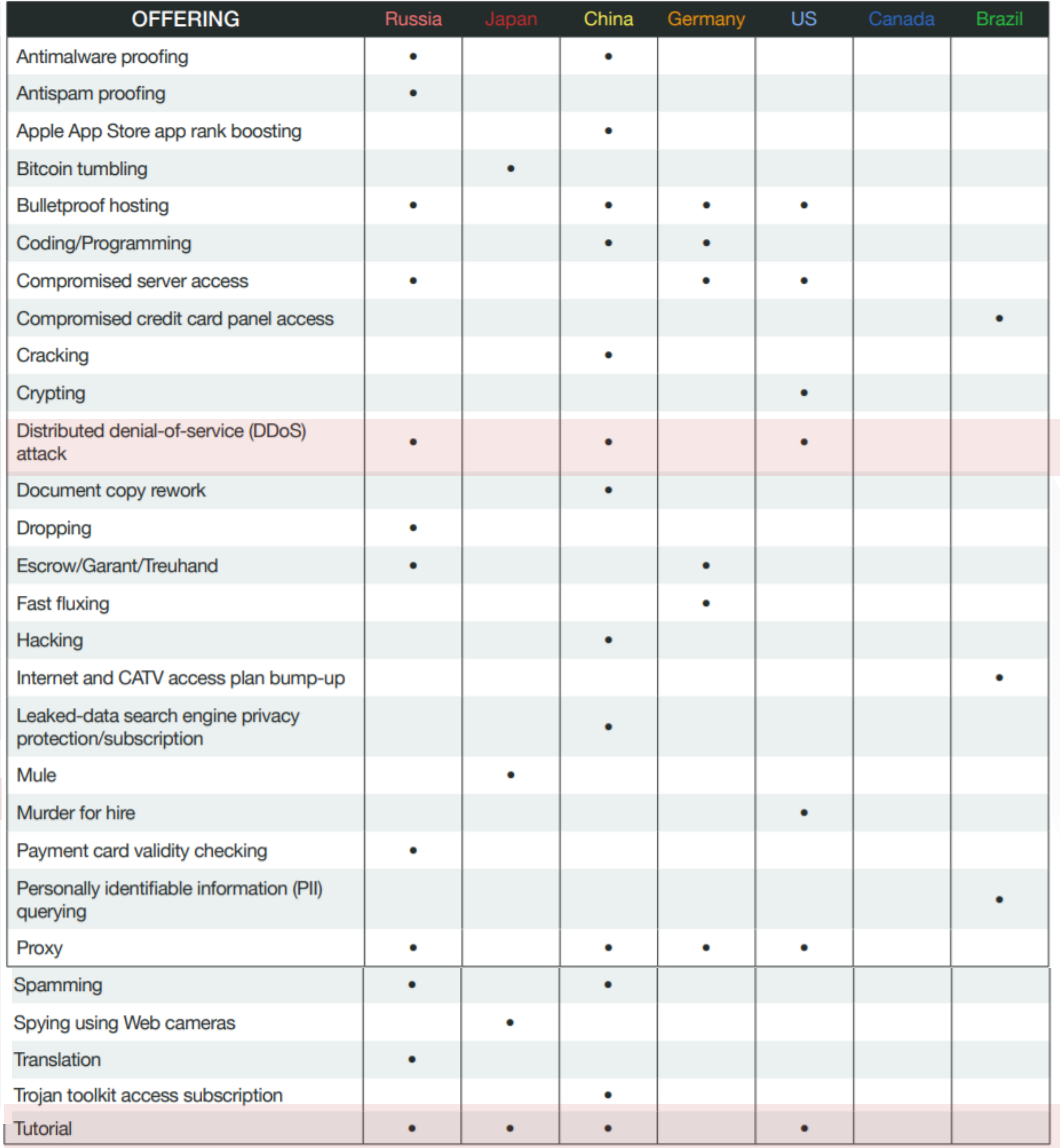


Keyword	Extremist and Terrorism promoting website		
	Website	URL	Category
Terrorist	TorLinks	http://torlinkbgs6aabns.onion/#political	Discussion Board
	Freenet	http://freenet7cul5qsz6.onion	Discussion Board
	FuckOff-And-Die.Com's Onion portal	http://3il6wiev2pnk7dat.onion	Discussion Board
	"name unavailable"	http://uudllt7casd3cykd.onion	Discussion Board
Extremism	Contranumenism Manifestation	http://contra6am7tdml6h.onion	Organization's Website
	Hack Canada	http://hackcanl2o4lvmnv.onion/	Organization's Website
National Secuirity	Freenet	http://freenet7cul5qsz6.onion	Discussion Board

Surfacing Collaborated Networks in Dark Web to
find Illicit and Criminal Content - International Cyber Crime Research Center (ICCRC)
School of Criminology, Simon Fraser University



OFFERING	Russia	Japan	China	Germany	US	Canada	Brazil
Agora invitation code/.onion site access					●		
ATM PIN pad skimmers			●				●
ATM skimmers			●				●
Bots			●	●			
Child-porn related goods		●					
Counterfeit money							●
Credit card clones					●	●	●
Credit card number generators							●
Crypters	●		●	●	●		●
Data dumps	●	●	●	●	●	●	●
Drugs		●		●	●	●	
Exploit kits	●		●	●	●		●
Fake documents	●	●	●	●	●	●	●
Fake websites			●		●	●	
How-to guides/modules			●		●	●	
Malware	●	●	●	●	●		●
Modified Android apps with prepaid credits paid for with stolen credit cards							●
Modified smart card readers and writers							●
Phone number databases		●			●	●	●
Pocket payment card skimmers			●				●
Point-of-sale (PoS) skimmers			●				●
Serial keys			●	●			
Social engineering toolkits			●				
Stolen Packstation accounts				●			
Weapons		●			●		
Web popularity boosters			●		●	●	●
Web traffic	●		●	●			



