Security Threats & Breaches
Cybersecurity Webinar Series

Speaker: Jeremiah O’Connor
Hostess: Kara Sullivan
Cisco Networking Academy
3 October 2018
Welcome to the 2nd session of the Cybersecurity webinar series

- Use the Q and A panel to ask questions.
- Use the Chat panel to communicate with attendees and panelists.
- A link to a recording of the session will be sent to all registered attendees.
- Please take the feedback survey at the end of the webinar.
• Cybersecurity Webinar Series

• Session 1: Cybersecurity Basics, Recording available
• Session 2: Security Threats & Breaches, Today!
• Session 3: A Career in Cybersecurity, 18 October

Access Series @
So you want to become a Cybersecurity Professional??

Jeremiah O’Connor – Cisco Security – October 2018
Agenda

1. Introduction
2. Background
3. Offensive
4. Defensive
5. Current Research/Roadmap
6. Conclusion
$ WHOIS Jeremiah

- Mad Scientist at Cisco Security
- M.S. in Computer Science, University of San Francisco
- Europol Virtual Currency Task Force
- National Cyber Investigative Joint Task Force
- OpenDNS ➔ Security and Trust
- Proud SFSPCA pitbull puppy owner
Cisco Security

- Data Science & Network Security
- Big Security Data
- DNS Traffic:
  - ~100B DNS requests per day
  - NEWLY SEEN DOMAINS!!
- Daily Tasks:
  - Detection Algorithms
  - Security Data Analysis
  - Distributed Systems
  - Big Data Engineering
  - Data Viz
Background
So you want to be a CyberSec Pro!?!?
WARNING!!!

IT'S NOT LIKE THE MOVIES!!!
IT'S MORE LIKE...

A REAL LIFE VIDEO GAME!!!
PHYSICAL SECURITY
Consultancy & Planning
Surveys & Audits
Response & Protection

RED TEAM
Testing Your Preparedness
Exercising Your Response

BLUE TEAM
Reinforcing Your Security
Building Your Resilience

CYBER SECURITY
Threat Modeling & Forensics
Advanced Cyber Defence
Risk Analysis
Offensive (Breaking)
OWASP Top 10 2017 Released

The OWASP Top 10 - 2017 is now available.

OWASP Top 10 Most Critical Web Application Security Risks

The OWASP Top 10 is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

We urge all companies to adopt this awareness document within their organization and start the process of ensuring that their web applications minimize these risks. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.

Translation Efforts

The OWASP Top 10 has been translated to many different languages by numerous volunteers. These translations are available as follows:
BUG BOUNTY LIST

A comprehensive, up to date list of bug bounty and disclosure programs from across the web curated by the Bugcrowd researcher community.
THE MOST TRUSTED HACKER-POWERED SECURITY PLATFORM

More Fortune 500 and Forbes Global 1,000 companies trust HackerOne to test and secure the applications they depend on to run their business.

GET STARTED  SEE HOW IT WORKS
Incident report on memory leak caused by Cloudflare parser bug

23 Feb 2017 by John Graham-Cumming.

Last Friday, Tavis Ormandy from Google's Project Zero contacted Cloudflare to report a security problem with our edge servers. He was seeing corrupted web pages being returned by some HTTP requests run through Cloudflare.

It turned out that in some unusual circumstances, which I'll detail below, our edge servers were running past the end of a buffer and returning memory that contained private information such as HTTP cookies, authentication tokens, HTTP POST bodies, and other sensitive data. And some of that data had been cached by search engines.

For the avoidance of doubt, Cloudflare customer SSL private keys were not leaked. Cloudflare has always terminated SSL connections through an isolated instance of NGINX that was not affected by this bug.

We quickly identified the problem and turned off three minor Cloudflare features (email obfuscation, Server-side Excludes, and Automatic HTTPS Rewrites) that were all using the parser. We have fixed the issue, rolled the changes back, and published a patch yesterday to stop any potential further leaks. We continue to monitor the situation.
### Threat Agents / Attack Vectors

<table>
<thead>
<tr>
<th>App Specific</th>
<th>Exploitability: 3</th>
</tr>
</thead>
</table>

Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users. **Injection flaws** occur when an attacker can send hostile data to an interpreter.

