FraudShare Webinar Series

August 21, 2019

Combating Cyber Crime through Strategic Partnerships

LIMRA
LOMA

CT Center for Digital Investigations
P.O. Box 535 Glastonbury, CT 06033 860-432-4866

Speakers

Brian McCabe
Senior Special Agent
US Secret Service

Matthew Brodacki
Police Captain
Town of Weston, CT

Richard Colangelo, Jr.
State's Attorney for the Judicial District of Stamford-Norwalk
State of CT

Introduction

1. Cyber awareness quiz
2. Cyber landscape
3. Sector's risk
4. Criminal organization structure
5. Dark web
6. Prevalent vector's (Social engineering, Ransomware and BEC)
7. Takeaway's from victims
8. Preventive

Cybersecurity Quiz

1. Which of the following companies have reported a large data breach in the past year?

A. Marriott International Inc.

B. British Airways

C. Adidas AG

D. Humana Inc.

E. All of the above

Cybersecurity Quiz

- **Answer: E.**

No industry is immune to hackers. These firms experienced a variety of cyberattacks, including one that collected data from the British Airways website as customers booked flights. At Humana , a network server was hacked. Marriott said intruders were likely lurking in its Starwood Hotels guest systems for two years before Marriott acquired the company in 2016, and for another two years after that.

Cybersecurity Quiz

2. What is the most common way data is breached?

A. Ransomware

B. Phishing

C. Corrupting mobile phones

D. Intercepting data on public Wi-Fi

E. Using hacking tools leaked from the National Security Agency.

Cybersecurity Quiz

Answer: B

According to a report by Verizon Communication Inc. Hackers disguise **phishing** emails to look legitimate but the emails contain malicious links to trick employees or consumers into revealing their credentials. Many people are fooled.

Cybersecurity Quiz

3. How much are companies and governments expected to spend on cybersecurity products and services this year globally?

A. $50 million

B. $50 billion

C. $124 million

D. $124 billion

E. $224 billion

Cybersecurity Quiz

Answer: D

This is a jump of more than 8% compared with last year, according to the report from Gartner Inc. citing the figures. The additional spending is being spurred in part by increasing regulatory requirements and the shortage of cybersecurity professionals.

Cybersecurity Quiz

4. Should you pay the ransom demanded by hackers who lock up your device or data (Ransomware)?

A. Yes

B. No

C. It depends

Cybersecurity Quiz

Answer: No

The U.S. government doesn’t encourage cyber crime victims to pay ransom to hackers. Victims should consider that criminals may not restore their data even if they pay.

Cybersecurity Quiz

5. Where were the biggest financial losses in the U.S. from cyber crimes in 2018?

A. Washington, D.C.

B. New York

C. Texas

D. California

E. Massachusetts

Cybersecurity Quiz

Answer: D

Victims from California reported total losses of more than $450 million to the Federal Bureau of Investigation’s Internet Crime Complaint Center last year. New Yorkers experienced the second-highest level of losses, at around $201 million.

Cybersecurity Quiz

6. What percentage of companies in the energy, health-care and manufacturing sectors experienced damaging cyberattacks in the past two years?

A. 50%

B. 20%

C. 78%

D. 90%

E. 15%

Cybersecurity Quiz

Answer: D

90% of businesses in these sectors suffered a cyberattack that led to data breaches, significant disruption or downtime of business operations, according to a 2019 survey from cybersecurity firm Tenable Inc. Sixty-two percent of companies in these sectors experienced two or more damaging cyberattacks in the past two years.

Cyber Landscape
Law Enforcement Perspective

FBI's 2018 Internet Crime Complaints Center (IC3) Crime Report

- IC3 received over 20,373 BEC/E-mail Account Compromises Complaints.
  - Losses attributed to the those complaints were over 1.2 billion.
  - Variates; Personal Email, Vendor, Spoofed Lawyer, W-2 and Real Estate Sector.
  - Rise in requesting victims for gift card.
- Payroll Diversion – 100 complaints, loss of 100 mil.
- Extortion – 51,146 extortion related complaints, loss of over $83 mil (242%).
- Tech Support Fraud – 14,408, losses of nearly $39 mil (161% increase).
- CT ranks 28th out of 57 reporting States with 3,134 complaints (victims).
- CA ranks #1 with 49,031 complaints, NY ranks #4 with 18,124 complaints.
- CT ranks 18th in losses $37,859,918.
- CA ranks #1 with $450,482,128 losses, NY ranks #2 with $210,090,065 losses.

Cyber Landscape
Private Sector Perspective

2019 Verizon Data Breach Report

- Report analyzed 41,686 security incidents of which 2013 were confirmed data breaches.
- Breach/Incident patterns in POS/Skimmers continue to decline.
- New data subset Financially Motivated Social Engineering
  - Attacks that do not have a goal of malware installation.
  - Focus on credential theft
  - Dupe victim into transferring funds into an accomplices account.
- Incidents top threat action varieties; DOS, Loss, C2 and Misdelivery.
- Beaches top threat action; Phishing, Stolen credentials, C2 and Privilege abuse.