OFFERING	Russia	Japan	China	Germany	US	Canada	Brazil
Antimalware proofing	●		●				
Antispam proofing	●						
Apple App Store app rank boosting			●				
Bitcoin tumbling		●					
Bulletproof hosting	●		●	●	●		
Coding/Programming			●	●			
Compromised server access	●			●	●		
Compromised credit card panel access							●
Cracking			●				
Crypting					●		
Distributed denial-of-service (DDoS) attack	●		●		●		
Document copy rework			●				
Dropping	●						
Escrow/Garant/Treuhand	●			●			
Fast fluxing				●			
Hacking			●				
Internet and CATV access plan bump-up							●
Leaked-data search engine privacy protection/subscription			●				
Mule		●					
Murder for hire					●		
Payment card validity checking	●						
Personally identifiable information (PII) querying							●
Proxy	●		●	●	●		
Spamming	●		●				
Spying using Web cameras		●					
Translation	●						
Trojan toolkit access subscription			●				
Tutorial	●	●	●		●		

TOOLS OF THE TRADE / CYBER CRIME AS A SERVICE

HACKING TOOLS & SERVICES	
Account Hacking Program	$12.99 (See more details on page 10)
Hacked Instagram Accounts in Bulk	1,000 - 10,000 accounts $15 - $60
Botnet: Blow-Bot Banking Botnet	Monthly Basic Rental $750 | Monthly Full Rental $1,200 | Monthly Support $150
Disdain Exploit Kit	Day $80, Week $500, Month $1,400
Stegano Exploit Kit: Chrome , FireFox, Internet Explorer, Opera, Edge	Unlimited Traffic, Day $2,000 Unlimited Traffic, Month $15,000
Microsoft Office Exploit Builder	Lite exploit builder $650 Full Version $1,000
WordPress Exploit	$100

HACKING TOOLS & SERVICES	
Password Stealer	$50
Android Malware Loader	$1,500
Western Union Hacking Bug For World Wide Transfer	$300
DDoS Attacks	Week long attack $500 - $1,200
ATM Skimmers: Wincor, Slimm, NCR, Diebold	$700 - $1,500
Hacking Tutorials	Multiple Tutorials $5 - $50

YOU CAN DDoS AN ORGANIZATION FOR

$10 HOUR

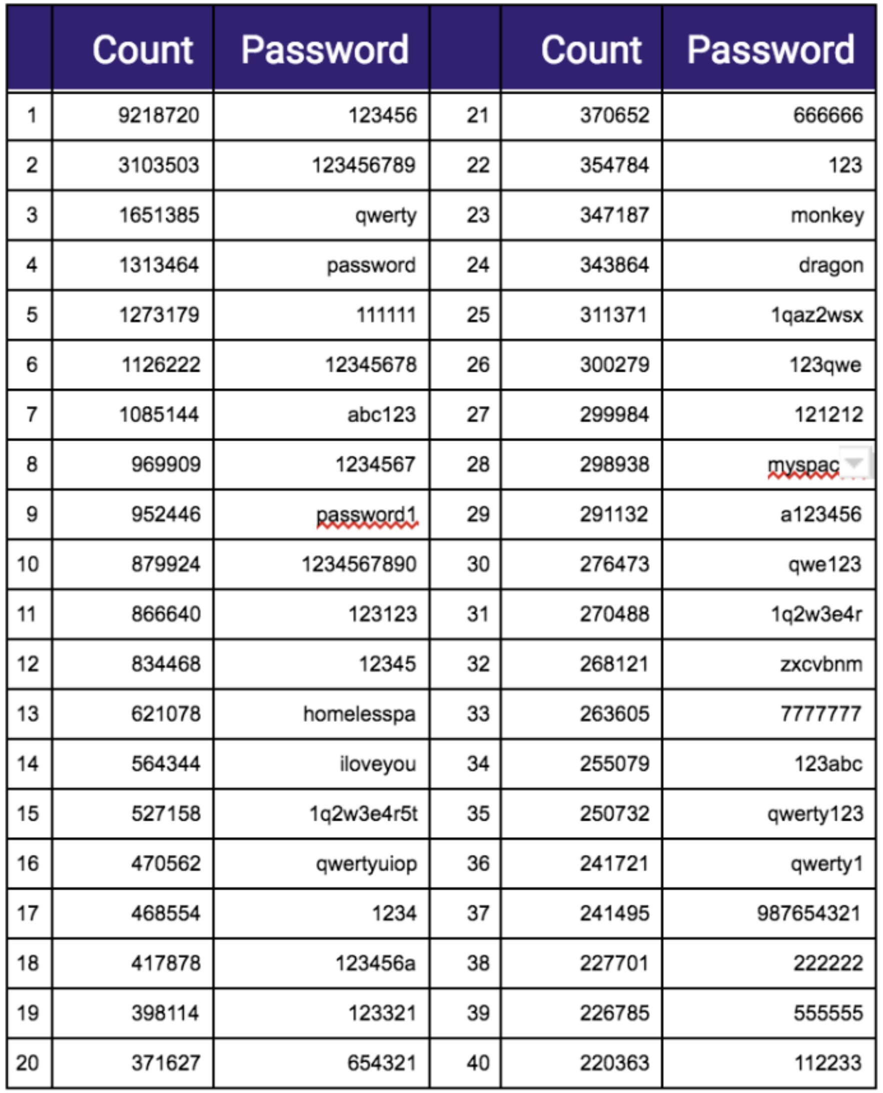
$200 DAY

84% of 1,010 organizations surveyed in a 2017 report had experienced at least one DDoS attack in the previous 12 months, and 86% of those attacked dealt with more than one during that period.