### Security Weakness

<table>
<thead>
<tr>
<th>Prevalence: 2</th>
<th>Detectability: 3</th>
</tr>
</thead>
</table>

Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries. Injection flaws are easy to discover when examining code. Scanners and fuzzers can help attackers find injection flaws.

### Impacts

<table>
<thead>
<tr>
<th>Technical: 3</th>
<th>Business</th>
</tr>
</thead>
</table>

Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover. The business impact depends on the needs of the application and data.

---

### Is the Application Vulnerable?

An application is vulnerable to attack when:

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures.
- Some of the more common injections are SQL, NoSQL, OS command,

---

### How to Prevent

Preventing injection requires keeping data separate from commands and queries.

- The preferred option is to use a safe API, which avoids the use of the interpreter entirely or provides a parameterized interface, or migrate to use Object Relational Mapping Tools (ORMs).

**Note:** Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data, or executes hostile data with EXECUTE IMMEDIATE or exec().

- Use positive or "whitelist" server-side input validation. This is not a complete defense as many applications require special characters, such as text areas
Choose the card that works for you

Cash Rewards credit card - $150 $200 online bonus offer >
4.5/5 (43,662)

Travel Rewards credit card - 20,000 25,000 online bonus points offer >
4.4/5 (11,756)

BankAmericard® credit card - Low intro APR offer >
4.3/5 (13,255)

Premium Rewards® credit card - Premium Rewards, flexible options >
4.4/5 (310)

Certified by J.D. Power for providing “An Outstanding Mobile Banking Experience.” Get the latest app
SQL Injection.

User-Id: srinivas
Password: mypassword

```
select * from Users where user_id= 'srinivas' and password = 'mypassword'
```

User-Id: ` OR 1= 1; /*
Password: */--

```
select * from Users where user_id= ' ` OR 1 = 1; /* ' and password = ' */--'
```

9lessons.blogspot.com
Top 10-2017 A7-Cross-Site Scripting (XSS)

Threat Agents / Attack Vectors

<table>
<thead>
<tr>
<th>App Specific</th>
<th>Exploitability: 3</th>
<th>Security Weakness</th>
<th>Detectability: 3</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated tools can detect and exploit all three forms of XSS, and there are freely available exploitation frameworks.</td>
<td>XSS is the second most prevalent issue in the OWASP Top 10, and is found in around two thirds of all applications. Automated tools can find some XSS problems automatically, particularly in mature technologies such as PHP, J2EE / JSP, and ASP.NET.</td>
<td>The impact of XSS is moderate for reflected and DOM XSS, and severe for stored XSS, with remote code execution on the victim's browser, such as stealing credentials, sessions, or delivering malware to the victim.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Is the Application Vulnerable?

There are three forms of XSS, usually targeting users' browsers:

- **Reflected XSS**: The application or API includes unvalidated and unescaped user input as part of HTML output. A successful attack can allow the attacker to execute arbitrary HTML and JavaScript in the victim's browser. Typically the user will need to interact with some malicious link that points to an attacker-controlled page, such as malicious watering hole websites, advertisements, or similar.

- **Stored XSS**: The application or API stores unsanitized user input that is viewed at a later time by another user or an administrator. Stored XSS is often considered a high or critical risk.

- **DOM XSS**: JavaScript frameworks, single-page applications, and APIs that dynamically include attacker-controllable data to a page are vulnerable to DOM XSS.

How to Prevent

Preventing XSS requires separation of untrusted data from active browser content. This can be achieved by:

- Using frameworks that automatically escape XSS by design, such as the latest Ruby on Rails, React JS. Learn the limitations of each framework's XSS protection and appropriately handle the use cases which are not covered.

- Escaping untrusted HTTP request data based on the context in the HTML output (body, attribute, JavaScript, CSS, or URL) will resolve Reflected and Stored XSS vulnerabilities. The OWASP Cheat Sheet 'XSS Prevention' has details on the required data escaping techniques.

- Applying context-sensitive encoding when modifying the browser document on the client side acts against DOM XSS. When this cannot be avoided,
1. Perpetrator discovers a website having a vulnerability that enables script injection.

2. Perpetrator injects the website with a malicious script that steals each visitor's session cookies.

3. For each visit to the website, the malicious script is activated.

4. Visitor's session cookie is sent to perpetrator.
Kevin Beaumont
@GossiTheDog

eNET, on AS10297 - the network which started the BGP DNS hijack yesterday - had a device with Cisco Smart Install enabled. Smart Install allows anybody, with no credentials, to retrieve the device config remotely - including admin credentials.