Incident Patterns

- Patterns

2019	2018
– Privilege Misuse	(DOS)
– Denial of Service	(Privilege Misuse)
– Crime ware	(Crime ware)
– Lost or stolen Assets	(Web applications)
– Web Applications	(Lost and stolen Assets)
– Miscellaneous Errors	(Mis. Errors)
– Cyber-Espionage	(Everything Else)
– Everything Else	(Cyber-Espionage)
– Espionage	(Point of Sale)
– POS	(Payment Card Skimmers)

Breach Type per Pattern

- Breach Type

2019	2018
– Web application	(Web applications)
– Miscellaneous Errors	(Mis. Errors)
– Privilege Misuse	(Point of Sale)
– Cyber-Espionage	(Privilege Misuse)
– Everything Else	(Cyber-Espionage)
– Crime ware	(Lost and Stolen assets)
– Lost or stolen assets	(Crime ware)
– Point of Sale/ Skimmers	(POS/Skimmers)
– Denial of Service	(DOS)

Summary of Findings: Breaches

Who ?

- Small Businesses – 43%
- Public Sectors – 16%
- Healthcare organization – 15%
- Financial Industry – 10%

Who is behind the breaches?

- Outsiders - 69%
- Organized crime - 39%
- Insiders - 34%
- Nation state or state affiliated - 23%
- Multiple parties – 5%
- Partners - 2%

Tactics and techniques used

- Hacking - 52%
- Social engineering- 33%
- Malware- 28%
- Misc. errors- 21%
- Misuse by authorized users– 15%
- Physical actions were present - 4%

Other commonalities

- Financially motivated - 71%
- Took months or longer to discover- 56%
- Phishing- 32%
- Stolen credentials- 29%
- Espionage – 25%

Sector's at Risk – Who, What and How?

Sector:	**ACCOMMODATIONS**
Who:	99% external, 1% internal
What:	93% payment, 5% personal, 2% credentials
How:	93% hacking, 91% malware
Target:	90% Breaches involve POS intrusions (Breaches on the rise)

Sector:	**EDUCATION**
Who:	81% external, 19% internal
What:	72% personal, 14% secrets, 11% medical
How:	48% hacking, 41% malware
Target:	20% Motivated by espionage, Social engineering scam (Breaches on the rise)

Sector:	**FINANCIAL**
Who:	79% external, 19% internal
What:	36% personal, 34% payment, 13% bank
How:	34% hacking, 34% physical
Target:	ATM payment card skimmers and DOS (Breaches on the decline)

Sector:	**HEALTHCARE**
Who:	43% external, 56% internal
What:	79% medical, 37% personal, 4% payment
How:	35% error, 24% misuse
Target:	Insider greater threat then outside (Breaches on the rise)

Sector:	**PROFESSIONAL**
Who:	70% external, 31% internal
What:	56% personal, 28% credentials, 16% internal
How:	50% hacking, 21% social
Target:	Involve phishing and stolen credentials (Breaches on the rise)

Sector's at Risk – Who, What and How?

Sector:	**INFORMATION**
Who:	74% external, 23% internal
What:	56% personal, 41% credentials, 9% internal
How:	57% hacking, 26% error
Target:	Web apps attacks, most often using stolen credentials (Breaches on the decline)

Sector:	**PUBLIC**
Who:	67% external, 34% internal
What:	41% personal, 24% secrets, 14% medical
How:	52% hacking, 32% social
Target:	44% contributed to cyber espionage (Breaches on the rise)

Sector:	**MANUFACTURING**
Who:	89% external, 13% internal
What:	32% personal, 30% secrets, 24% credentials
How:	66% hacking, 34% malware
Target:	47% of the breaches involved the theft of intellectual property (Breaches on decline)

Sector:	**RETAIL**
Who:	91% external, 10% internal
What:	73% payment, 16% personal, 8% credentials
How:	46% hacking, 40% physical
Target:	Web apps leveraging poor validation of inputs or stolen credentials (Breaches on rise)