Amor Black Market Report 2018

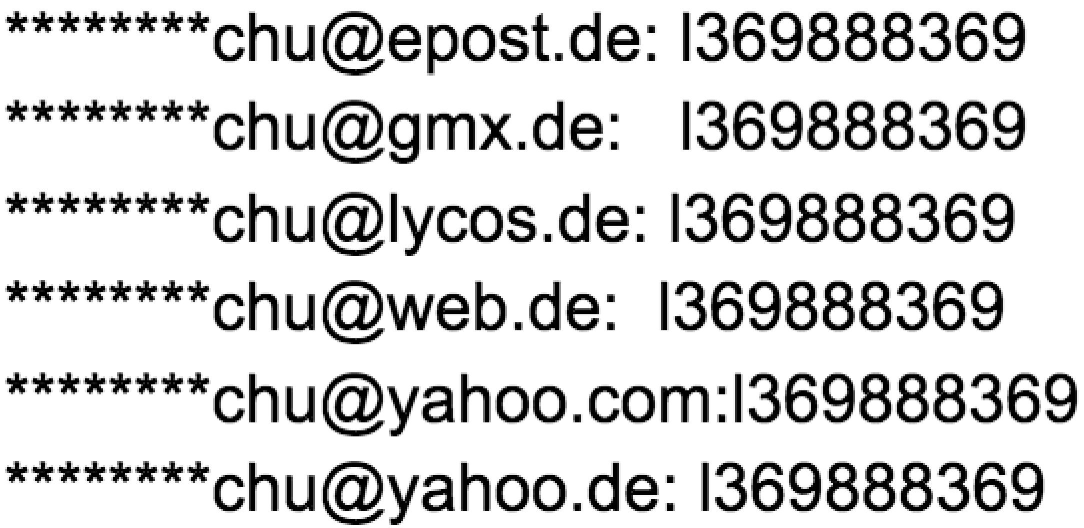
PASSWORD STUFFING

1.4 Billion Clear Text Credentials Discovered in a Single Database – 4iQ Analysis



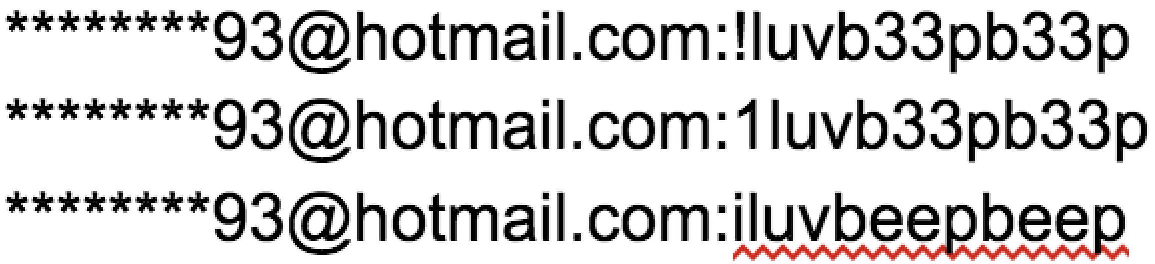
	Count	Password		Count	Password
1	9218720	123456	21	370652	666666
2	3103503	123456789	22	354784	123
3	1651385	qwerty	23	347187	monkey
4	1313464	password	24	343864	dragon
5	1273179	111111	25	311371	1qaz2wsx
6	1126222	12345678	26	300279	123qwe
7	1085144	abc123	27	299984	121212
8	969909	1234567	28	298938	myspac
9	952446	password1	29	291132	a123456
10	879924	1234567890	30	276473	qwe123
11	866640	123123	31	270488	1q2w3e4r
12	834468	12345	32	268121	zxcvbnm
13	621078	homelesspa	33	263605	7777777
14	564344	iloveyou	34	255079	123abc
15	527158	1q2w3e4r5t	35	250732	qwerty123
16	470562	qwertyuiop	36	241721	qwerty1
17	468554	1234	37	241495	987654321
18	417878	123456a	38	227701	222222
19	398114	123321	39	226785	555555
20	371627	654321	40	220363	112233

Repetition



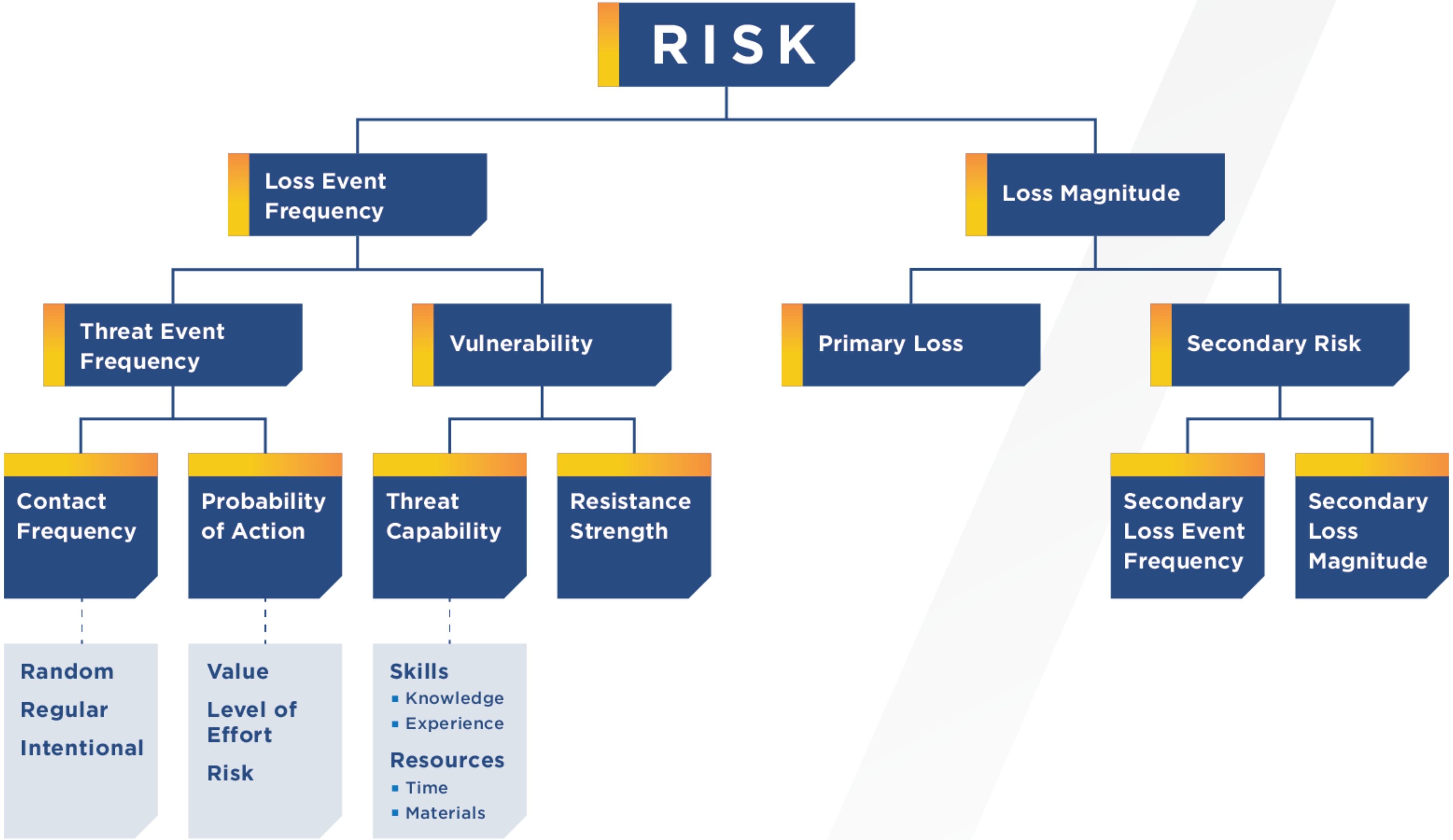
```
********chu@epost.de: l369888369
********chu@gmx.de:   l369888369
********chu@lycos.de: l369888369
********chu@web.de:  l369888369
********chu@yahoo.com:l369888369
********chu@yahoo.de: l369888369
```