Tony Adams @tadams0620
@cloudflare reported that the @myetherwallet BGP hijack originated from AS10297, @enetinc of Columbus, OH. Was SIET used to gain a foothold in ENET with lateral movement to routing gear? Shodan shows eNet has...
AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet

Audacious BGP seizure of Route 53 IP addys followed by crypto-cyber-heist

By Shaun Nichols in San Francisco 24 Apr 2018 at 19:04

Updated Crooks today hijacked internet connections to Amazon Web Services systems to ultimately steal a chunk of alt-coins from online cryptocurrency website MyEtherWallet.com.
The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

What leaks in practice?  

How to stop the leak?
Defensive (Building)
MALWARE
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.
We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Contact Us

Check Payment

Decrypt
THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY


IT WAS A perfect sunny summer afternoon in Copenhagen when the world’s largest shipping conglomerate began to lose its mind.

The headquarters of A.P. Møller-Maersk sits beside the breezy, cobblestoned esplanade of Copenhagen’s harbor. A ship’s mast carrying the Danish flag is planted by the building’s northeastern corner, and six stories of blue-tinted windows look out over the water, facing a dock where the Danish royal family parks its yacht. In the building’s basement, a data center that processes a torrent of container ship manifests...
**Steps**

1. The threat actor compromises a website.
2. Users connect to the compromised website and the cryptomining script executes.
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor.
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins.
THE STRUCTURE OF A BOTNET

C&C-SERVERS
(COMMAND & CONTROL)

INFECTED COMPUTERS
(ZOMBIES)

SOURCE: BLOGG.TKJ.SE
HOW EXPLOIT KITS WORK

1. Malicious link in a phishing email sends user to a compromised site
2. Webpage hosting the exploit kit
3. Kit scans for vulnerability to exploit (e.g., Flash)

1. Malicious ad on a legitimate site redirects user to compromised site

Start here...
Delivery Vectors

Email

Search Engine Ads

Communication Channel
New Cyber Threat Landscape

- Lower barrier of entry for attackers these days
- Open sourcing of exploits/malware
- Nation-State level relations evolving (ie. Russia, North Korea, Iran, etc.)
- Technology evolving/IOT
- Lack of CyberSec Professionals!!
Cisco Umbrella
“Newly Seen”

Shallow Layer
- FQDN Classification
- Fetch Page Source
- HTML Content Classification

Deeper Layers
- Malicious Infrastructure Classification
- Blocking/Threat Intelligence/LE Reporting

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Detected Site: lcoinbase.com
Score: 0.9941726922988892
Corpus hit: Coinbase/www.coinbase.com.html
Timestamp: 2016–08–01T01:44:05.296Z
Detected Site: www.myetnerwallet.com.send-status.info
Timestamp: 2018-09-26 01:49:47.140102
Score: 0.994288027287
Corpus Hit: MyEtherWallet/myetherwallet-com.org.html
Detected Site: paxful.com.pl
Score: 0.974158465862
Corpus Hit: Paxful/2fa-paxful.com_login.html
Create New Wallet

Enter a password

Do NOT forget to save this!

Create New Wallet

This password encrypts your private key. This does not act as a seed to generate your keys. You will need this password + your private key to unlock your wallet.

How to Create a Wallet • Getting Started
Inside North Korea’s Hacker Army

The regime in Pyongyang has sent hundreds of programmers to other countries. Their mission: Make money by any means necessary. Here’s what their lives are like.
Sutton's law

Sutton's law states that when diagnosing, one should first consider the obvious. It suggests that one should first conduct those tests which could confirm (or rule out) the most likely diagnosis. It is taught in medical schools to suggest to medical students that they might best order tests in that sequence which is most likely to result in a quick diagnosis, hence treatment, while minimizing unnecessary costs. It is also applied in pharmacology, when choosing a drug to treat a specific disease you want the drug to reach the disease. It is applicable to any process of diagnosis, e.g. debugging computer programs. Computer-aided diagnosis provides a statistical and quantitative approach.