Criminal Organization Structure

Operate as businesses – Top to bottom model

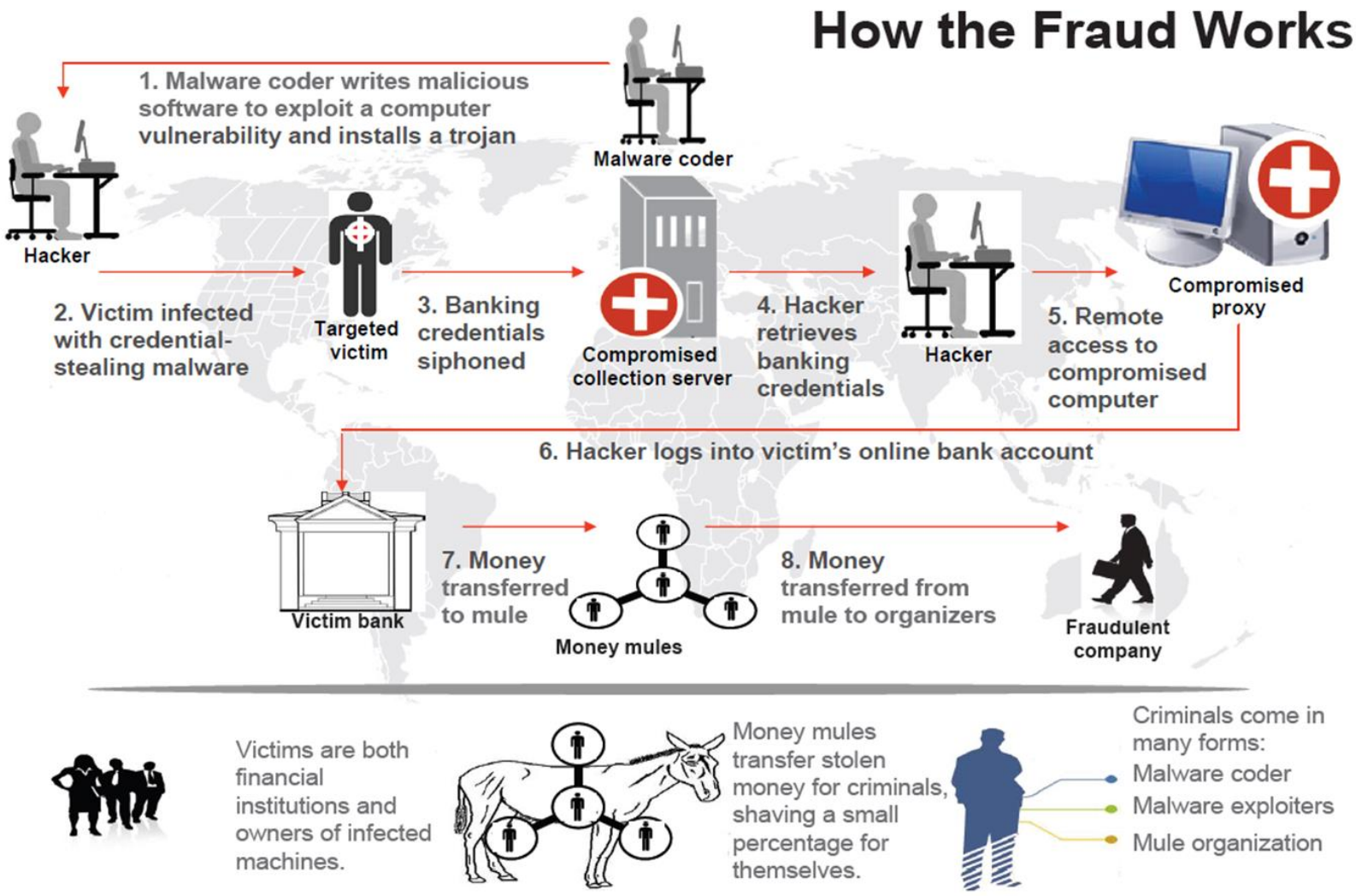
Department	Description
C-Suite	Sets design and targets businesses – Eastern Europe, West Africa
IT Wing	Carries out hacking, malware, email monitoring – Global
HR/Recruitment	Recruits IT wing, financial actors – Eastern Europe, West Africa
Finance/Banking	Sets process for wire transfers and Money Laundering – Global, Local
Enforcers	Ensures financial cooperation and following of orders – Global
Admins	Maintain shell companies and legitimate business liaisons – Local
Burn party	After successful schemes, enterprise burns all materials – Global

Money Laundering Process

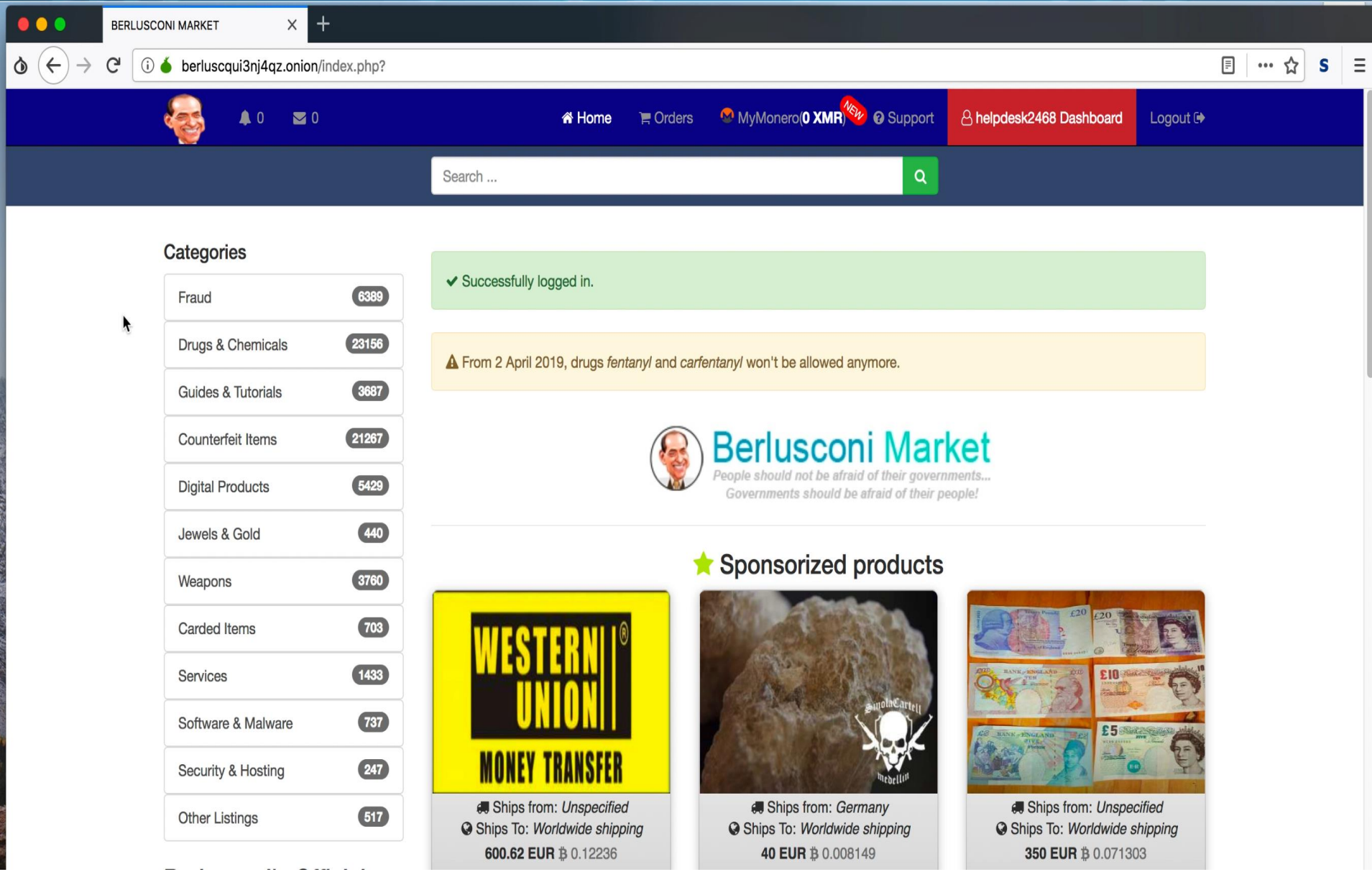
In any Business Email Compromise, the main goal of the criminal actor is to move the proceeds of the criminal activity as quickly as possible –time is money. BEC actors accomplish this through a variety of relatively standard means of money laundering such as:

- Use of unwitting money mules –romance schemes, work from home scams, etc.
- Use of knowing money mules to set up domestic shell companies and bank accounts.
- Utilizing Western Union/Money Gram/Postal Money orders to move smaller amounts of the funds quickly
- Use of lower-rate check cashing services i.e. SeńorCheck Cashing
- Quick purchase of assets –vehicle, luxury goods
- Use of internationally based shell companies in Hong kong, China, Macau, etc.
- Use of virtual currency
- Use of standard cash withdrawals below the reporting threshold

Online Banking Account Takeover



DARK WEB


BERLUSCONI MARKET
berluscqui3nj4qz.onion/index.php?
0
0
Home
Orders
MyMonero(0 XMR)
NEW
Support
helpdesk2468 Dashboard
Logout
Search ...
Categories
Fraud 6389
Drugs & Chemicals 23156
Guides & Tutorials 3687
Counterfeit Items 21267
Digital Products 5429
Jewels & Gold 440
Weapons 3760
Carded Items 703
Services 1433
Software & Malware 737
Security & Hosting 247
Other Listings 517
Successfully logged in.
From 2 April 2019, drugs fentanyl and carfentanyl won't be allowed anymore.
Berlusconi Market
People should not be afraid of their governments...
Governments should be afraid of their people!
Sponsorized products
WESTERN UNION
MONEY TRANSFER
Ships from: Unspecified
Ships To: Worldwide shipping
600.62 EUR ฿ 0.12236
Ships from: Germany
Ships To: Worldwide shipping
40 EUR ฿ 0.008149
Ships from: Unspecified
Ships To: Worldwide shipping
350 EUR ฿ 0.071303

Dark Web

BERLUSCONI MARKET

berluscqui3nj4qz.onion/index.php?c=listings&a=search&cat=7&page=2

0 0 Home Orders MyMonero(0 XMR) NEW Support helpdesk2468 Dashboard Logout

Worldwide shipping
Escrow Type: **Full Escrow**
Sold: 0

No picture

CUSTOM BRAINHAZE

g00d00 [+1018|–18] Trusted
Ships from: Italy
Worldwide shipping
Escrow Type: **Finalize Early**
Sold: 0

725 EUR
฿ 0.148049
Buy Now
$ Currencies:

HALF PRICE Xanax 2mg x 500 Bars Alprazolam

monoko [+548|–2] On vacation
Ships from: United Kingdom
Worldwide shipping
Escrow Type: **Full Escrow**
Sold: 0

205.28 EUR
฿ 0.041919
Buy Now
$ Currencies:

Sample - 0,3g Afghan Heroin

Lucky-Aide [+20|–0]
Ships from: Germany
Worldwide shipping
Escrow Type: **Full Escrow**
Sold: 3

17 EUR
฿ 0.003471
Buy Now
$ Currencies:

Dark Web

BERLUSCONI MARKET

berluscqui3nj4qz.onion/index.php?c=listings&a=search&cat=42

0 0 Home Orders MyMonero(0 XMR) NEW Support helpdesk2468 Dashboard Logout

- Guides & Tutorials 3687
- Counterfeit Items 21269
- Digital Products 5429
- Jewels & Gold 440
- **Weapons 3760**
  - Ammunition
  - Pistols
  - Long-Range Guns
  - Explosives
  - Hand Weapons
  - Other
- Carded Items 703
- Services 1433
- Software & Malware 737

get one of the most recent glock 19

pacassy [+6|–0]

Ships from: United States

Worldwide shipping

Escrow Type: **Full Escrow**

Sold: 0

343.64 EUR

฿ 0.070173

Buy Now

$ Currencies:

GLOCK G19 Gen4 MOS 9mm 4.02" 15 Rds PG1950203MOS

Mueldaves [+6|–0]

Ships from: Unspecified

Worldwide shipping

Escrow Type: **Full Escrow**

Sold: 0

350 EUR

฿ 0.071472

Buy Now

$ Currencies:

CLEAN AK 47

pacassy [+6|–0]

Ships from: United States

Worldwide shipping

Escrow Type: **Full Escrow**

Sold: 0

1199.76 EUR

฿ 0.244997

Buy Now

$ Currencies:

Get your National ID Card and Residence Permit .