Simple Patterns



```
********93@hotmail.com:!luvb33pb33p
********93@hotmail.com:1luvb33pb33p
********93@hotmail.com:iluvbeepbeep
```

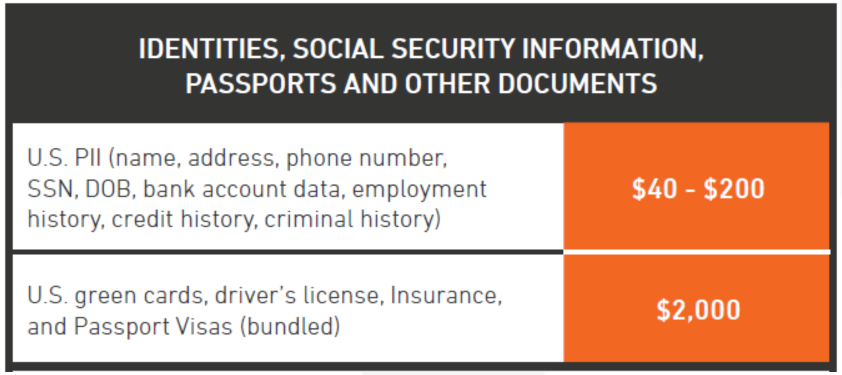
THE FAIR MODEL



THREAT COMMUNITIES

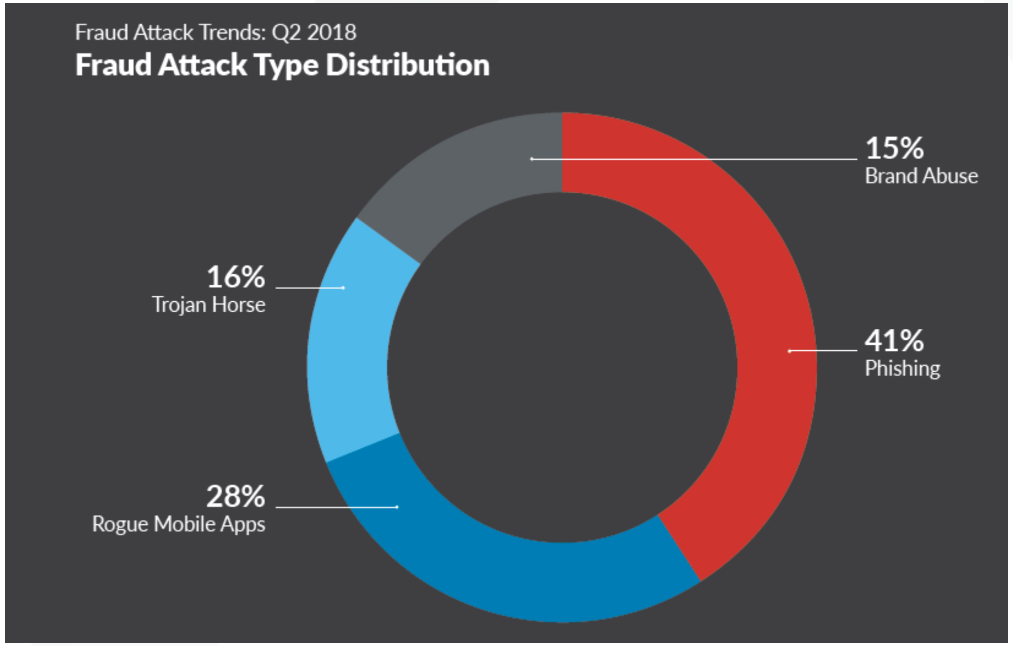
ORGANIZED RETAIL CRIME-IDENTITY THEFT /BEC

- Factors
  - Global in nature, complex business models
  - Identity theft, PII
  - Emerging data protection laws (compliance risk)
  - Identities are used to fraud financial institutions, retailers, airlines, etc.
  - Business Email Compromise (BEC) targets the organization directly
  - Credential Stuffing
- Loss magnitude
  - Levees and fines from regulatory agencies
  - Credit / Fraud reporting
  - Forensics services
  - Litigation / Legal Services
  - Lost Revenue (esp BEC)



IDENTITIES, SOCIAL SECURITY INFORMATION, PASSPORTS AND OTHER DOCUMENTS	
U.S. PII (name, address, phone number, SSN, DOB, bank account data, employment history, credit history, criminal history)	$40 - $200
U.S. green cards, driver's license, Insurance, and Passport Visas (bundled)	$2,000

