WHAT LURKS ON THE DARKWEB

Chris Patteson
Executive Director – Risk Transformation Office
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..
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
VPN Tips
• Must have high grade encryption
• Hides logs

WHAT TOOLS DO I NEED TO EXPLORE THE DARK WEB?
WHAT IS YOUR DESTINATION

Top Markets

- Up / Online - Dream Market - 95.8%
- Up / Online - Point / Torzha Free Market - 89.77%
- Up / Online - WallStreet Market - 89.39%
- Up / Online - DNStats TOR - 98.6%
- Up / Online - Dream Market alternate 1 - 80.65%
- 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 - ApocalypS Market - 92.28%
- 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 - BitCook - 95.12%
- Up / Online - BlockChain info - 85.67%
- Up / Online - CGMC - 97.05%
- Up / Online - CharlieUK - 90.23%
- Down / Offline - Dark Rabbit Market - 70.11%
- Down / Offline - Darknet Avengers - 70.46%
- Up / Online - Deep Sea - 98.51%
- Down / Offline - DHL - 94.82%

Other Markets

- Down / Offline - EuroPills - 79%
- Down / Offline - ApocalypS Market - 92.28%
- 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 - BitCook - 95.12%
- Up / Online - BlockChain info - 85.67%
- Up / Online - CGMC - 97.05%
- Up / Online - CharlieUK - 90.23%
- Down / Offline - Dark Rabbit Market - 70.11%
- Down / Offline - Darknet Avengers - 70.46%
- Up / Online - Deep Sea - 98.51%
- Down / Offline - DHL - 94.82%

Surfacing Collaborated Networks in Dark Web to find illicit and criminal content - International Cyber Crime Research Center (ICCRC) School of Criminology, Simon Fraser University
<table>
<thead>
<tr>
<th>OFFERING</th>
<th>Russia</th>
<th>Japan</th>
<th>China</th>
<th>Germany</th>
<th>US</th>
<th>Canada</th>
<th>Brazil</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agora invitation code/onion site access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATM PIN pad skimmers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATM skimmers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bots</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Child-porn related goods</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Counterfeit money</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit card clones</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit card number generators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crypters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data dumpas</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drugs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit kits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fake documents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fake websites</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How-to guides/modules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified Android apps with prepaid credits paid for with stolen credit cards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modified smart card readers and writers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone number databases</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pocket payment card skimmers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Point-of-sale (PoS) skimmers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social engineering toolkits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stolen Packstation accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weapons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web popularity boosters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antimalware proofing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antispam proofing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apple App Store app rank boosting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bitcoin tumbling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulletproof hosting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coding/Programming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compromised server access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compromised credit card panel access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crypting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed denial-of-service (DDoS) attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document copy rework</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dropping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Escrow/Garant/Truhand</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fast fluxing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet and CATV access plan bump-up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leaked data search engine privacy protection/subscription</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mule</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Murder for hire</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment card validity checking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personally identifiable information (PII) querying</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spamming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spying using Web cameras</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Translation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trojan toolkit access subscription</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Forward Looking Threat Research Team – Trend Micro / Trend Labs
## TOOLS OF THE TRADE / CYBER CRIME AS A SERVICE

<table>
<thead>
<tr>
<th>HACKING TOOLS &amp; SERVICES</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Hacking Program</td>
<td>$12.99 (See more details on page 10)</td>
</tr>
<tr>
<td>Hacked Instagram Accounts in Bulk</td>
<td>1,000 - 10,000 accounts $15 - $60</td>
</tr>
<tr>
<td>Botnet: Blow-Bot Banking Botnet</td>
<td>Monthly Basic Rental $750</td>
</tr>
<tr>
<td>Disdain Exploit Kit</td>
<td>Day $80, Week $500, Month $1,400</td>
</tr>
<tr>
<td>Stegano Exploit Kit: Chrome, Firefox, Internet Explorer, Opera, Edge</td>
<td>Unlimited Traffic, Day $2,000</td>
</tr>
<tr>
<td>Microsoft Office Exploit Builder</td>
<td>Lite exploit builder $650</td>
</tr>
<tr>
<td>WordPress Exploit</td>
<td>$100</td>
</tr>
<tr>
<td>Password Stealer</td>
<td>$50</td>
</tr>
<tr>
<td>Android Malware Loader</td>
<td>$1,500</td>
</tr>
<tr>
<td>Western Union Hacking Bug For World Wide Transfer</td>
<td>$300</td>
</tr>
<tr>
<td>DDoS Attacks</td>
<td>Week long attack $500 - $1,200</td>
</tr>
<tr>
<td>ATM Skimmers: Wincor, Slimm, NCR, Diebold</td>
<td>$700 - $1,500</td>
</tr>
<tr>
<td>Hacking Tutorials</td>
<td>Multiple Tutorials $5 - $50</td>
</tr>
</tbody>
</table>