2500 EUR

฿ 0.510512

Buy Now

$ Currencies:

Dark Web

BERLUSCONI MARKET

berluscqui3nj4qz.onion/index.php?c=listings&a=search&q=ssn

0 0 Home Orders MyMonero(0 XMR) NEW Support helpdesk2468 Dashboard Logout

osquare [+5|–0]

Escrow Type: **Full Escrow**

Sold: 0

REGISTERED DRIVERS LICENSE,ID CARDS,SSN AND RESIDENT PERMITS..FOR DIFFERENT COUNTRIES AVAILABLE

1200 EUR
฿ 0.245046

Buy Now

$ Currencies:

Rapidseller [+1|–0]

Ships from: Europe

Worldwide shipping

Escrow Type: **Full Escrow**

Sold: 0

Where to buy USA and Canadian passports, drivers license, ID cards, SSN,visas

1000 EUR
฿ 0.204205

Buy Now

$ Currencies:

jorge22 [+0|–0]

Ships from: Germany

Worldwide shipping

Escrow Type: **Full Escrow**

Sold: 0

25 High Balance Wells Fargo Bank Accounts/ SSN/ DL

2490 EUR
฿ 0.50847

Buy Now

$ Currencies:

Social Engineering

Definition:

Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of a potential victim's natural tendencies and emotional reactions.

Types:

1. **Phishing** - Most common, attacker creates website or support portal of renowned company and sends links to targets via email or social media platform.
2. **Spear Phishing** - Spear Phishing can be assumed as a subset of Phishing. Although a similar attack, it requires an extra effort from the side of the attackers. They need to pay attention to the degree of uniqueness for the limited number of users they target (C Suite).
3. **Vishing** – Vishing is similar to phishing but it uses the phone. attackers recreate the IVR (Interactive Voice Response) system of a company. They attach it to a toll-free number and trick people into calling the phone number and entering their details.

Social Engineering Types Cont'd

4. **Pretexting -** Based on a scripted scenario presented in front of the targets, used to extract PII or some other information. An attacker might impersonate another person or a known figure. An example of pretexting can be fake emails you receive from your distant friends in need of money. Probably, someone hacked their account or created a fake one.
5. **Baiting -** Attackers infected USB drive or disk at public places with a hope of someone picking it up out of curiosity and using it on their devices. A more modern example of baiting can be found on the web. Various download links, mostly containing malicious software, are thrown in front of random people hoping someone would click on them.
6. **Quid pro quo –** Technique in which the attacker poses as technical support. They make random calls to a company's employees claiming that they're contacting them regarding an issue. Sometimes, such people get the chance to make the victim do things they want. It can be used for everyday people also.

Social Engineering

Psychology of social engineering: Attackers manipulate your emotions.

1. Curiosity – High profile news stories, gossip and celebrities.
2. Fear – Warns of something bad will happen to you.
3. Trust – Message comes from a trusted individual or organization.
4. Need – Message mentions personal details about you or something of interest.
5. Generosity – Attackers know that people are generous, especially times of disaster.
6. Desire – Free gift or great deal.

Clues of an Attack:

1. Emotional manipulation
2. Requested private information.
3. Irregular email – missing recipient address in email or aliased sender address.
4. General or missing greeting.
5. Typos and grammatical errors.
6. Incorrect or confusing text.
7. Directed to do something.
8. Links attached to the email.

Social Engineering - Prevention

- Remember Social engineering utilizes all of our modern media for their attacks: emails, instant messages, social networks, phones and even faexs.
- Be suspicious of emails that prey on emotions (Curiosity, Fear, Trust, Need, Generosity and Desires).
- Look for Clues.
- Delete messages that ask for private information or look suspicious.
- Don’t click on links (URL’s) or call phone numbers provided in messages.
- Investigate any link before you click on it (Attackers often hide malicious links among several legitimate ones.

RANSOMWARE

How Should I Respond to an Attack

** Victims should reach out to law enforcement before making contact with the bad actor. Once initial contact is made, this potentially starts the clock, which will reduce the allowable time to respond.

Characteristics of Ransomware malware infections:

Non-encrypting ransomware locks the screen (restricts access to files but does not encrypt them).

Ransomware that **encrypts the Master Boot Record (MBR)** prevents the victims' computers from being booted up in a live environment (what most people consider a ransomware attack).

Leakage or "**extortionware**" exfiltrates data that the attackers threaten to release if ransom is not paid.

Mobile Device Ransomware (infects cell-phones through drive-by downloads or fake apps).

** The USSS/Law Enforcement does not encourage victims to pay the demand.

1. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom while others have been continually extorted by new demands.
2. On average, paying the ransom results in decryption of 77% of the network data.

RANSOMWARE MITIGATION

The following are instructions and advice an investigator can provide to the victim to help mitigate this type of network attack.

1. Advise the victim to isolate the compromised portion of their network ASAP, but do not power down or shut off any system affected by the ransomware (this includes both wired and wireless networks).
2. Determine if communication has occurred with the attacker; if yes, by whom (if the victim is a large Corp., often it will be a company's attorney).
3. Collect all available log information.
4. Try to discover the characteristics of the malware infection to determine the appropriate investigative response.
5. Ransomware attacks are the result of poor or defective security standards, therefore, the entire system should not be trusted. Advise the victim that all communications regarding the compromise, should be "out of band" (phone).
6. Use the oldest back-up to restore the system

RANSOMWARE MITIGATION - TRIAGE

The below list is an example of key data to collect when responding to a ransomware event.