Amor Black Market Report 2018



RSA Fraud Risk Intelligence - Q2 1028

THREAT COMMUNITIES

REGULATORS-IDENTITY THEFT

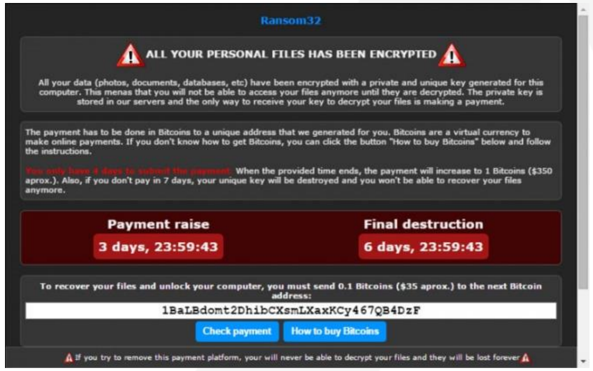
2018 Updates on the heels of GDPR

- **Alabama (SB 318)** – ***Alabama passes its first data breach notification law.***
- **Arizona (HB 2145)** – ***Arizona updates its breach notification law to expand the definition of personal information and tighten notification timelines, among other things.***
- **Colorado (HB 1128)** – ***Colorado strengthens consumer protections by requiring formal information security policies as well as increased oversight of third parties.***
- **Iowa (HF 2354)** – ***Iowa passes legislation regulating online services and mobile apps for students***.
- **Louisiana (Act. No. 382)** – ***Louisiana amends its data breach law.***
- **Nebraska (LB 757)** – ***Nebraska enacts requirement to maintain reasonable security practices and procedures and flow down those obligations to third parties.***
- **Oregon (SB 1551)** – ***Oregon amends its breach notification rules***.
- **South Carolina (H4655)** – ***South Carolina imposes heightened breach notification and security requirements on the insurance industry.***
- **South Dakota (SB No. 62) –** ***South Dakota enacts its first data breach notification law***
- **Vermont (H. 764)** – ***Vermont passes legislation to regulate data brokers***.
- **Virginia (HB 183)** – ***Virginia amends its breach notification law to include income tax information.***

THREAT COMMUNITIES

ORGANIZED CRIME- RANSOMWARE

- Factors
  - May be the act of as few as 100 to 200 running cybercrime as a service
  - Financially Lucrative with little chance of arrest
  - Trend Micro reported seeing 79 new ransomware families in 2016, compared to 29 new ransomware families in all of 2015
- Loss magnitude
  - Paid ransom (Bitcoin)
  - Forensics services
  - Litigation / Legal Services



Ransom32

ALL YOUR PERSONAL FILES HAS BEEN ENCRYPTED

All your data (photos, documents, databases, etc) have been encrypted with a private and unique key generated for this computer. This menas that you will not be able to access your files anymore until they are decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is making a payment.

The payment has to be done in Bitcoins to a unique address that we generated for you. Bitcoins are a virtual currency to make online payments. If you don't know how to get Bitcoins, you can click the button "How to buy Bitcoins" below and follow the instructions.

You only have 4 days to submit the payment. When the provided time ends, the payment will increase to 1 Bitcoins ($350 aprox.). Also, if you don't pay in 7 days, your unique key will be destroyed and you won't be able to recover your files anymore.

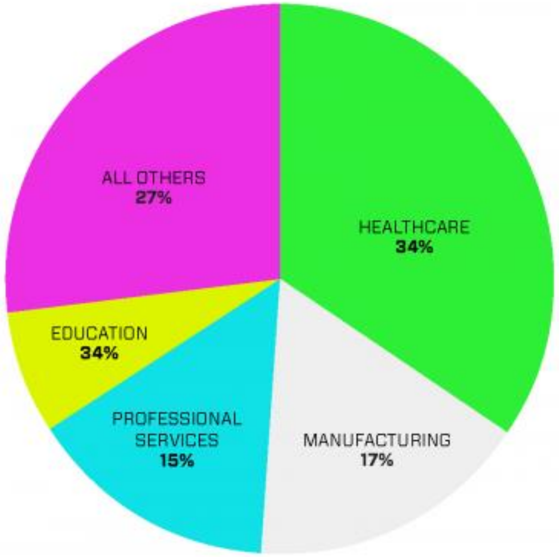
Payment raise: 3 days, 23:59:43

Final destruction: 6 days, 23:59:43

To recover your files and unlock your computer, you must send 0.1 Bitcoins ($35 aprox.) to the next Bitcoin address:

1BaLBdomt2DhibCXsmLXaxKCy467QB4DzF

If you try to remove this payment platform, your will never be able to decrypt your files and they will be lost forever



RANSOMWARE 2017

TOP 10 INDUSTRIES IMPACTED

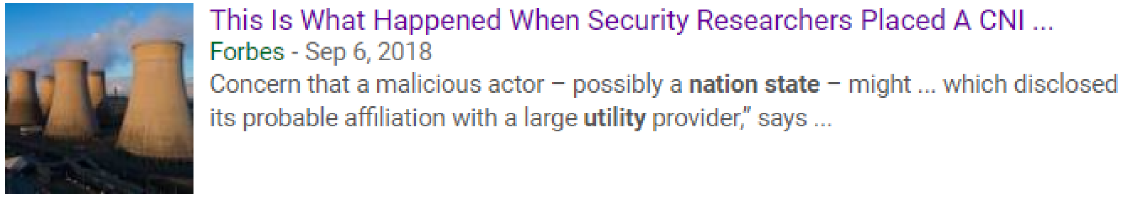
1. Healthcare	34%
2. Manufacturing	17%
3. Professional Services	15%
4. Education	34%
5. All Others	27%