A more thorough analysis will consider the false positive rate of the test and the possibility that a less likely diagnosis might have more serious consequences. A competing principle is the idea of performing simple tests before more complex and expensive tests, moving from bedside tests to blood results and simple imaging such as ultrasound and then more complex such as MRI then specialty imaging. The law can also be applied in prioritizing tests when resources are limited, so a test for a treatable condition should be performed before an equally probable but less treatable condition.

The law is named after the bank robber Willie Sutton, who reputedly replied to a reporter’s inquiry as to why he robbed banks by saying “because that’s where the money is.” In Sutton's 1976 book Where the Money Was, Sutton denies having said this.1[2]

A similar idea is contained in the physician's adage, “When you hear hoofbeats, think horses, not zebras.”
WannaCry's bitcoins were converted to Monero, researchers say

Three months after WannaCry impacted more than 300,000 computers in over 150 countries, the bitcoins paid by victims have been

(Getty)
Why Is North Korea So Interested in Bitcoin?

September 11, 2017 | by Luke McNamara

In 2016 we began observing actors we believe to be North Korean utilizing their intrusion capabilities to conduct cyber crime, targeting banks and the global financial system. This marked a departure from previously observed activity of North Korean actors employing cyber espionage for traditional nation state activities. Yet, given North Korea’s position as a pariah nation cut off from much of the global economy – as well as a nation that employs a government bureau to conduct illicit economic activity – this is not all that surprising. With North Korea’s tight control of its military and intelligence capabilities, it is likely that this activity was carried out to fund the state or personal coffers of Pyongyang’s elite, as international sanctions have constricted the Hermit Kingdom.

Now, we may be witnessing a second wave of this campaign: state-sponsored actors seeking to steal bitcoin and other virtual currencies as a means of evading sanctions and obtaining hard currencies to fund the regime. Since May 2017, we have observed North Korean actors target at least three South Korean cryptocurrency exchanges with the suspected intent of stealing funds. The spearphishing we have observed in these cases often targets personal email accounts of employees at digital currency exchanges, frequently using tax-themed lures and deploying malware (PEACHPIT and similar variants) linked to North Korean actors suspected to be responsible for intrusions into global banks in 2016.
AlienVault labs recently analysed an application compiled on Christmas Eve 2017. It is an Installer for software to mine the Monero crypto-currency. Any mined currency is sent to Kim Il Sung University in Pyongyang, North Korea.

The Installer copies a file named intelservice.exe to the system. The filename intelservice.exe is often associated with crypto-currency mining malware. Based on the
North Korea Bitten by Bitcoin Bug

Financially Motivated Campaigns Reveal New Dimension of the Lazarus Group

Darien Huss
Bitcoin WARNING: ISIS using cryptocurrency to fund reign of terror as Bitcoin price soars

As the Bitcoin price soars, grotesque terror network ISIS has been using the cryptocurrency to fund its reign of terror.

By JOE BARNES
PUBLISHED: 09:33, Sun, Dec 17, 2017 | UPDATED: 09:33, Sun, Dec 17, 2017
Coinhoarder Case
The latest global phishing attacks aimed at #bitcoin users via Google Ads @owen_lystrup @jmoconnor415 @CiscoSecurity ow.ly/SL1d309xp77

8:10 AM - 3 Mar 2017

fabio @rodfabio1 · Mar 4
@blockchain @owen_lystrup @jmoconnor415 @CiscoSecurity i m trying to login into my wallet but i dont recieve email of confirmation ??

Leo @leomanu79 · Mar 4
@blockchain @owen_lystrup @jmoconnor415 @CiscoSecurity can you tell why login confirmation emails are not being sent? cant login to wallet!

Gallab @bokzamo · Mar 4
@blockchain i m trying to login into my wallet but i dont recieve email of
Bitcoin Wallet Phish Boom Reveals Rogue Hosters

By Artsiom Holub, Dina Mahjeub and Jerefniah O’Connor
June 20, 2016

Whois Emails Used for More Bitcoin Phishing

With the rise of Bitcoin technology, more and more attackers will be attempting to spoof these online wallets in order to steal credentials. OpenDNS is at the forefront of detecting these types of new anomalies. By pivoting on the identified malicious domains and leveraging OpenDNS data, we were able to identify at least 6 emails used to register domains for blockchain spoof campaigns. Below is a selection of the emails in question, which have been and, as of this writing, are still being used to register more than 100 Bitcoin and blockchain phishing domains.

mopadrehop@thraml.com
stopracuho@thraml.com
tdorost@thraml.com
boalbits@yandex.com
iselbtc@yandex.com
iselbtc1234567@gmail.com
All your files have been encrypted!