1. Detailed victim information to include organization name, sector, systems affected, technical POC, and loss amount.
2. If available, ransomware variant name.
3. Original email(s) with full headers and any attachments (if the attack was executed by phishing).
4. Copies of any executables or other files dropped onto the system after accessing malicious attachments, including splash page.
5. Any domains or IP addresses communicated with just prior to or during infection.
6. The Bitcoin address (or other requested virtual currency address) to which payment is requested, and the amount being requested.
7. Was the ransom paid? If so, the amount and the Bitcoin address to which the payment was made.
8. If available, any forensic analysis or incident response reports completed.
9. If available, any memory captures taken during execution of the malware.
10. Status of the infection.

RANSOMWARE - PREVENTION

The following measures can make a system or network more secure against malware or similar types of attacks:

1. Update software and operating systems with the latest patches. This one of the most common vulnerabilities that is easily fixable.
2. Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
3. Use application whitelisting to allow only approved programs to run on a network.
4. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
5. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
6. Configure firewalls to block access to known malicious IP addresses.

Business Email Compromise (BEC's)

Definition:

Business Email Compromise is a sophisticated fraud scheme targeting businesses working with other parties that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business or personal e-mail accounts through social engineering, malware, or computer intrusion techniques. Once compromised, a fraudulent email is sent directing victims to unknowingly conduct unauthorized transfers of funds.

Overview:

1. Firm employees have email discussion with a client.

   1a. Communication intercepted by hackers!

2. Hackers create spoofed email emulating client.

   2a. Hackers send spoofed email as client requesting transfer of funds.

3. Instructions seem legitimate, firm transfers funds to fraudsters account.

Business Email Compromise (BEC)

5 types of BEC's

1. **CEO Fraud scheme** – Impersonate CEO, request for fund transfer from CEO to CFO.
2. **Bogus Invoice scheme** – Impersonates supplier for invoice payments.
3. **Account Compromise scheme** – Impersonates company and sends requests for payments.
4. **Data theft scheme** – PII or W2's targets (Human Resources, Bookkeeping and Financial auditors).
5. **Attorney Impersonation scheme** – Impersonates attorney (corporate and real estate most common).

BEC's - Preventative Measures

- ✓ Register all similar domain names that can be used for spoofing attacks
- ✓ Create email rules that flag and delineate emails received from unknown domains. Also monitor creation of new email rules within the email server environment
- ✓ Authenticate all financial transactions through use of dual factor authentication methods
- ✓ Confirm all changes in payment methods with source using trusted and authenticated information
- ✓ Know the habits of those with whom financial transactions are conducted
- ✓ Educate employees, clients, vendors, etc. on Business Email Compromise
- ✓ Conduct a Business Email Compromise drill similar to anti-phishing exercises

Takeaways from Victims

- **Do a better job of reviewing the insurance coverage:**
  - Unfortunately, we turned down an $859 insurance policy that would have covered this claim. We turned it down because we thought we had such good procedures in place that we did not need the coverage. We also should have thought more about the coverage in our review of risk overall. If we had purchased this insurance, we also would have needed to change the way we look at insurance. It's not a policy you just buy and put on the shelf.
- **Don't make assumptions**:
  - All along the way, we had great employees that were involved in various aspects of this wire fraud. But each person involved made an assumption that was incorrect. Here are some examples of assumptions that hurt us:
  - The first person getting the email assumed it was from our vendor.
  - We had a process step to call the vendor and verify the wire change instructions. Instead we received a call verifying the wire. We assumed it was from the correct party.
  - A person in accounting questioned the wire. But her supervisor felt that if it was approved by purchasing it must be ok.
  - Two other people approving and reviewing wires assumed that if it got this far it must be ok.
- **Pay better attention to the details and don't take shortcuts:**
  - This is a big one. We are all busy and we all want to clear things off of our desks. I think the criminals count on that. They counted on us accepting the call from them confirming the wire.
  - The name on the wire was different. If we had slowed down a little, we would have picked up that change.
  - We had a system in place. But several people in the process took a little shortcut. It was all of us taking these little shortcuts that hurt us.
- **Incorporate into our system a better process to review risk. Have written checklists that are followed and reviewed.**
  - We now have a risk team. We have greatly expanded our use of experts and consultants to review risks throughout our system. For example, we have contracted with a company to simulate emails that look legitimate but may have a virus attached.

Takeaways from Victims – Lessons Learned

- **This fraud also required us to think about risks in a different way.**

- **We have now improved our training and our checklists:**
  - We find that written checklist are a big help.

- **We have a much stronger system now to review any changes requested from customers:**
  - We are spending more time training employees to feel confident and to push back if they see a problem. They don't have to go along just because the supervisor says it is ok.

- **Don't be so confident:**
  - Candidly, we were overconfident. We thought we had good systems in place. We had identified risks from weather and had added generators. We identified risk on checks and had added positive pay. (This actually caught some fraudulent checks.) We thought we had a good process to avoid wire fraud.
  - We became too confident it would not be us.
  - Now we are much more open to the idea that the criminals are very smart and very creative.