Cylance

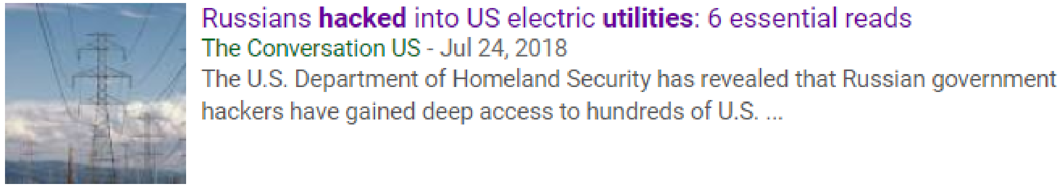
THREAT COMMUNITIES

NATION STATES

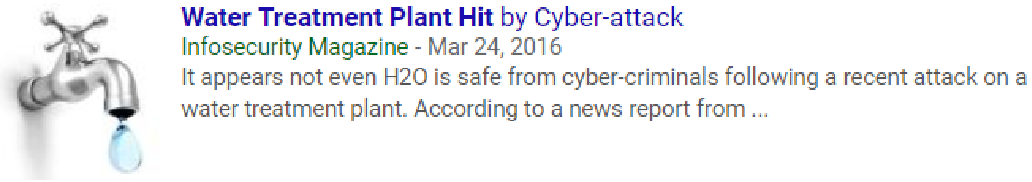
- Factors
  - May be targeted attack or collateral damage
  - Extremely organized and well funded groups
  - APT (east / west exploits)
  - Wide range of tools
- Loss magnitude
  - Complete rebuild of organizational infrastructure
  - Lost Revenue
  - Forensics services
  - Litigation / Legal Services



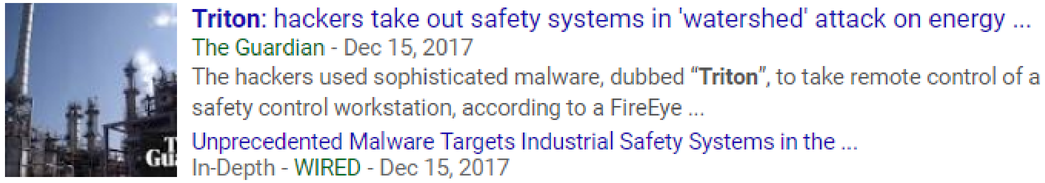
This Is What Happened When Security Researchers Placed A CNI ...
Forbes - Sep 6, 2018
Concern that a malicious actor – possibly a **nation state** – might ... which disclosed its probable affiliation with a large **utility** provider," says ...



Russians **hacked** into US electric **utilities**: 6 essential reads
The Conversation US - Jul 24, 2018
The U.S. Department of Homeland Security has revealed that Russian government hackers have gained deep access to hundreds of U.S. ...



Water Treatment Plant Hit by Cyber-attack
Infosecurity Magazine - Mar 24, 2016
It appears not even H2O is safe from cyber-criminals following a recent attack on a water treatment plant. According to a news report from ...



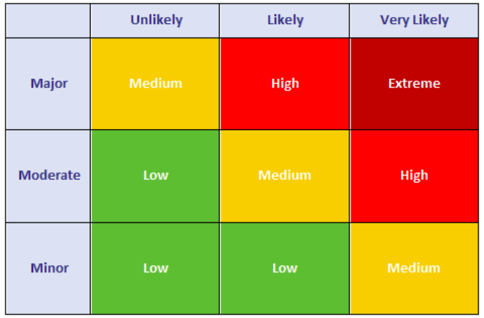
Triton: hackers take out safety systems in 'watershed' attack on energy ...
The Guardian - Dec 15, 2017
The hackers used sophisticated malware, dubbed "**Triton**", to take remote control of a safety control workstation, according to a FireEye ...
Unprecedented Malware Targets Industrial Safety Systems in the ...
In-Depth - WIRED - Dec 15, 2017

HOW ARE YOU TRACKING RISK?

Emerging

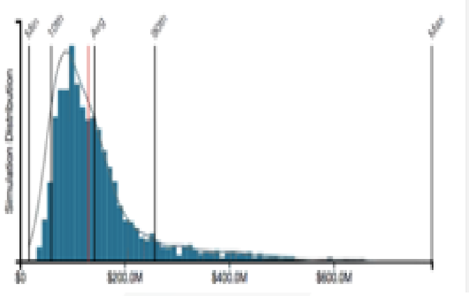
Ad-Hoc

Spreadsheet Analysis

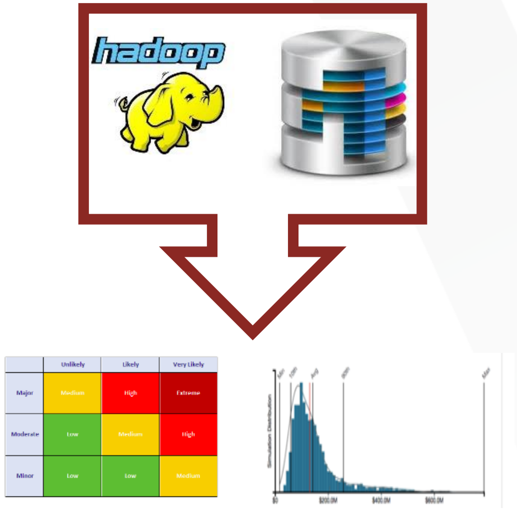


	Unlikely	Likely	Very Likely
Major	Medium	High	Extreme
Moderate	Low	Medium	High
Minor	Low	Low	Medium