All your documents (databases, texts, images, videos, musics etc.) were encrypted. The encryption was done using a secret key that is now on our servers.

To decrypt your files you will need to buy the secret key from us. We are the only on the world who can provide this for you.

What can I do?

Pay the ransom, in bitcoins, in the amount and wallet below. You can use LocalBitcoins.com to buy bitcoins. Email Us at *********@***********

Bitcoin Amount: 0.5

Wallet for Sending Bitcoins:
1FfrH3KokFDpg5TABBW8sySe6nM4mFTNvT
All your files have been encrypted!

All your documents (databases, texts, images, videos, musics etc.) were encrypted. The encryption was done using a secret key that is now on our servers.

To decrypt your files you will need to buy the secret key from us. We are the only on the world who can provide this for you.

Note that every 6 hours, a random file is permanently deleted. The faster you are, the less files you will lose.

Also, in 96 hours, the key will be permanently deleted and there will be no way of recovering your files.

What can I do?

Contact us by email telling your ID (below) and wait for us to send the instructions.

Contact us by: ransom64@sigaint.org

As a proof, you can send one encrypted file, so we will send it back decrypted. Use it as a guarantee that we can decrypt your files.

Next Russian Roulette file deletion:
5 hours, 52 minutes and 17 seconds

Last (0) file deleted:

Your ID: 8B18FF14 Got the code? AA5D5974D3

Copy to clipboard

Time until total loss: 3 days, 23 hours, 52 minutes and 17 seconds
## Online builder

You must have **license** to use builder.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver address</td>
<td></td>
<td>Receiver address should be put in with protocol and without slash on end. Example: <a href="http://onionsite.onion/p.php">http://onionsite.onion/p.php</a></td>
</tr>
<tr>
<td>Payment page</td>
<td></td>
<td>Payment page should be written in the same way.</td>
</tr>
<tr>
<td>Encryption method</td>
<td>AES 256</td>
<td>In locker message word <code>{IDENTY}</code> would be replaced with User ID so that you can construct links to the payment page. Example <a href="http://ytrfyedvdasv.onion/payment.php?ID=AAAA-AAAA-AAAA">http://ytrfyedvdasv.onion/payment.php?ID=AAAA-AAAA-AAAA</a></td>
</tr>
<tr>
<td>Default decryptor</td>
<td>Automatic</td>
<td></td>
</tr>
<tr>
<td>UAC bypass</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>Locker message</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Create build][Download panel]

[Panel setup short guide]
Multiple cybercriminal operations

BTC

Phishing Victims

Phishing Operator

Purchase RaaS

RaaS Operator

Ransomware

BTC as Ransomware payment

USD to buy BTC

Ransomware victims
Law Enforcement (Public)

Effective Collaboration

Private Sector (Industry/Private)

Wallets/Exchanges (Financial/Private)
Buying bitcoins instantly?

I sell BTC P2P for $639.25/BTC...you'll spend at least $200/BTC more if you don't buy P2P.

Moneypak to BTC by [deleted] in DarkNetMarkets

Fuck that I'll buy and sell BTC P2P all day...all the scammers out there can die a slow painful death!
Welcome to Reddit,
the front page of the internet.

and subscribe to one of thousands of communities.

there doesn't seem to be anything here
The World's Most Popular Bitcoin Wallet

100 Million+ Transactions
12 Million+ Wallets
140+ Countries Served

CREATE YOUR WALLET
or
LOGIN NOW
Details for 91.220.101.14
Hosting 0 malicious domains for 1 week

<table>
<thead>
<tr>
<th>Prefix</th>
<th>ASN</th>
<th>Network Owner Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>91.220.101.0/24</td>
<td>AS 34259</td>
<td>HIGHLOADSYSTEMS, UA 86400</td>
</tr>
</tbody>
</table>

| Requester geo distribution | NG | US | IN | IE | ?? | FR | NL | VN | GH | UA | PH | CA | GB | DZ | EG | PE | MY | ZA | RU | RO | PL | EU | HK | JP | LK | BR | AU | EE | TH | BD |
|---------------------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|                           | 38.30% | 12.06% | 5.67% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% | 2.84% |