"Trust But Verify"

Global Security Incident Notification Triggers & Contacts

Security Incident Trigger Events

Incident Type	Incident Examples
PC, Laptop or Portable Storage Device Lost or Stolen	Device lost or stolen – No Sensitive Data Device lost or stolen –Confidential Data Exposed Device lost or stolen – PII Data Exposed
Credit Card Violation	Unauthorized Access to logical or physical CC Data (CHD)
Social Engineering	Spoofing – request for disbursements Phone calls into **company** Emails and Spam into **company**
Attack	Denial of Service Network Attack Criminal Attack
Security Technology Vulnerability	Security Logging Encryption & Key Management Zero Day Exploits, Patches and Bugs (i.e.: BASH)
Unauthorized Access	Unauthorized Use of Privileged Accounts Unauthorized Application or Account access Excessive Login Attempt
Wireless	Corporate Wireless breach or unauthorized access Business Unit(s) Wireless breach or unauthorized access
Privacy Violation	PII Data that is improperly used **company** employee(s)
Fraud (Transaction)	Gift Card Internal Gift Card External e-Certs Internal e-Certs External Credit Card Fraud – External Credit Card Fraud – Internal (misuse of corporate card)
Privacy Complaint	Complaint regarding the processing of PII Data
Security Violations	Security Policy Violations (Internal only) Workplace Violence Physical Security
Third Party	Security Incident initiated by a 3rd Party Vendor.

Security Incident Contact Numbers

Upon identification of any Incident, or perceived incident, you should immediately notify the Service Desk and they will initiate the Incident Response Process and escalate as necessary.

Notification Method	Toll Free #
U.S. Service Desk	(123)456-7899 Choose option #1
International Service Desk	+44 (0) 23 1234567 Choose option #1 +44 (0) 23 1234567 Choose option #1
Global Online Report	Complete an online incident report: http://servicedesk.com

Security Incident Team Escalation Numbers

First Contact O: 123-456-7899
M: 123-456-7899
Second contact O: 123-456-7899
M: 123-456-7899
Third Contact O: +44 (0) 123 456 789
M: +44 (0) 123 456 789

Electronic Crimes Task Force/Cyber Working Groups

- The ECTF model relies on trusted partnerships between the law enforcement community, the private sector, and members of academia to combat cyber crime through information sharing, coordinated investigations, technical expertise, and training (NCFI).

- These ECTFs are a strategic alliance of over 4,000 private sector partners; over 2,500 international, federal, state and local law enforcement partners; and over 350 academic partners.

- Since inception, the ECTFs have prevented over $13 billion in potential losses to victims and arrested approximately 10,000 individuals.

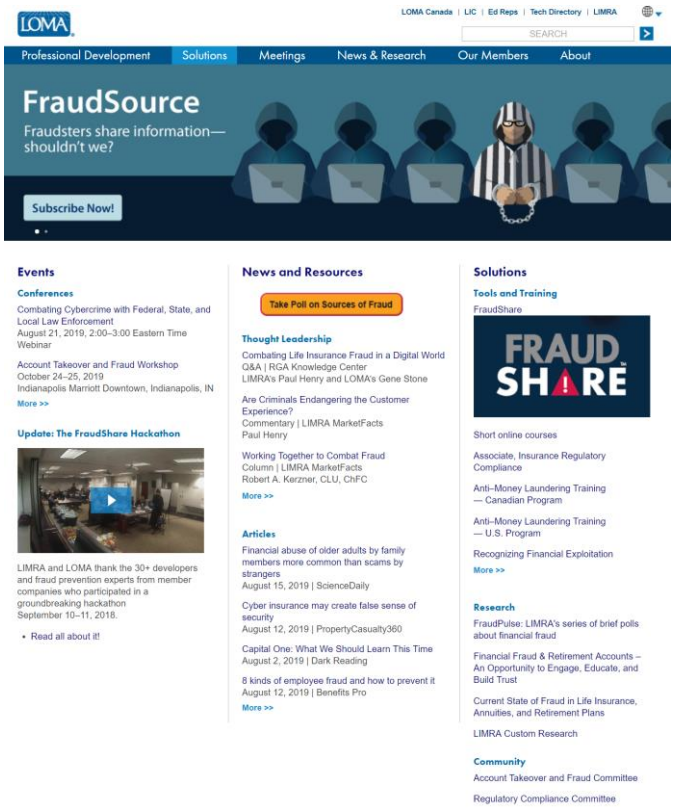
National Computer Forensic Institute

- The NCFI facility will train approximately **1,500** state and local law enforcement officers, prosecutors, and judges annually.
- Since its opening in May 2008, NCFI has trained approximately **8,100** individuals.
- This includes **5,200** state and local investigators, **2,300** prosecutors and **600** Judges from all 50 states, three U.S. territories and over 2,000 agencies nationwide.