84% of 1,010 organizations surveyed in a 2017 report had experienced at least one DDoS attack in the previous 12 months, and 88% of those attacked dealt with more than one during that period.
## 1.4 Billion Clear Text Credentials Discovered in a Single Database – 4iQ Analysis

<table>
<thead>
<tr>
<th>Count</th>
<th>Password</th>
<th>Count</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9218720</td>
<td>21</td>
<td>370652</td>
</tr>
<tr>
<td>2</td>
<td>3103503</td>
<td>22</td>
<td>384784</td>
</tr>
<tr>
<td>3</td>
<td>1651385</td>
<td>23</td>
<td>347167</td>
</tr>
<tr>
<td>4</td>
<td>1313464</td>
<td>24</td>
<td>343864</td>
</tr>
<tr>
<td>5</td>
<td>1273179</td>
<td>25</td>
<td>311371</td>
</tr>
<tr>
<td>6</td>
<td>1126222</td>
<td>26</td>
<td>300279</td>
</tr>
<tr>
<td>7</td>
<td>1085144</td>
<td>27</td>
<td>299984</td>
</tr>
<tr>
<td>8</td>
<td>969909</td>
<td>28</td>
<td>298938</td>
</tr>
<tr>
<td>9</td>
<td>952446</td>
<td>29</td>
<td>291132</td>
</tr>
<tr>
<td>10</td>
<td>879924</td>
<td>30</td>
<td>276473</td>
</tr>
<tr>
<td>11</td>
<td>866640</td>
<td>31</td>
<td>270488</td>
</tr>
<tr>
<td>12</td>
<td>834468</td>
<td>32</td>
<td>268121</td>
</tr>
<tr>
<td>13</td>
<td>621078</td>
<td>33</td>
<td>263605</td>
</tr>
<tr>
<td>14</td>
<td>564344</td>
<td>34</td>
<td>255079</td>
</tr>
<tr>
<td>15</td>
<td>527158</td>
<td>35</td>
<td>250732</td>
</tr>
<tr>
<td>16</td>
<td>470592</td>
<td>36</td>
<td>241721</td>
</tr>
<tr>
<td>17</td>
<td>468554</td>
<td>37</td>
<td>241495</td>
</tr>
<tr>
<td>18</td>
<td>417878</td>
<td>38</td>
<td>227701</td>
</tr>
<tr>
<td>19</td>
<td>398114</td>
<td>39</td>
<td>226785</td>
</tr>
<tr>
<td>20</td>
<td>371627</td>
<td>40</td>
<td>220363</td>
</tr>
</tbody>
</table>

### Repetition
- chuepost.de: l369888369
- chugmx.de: l369888369
- chulycos.de: l369888369
- chuweb.de: l369888369
- chu@yahoomail.com:l369888369
- chu@yahoo.de: l369888369

### Simple Patterns
- 93@hotmail.com: iluvb33pb33p
- 93@hotmail.com: 1luvb33pb33p
- 93@hotmail.com: iluvbeepbeep
THE FAIR MODEL

RISK

Loss Event Frequency

Threat Event Frequency
- Contact Frequency
  - Random
  - Regular
  - Intentional
- Probability of Action
- Threat Capability

Vulnerability
- Resistance Strength
  - Skills
    - Knowledge
    - Experience
  - Resources
    - Time
    - Materials

Loss Magnitude

Primary Loss
- Secondary Loss Event Frequency
- Secondary Loss Magnitude

Secondary Risk
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)

Amor Black Market Report 2018

RSA Fraud Risk Intelligence - Q2 1028
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
### 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
HOW ARE YOU TRACKING RISK?

- Ad-Hoc
- Spreadsheet Analysis
- 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

RISK

Loss Event Frequency
- Threat Event Frequency
  - Contact Frequency
    - Random
    - Regular
    - Intentional
  - Probability of Action
    - Value
    - Level of Effort
    - Risk
- Vulnerability
  - Threat Capability
  - Resistance Strength
    - Skills
      - Knowledge
      - Experience
    - Resources
      - Time
      - Materials
- Loss Magnitude
  - Primary Loss
  - Secondary Risk
    - Secondary Loss Event Frequency
    - Secondary Loss Magnitude
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
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