<table>
<thead>
<tr>
<th>Predicted requester geo distribution</th>
</tr>
</thead>
</table>

| Requester geo distribution (normalized) | NG | US | IN | IE | ?? | FR | NL | VN | GH | UA | PH | CA | GB | DZ | EG | PE | MY | ZA | RU | RO | PL | EU | HK | JP | LK | BR | AU | EE | TH | BD |
|----------------------------------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|                                        | 46.29% | 18.81% | 6.44% | 5.91% | 2.79% | 2.77% | 2.12% | ?? | 1.72% | 1.65% | 1.56% | 1.39% | 1.32% | 1.30% | 0.92% | 0.79% | 0.61% | 0.54% | 0.39% | 0.38% | 0.33% | 0.29% | 0.28% | 0.26% | 0.26% | 0.18% | 0.12% | 0.11% | 0.10% | 0.09% |

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
### General Information

<table>
<thead>
<tr>
<th>AS number</th>
<th>34259 (AS34259 / ASN34259)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>TOV Highload Systems</td>
</tr>
<tr>
<td>Country</td>
<td>Ukraine (UA)</td>
</tr>
<tr>
<td>Allocation date</td>
<td>2007-09-24 by RIPE</td>
</tr>
<tr>
<td>Number of IPv4 addresses</td>
<td>1,024</td>
</tr>
<tr>
<td>ASRank (based on number of IPv4)</td>
<td>27,922</td>
</tr>
<tr>
<td>Number of IP prefixes</td>
<td>3 (IPv4) 0 (IPv6)</td>
</tr>
<tr>
<td>AS has bogon prefixes</td>
<td>No</td>
</tr>
<tr>
<td>Number of peers</td>
<td>2 (IPv4) 0 (IPv6)</td>
</tr>
</tbody>
</table>

### Hosting Summary

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of domains hosted</td>
<td>129</td>
</tr>
<tr>
<td>Number of adult domains hosted</td>
<td>2</td>
</tr>
<tr>
<td>Number of name servers hosted</td>
<td>66</td>
</tr>
<tr>
<td>Number of SPAM hosts hosted</td>
<td>0</td>
</tr>
<tr>
<td>Number of open proxies hosted</td>
<td>0</td>
</tr>
<tr>
<td>Number of mail servers hosted</td>
<td>0</td>
</tr>
<tr>
<td>Number of IDN domains hosted</td>
<td>0</td>
</tr>
<tr>
<td>Number of domains in Alexa top million</td>
<td>12</td>
</tr>
</tbody>
</table>
Known domains hosted by 91.220.101.113

bloakchian.info  https-blockchian.in  https-blockchians.in  http-blockchian.in  https-blockchain.net  www.https-blockchians.in  https-blockchian.in
https-blockchain.in  www.blockchain.biz  blockchain-home.info  https-blockchian.net  blokchiai.net  blokchian.net  https-blokchian.co
blokchian.info  blockchian.biz

Known domains hosted by 91.220.101.106

Welcome!

Site vblockchain.info just created.
Real content coming soon.
### Latest Blocks

<table>
<thead>
<tr>
<th>Height</th>
<th>Age</th>
<th>Transactions</th>
<th>Total Sent</th>
<th>Relayed By</th>
<th>Size (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>455744</td>
<td>6 minutes</td>
<td>1930</td>
<td>23,040.46 BTC</td>
<td>BitFury</td>
<td>998.23</td>
</tr>
<tr>
<td>455743</td>
<td>20 minutes</td>
<td>1649</td>
<td>13,981.18 BTC</td>
<td>SlushPool</td>
<td>998.11</td>
</tr>
<tr>
<td>455742</td>
<td>23 minutes</td>
<td>2638</td>
<td>28,523.42 BTC</td>
<td>AntiPool</td>
<td>998.17</td>
</tr>
<tr>
<td>455741</td>
<td>51 minutes</td>
<td>2246</td>
<td>20,388.90 BTC</td>
<td>BitFury</td>
<td>998.13</td>
</tr>
</tbody>
</table>

### New to Bitcoin?

Like paper money and gold before it, bitcoin and ether allow parties to exchange value. Unlike their predecessors, they are digital and decentralized. For the first time in history, people can exchange value without intermediaries which translates to greater control of funds and lower fees.
The World's Most Popular Bitcoin Wallet