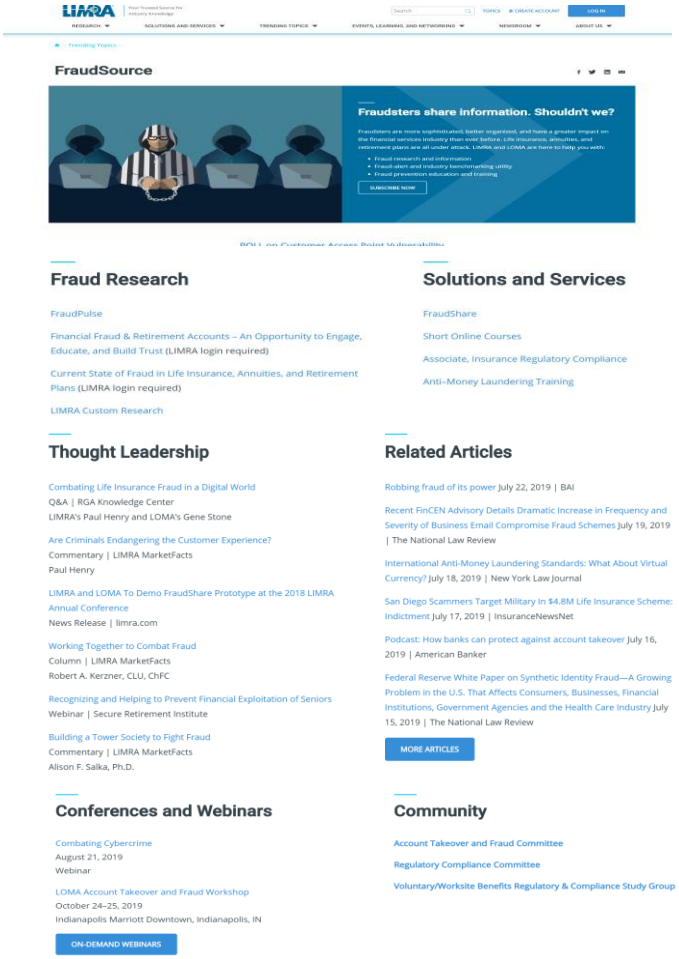
Partners in Crime

- Technical Investigative Unit (TIU)
  - 11 Towns
  - 2 Academic Institution
- Shoreline Technical Investigative Unit (STIU)
  - 10 Towns
  - 2 Academic Institution
- Eastern Technical Investigative Unit (ETIU)
  - 6 Towns
  - 1 Academic Institution
- Connecticut Center for Digital Investigations (CDI)
  - 10 towns
  - 2 Academic Institutions
- Connecticut State Police(CSP)
  - State's Incident Response Team (4 person)

LIMRA/LOMA FraudSource

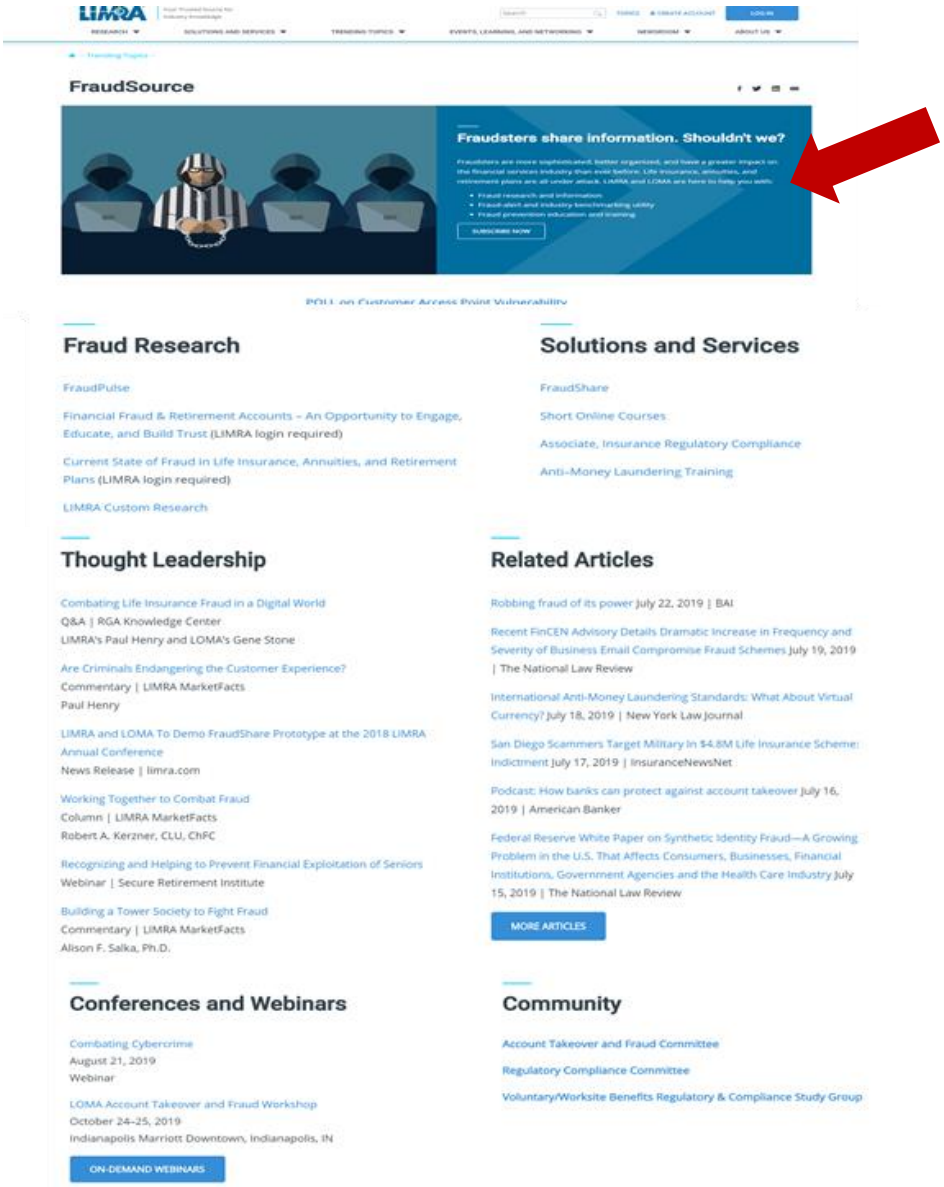


www.LOMA.org/FraudSource



www.LIMRA.com/FraudSource

LIMRA/LOMA FraudSource



Your Trusted Source for *Industry Knowledge*

LOMA®

LIMRA®

Thank You!