Risk Register Matrix



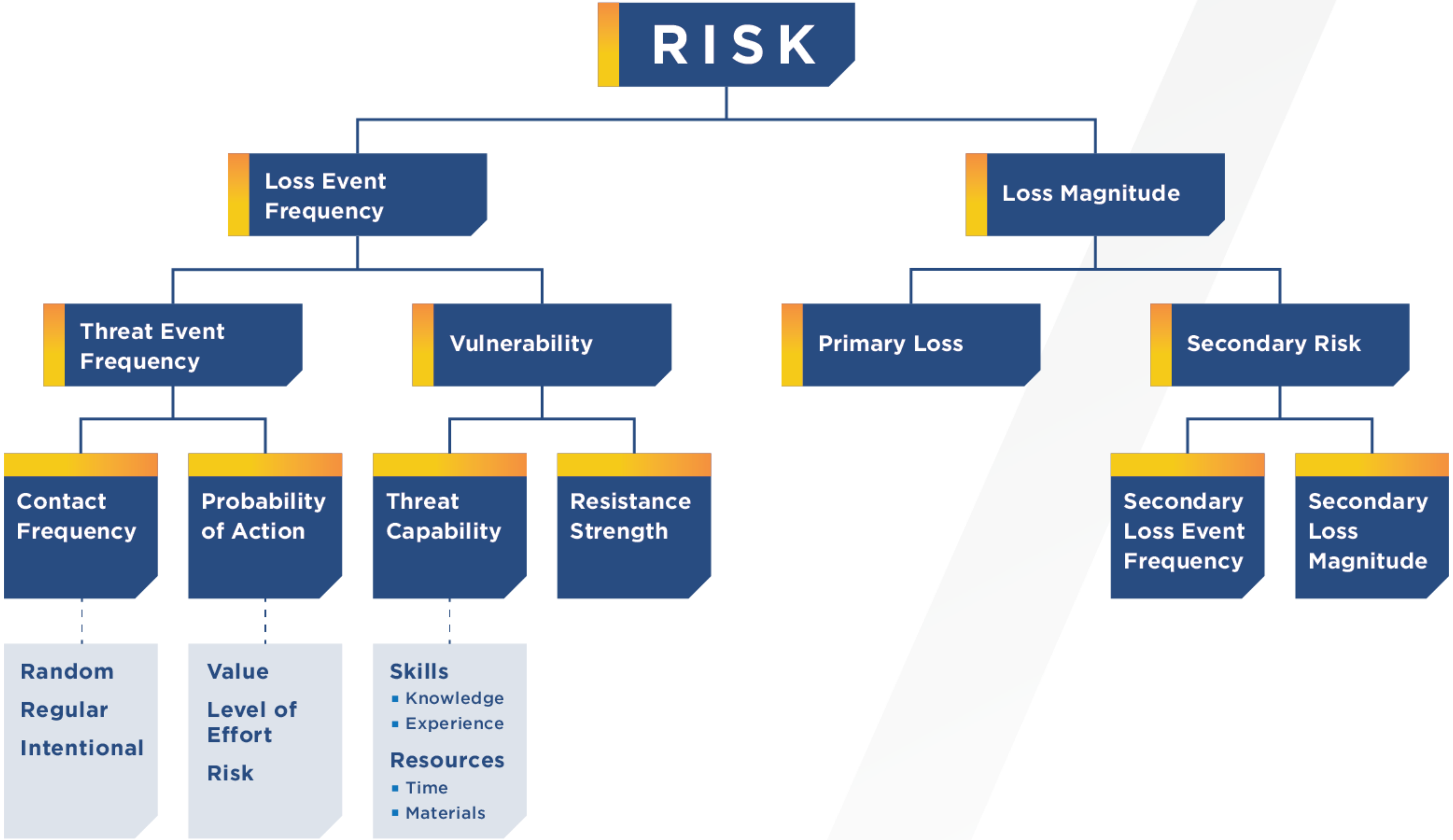
Risk Modeling (e.g. FAIR, Actuarial)



Dynamic Risk Modeling

Increasing Targeting, Precision, Automation, Complexity and Reduction of Risk and Control Overlap

THE FAIR MODEL



CPAT'S BASICS LIST

- Know your IT assets….all of them! How else can you prioritize?
- It will happen one day…
  - BC/DR
  - Air-gapped Backups
  - Bitcoin
  - Forensics Retainers
- Basic Hygiene with a Vulnerability Risk Management Program
- Start thinking with FAIR
  - Which threat communities actually pose a risk? Study the Adversaries!
  - What assets are they coming after?
  - What is the loss magnitude
  - What is the probability this happens this year? Next year? In 5 years?
  - Start selecting the best countermeasures
- 2 Factor everywhere…or at least the option!

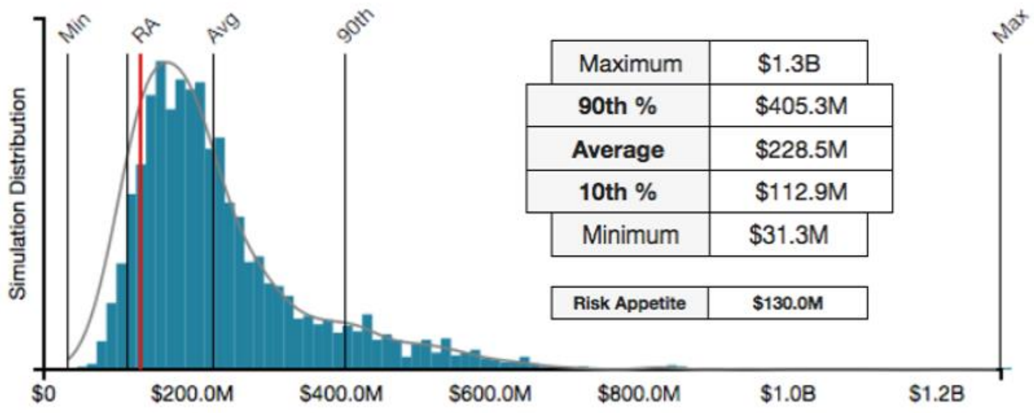
OTHER COUNTERMEASURES TO CONSIDER

- Tabletops
- Deception (pick up East / West traffic)
- Email Sandboxing
- VDI where possible
- DarkWeb Research Tools
- Management of Admin rights….PAM

RSA ARCHER CYBER RISK QUANTIFICATION

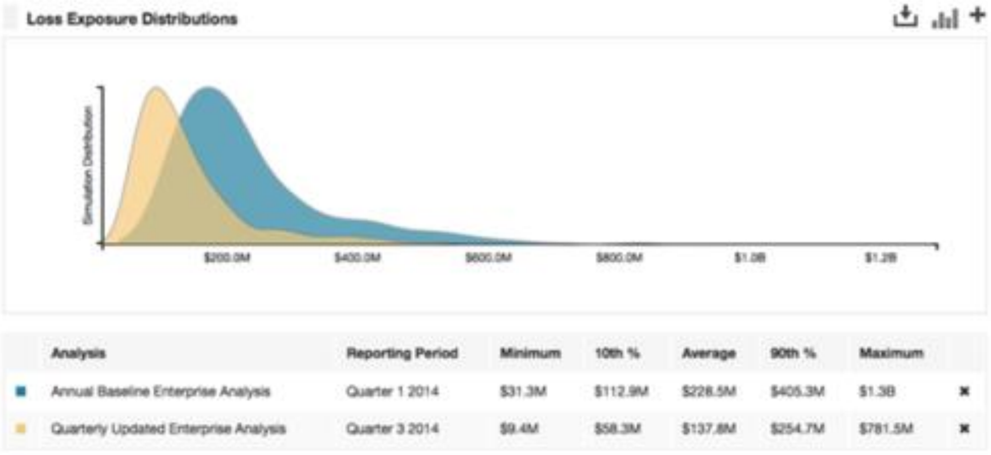
Key Features

- Built-in risk calibration and analysis engine for cyber risk calculation
- Templated workflow for easy scenario modeling
- On-demand risk analytics for answers to questions on the fly
- Mathematical simulations to build your risk profile with limited data
- Existing loss tables based on industry data
- Easy-to-use SaaS application
- User-friendly interface



Maximum	$1.3B
90th %	$405.3M
Average	$228.5M
10th %	$112.9M
Minimum	$31.3M

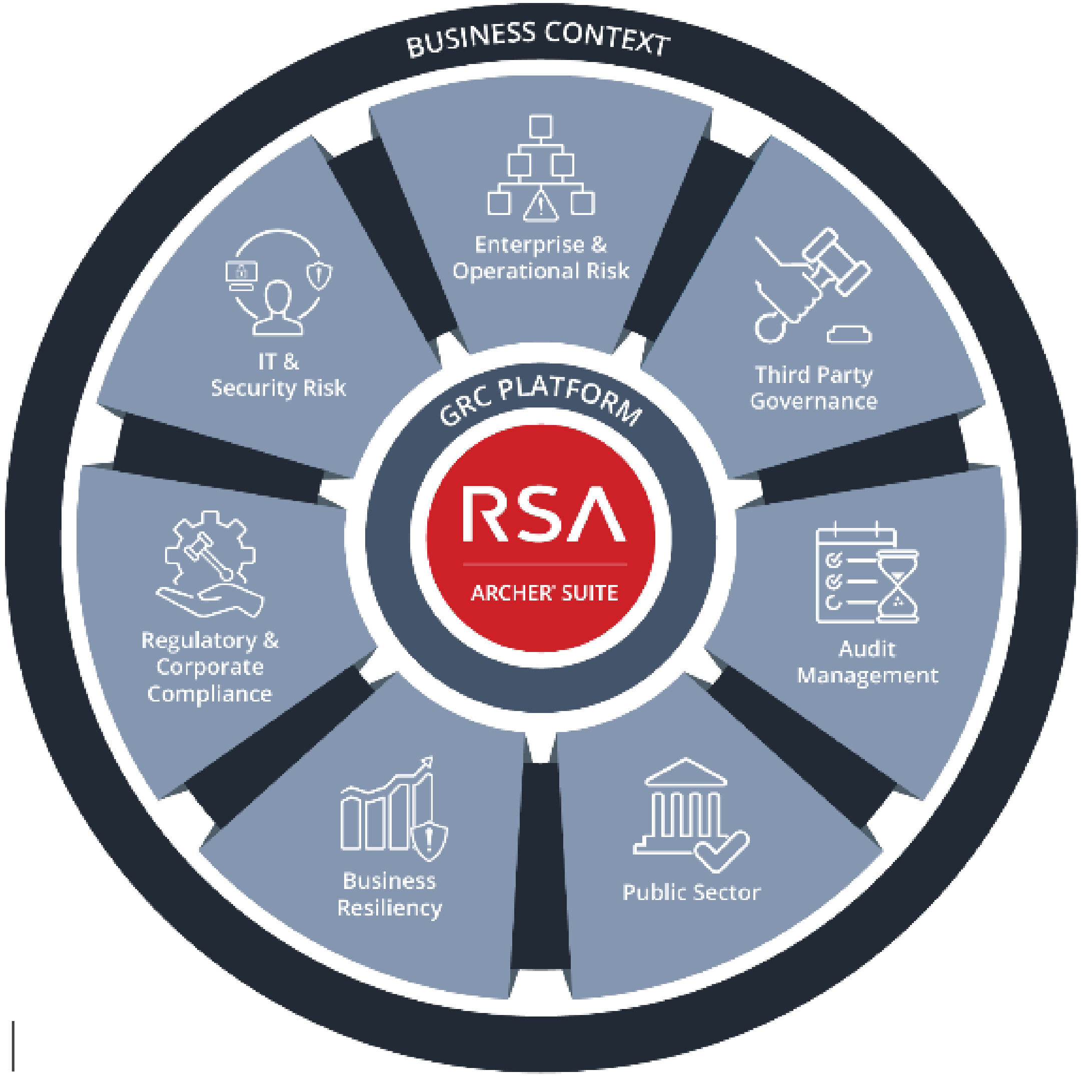
Risk Appetite	**$130.0M**


Loss Exposure Distributions

	Analysis	Reporting Period	Minimum	10th %	Average	90th %	Maximum	
🟦	Annual Baseline Enterprise Analysis	Quarter 1 2014	$31.3M	$112.9M	$228.5M	$405.3M	$1.3B	✖
🟨	Quarterly Updated Enterprise Analysis	Quarter 3 2014	$9.4M	$58.3M	$137.8M	$254.7M	$781.5M	✖

RSA ARCHER – THANK YOU

OPEN DISCUSSION



RSA Archer customers

1,300+ GRC deployments

9 of the Fortune 10

38 of the Fortune 50

69 of the Fortune 100

10 out of 10 biggest U.S. banks*

Global operations

~$1B revenue

2,700+ employees

1,000+ technology partners

30+ years of cybersecurity expertise

15+ years of risk expertise