100 Million+ Transactions
12 Million+ Wallets
140+ Countries Served
This certificate has been verified for the following uses:

- SSL Client Certificate
- SSL Server Certificate

### Issued To
- Common Name (CN): sni237902.cloudflaressl.com
- Organization (O): <Not Part Of Certificate>
- Organizational Unit (OU): Domain Control Validated

### Issued By
- Common Name (CN): COMODO ECC Domain Validation Secure Server CA 2
- Organization (O): COMODO CA Limited
- Organizational Unit (OU): <Not Part Of Certificate>

### Period of Validity
- Begins On: April 5, 2017
- Expires On: October 12, 2017

### Fingerprints
<table>
<thead>
<tr>
<th>Domain</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>blockchain.link</td>
<td>Malware, Phishing</td>
</tr>
<tr>
<td>allportal.top</td>
<td>Malware</td>
</tr>
<tr>
<td>aviabiletz.click</td>
<td>Malware</td>
</tr>
<tr>
<td>aviabiletz.site</td>
<td>Malware</td>
</tr>
<tr>
<td>aviabiletz.space</td>
<td>Malware</td>
</tr>
<tr>
<td>aviabiletz.click</td>
<td>Malware</td>
</tr>
<tr>
<td>blockchain.org</td>
<td>Malware</td>
</tr>
<tr>
<td>c2p.click</td>
<td>Malware</td>
</tr>
<tr>
<td>card-2-card.space</td>
<td>Malware</td>
</tr>
<tr>
<td>card-2card.space</td>
<td>Malware</td>
</tr>
<tr>
<td>card-to-card.click</td>
<td>Malware</td>
</tr>
<tr>
<td>card-to-card.space</td>
<td>Malware</td>
</tr>
<tr>
<td>card2-card.space</td>
<td>Malware</td>
</tr>
<tr>
<td>card2card.click</td>
<td>Malware</td>
</tr>
<tr>
<td>card2card.pro</td>
<td>Malware</td>
</tr>
<tr>
<td>card2card.site</td>
<td>Malware</td>
</tr>
<tr>
<td>card2card.space</td>
<td>Malware</td>
</tr>
<tr>
<td>card2card.website</td>
<td>Malware</td>
</tr>
<tr>
<td>card2card.transfer.space</td>
<td>Malware</td>
</tr>
<tr>
<td>car2card.transfer.space</td>
<td>Malware</td>
</tr>
<tr>
<td>cardto-card.space</td>
<td>Malware</td>
</tr>
<tr>
<td>cardto-card.click</td>
<td>Malware</td>
</tr>
<tr>
<td>cardtransfer.space</td>
<td>Malware</td>
</tr>
<tr>
<td>l-aviabiles.online</td>
<td>Malware</td>
</tr>
<tr>
<td>pay2card.space</td>
<td>Malware</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>bing-ads.org</td>
<td>Malware</td>
</tr>
<tr>
<td>bing-advertise.net</td>
<td>Malware</td>
</tr>
<tr>
<td>bjxinheyuan.com</td>
<td>Malware</td>
</tr>
<tr>
<td>blogsblogos.com</td>
<td>Malware</td>
</tr>
<tr>
<td>blokcheain.info</td>
<td>Malware</td>
</tr>
<tr>
<td>blokcheain.info</td>
<td>Malware</td>
</tr>
<tr>
<td>blokcheien.info</td>
<td>Malware</td>
</tr>
<tr>
<td>blokcheien.info</td>
<td>Malware</td>
</tr>
<tr>
<td>blokchenin.info</td>
<td>Malware</td>
</tr>
<tr>
<td>blokchiean.com</td>
<td>Malware</td>
</tr>
<tr>
<td>blokchieans.info</td>
<td>Phishing</td>
</tr>
<tr>
<td>blokchiein.info</td>
<td>Malware</td>
</tr>
<tr>
<td>blokchines.info</td>
<td>Malware</td>
</tr>
<tr>
<td>blokchnies.info</td>
<td>Malware</td>
</tr>
<tr>
<td>blokchiein.info</td>
<td>Malware</td>
</tr>
<tr>
<td>busscar.net</td>
<td>Malware</td>
</tr>
</tbody>
</table>
## LATEST BLOCKS

<table>
<thead>
<tr>
<th>Height</th>
<th>Age</th>
<th>Transactions</th>
<th>Total Sent</th>
<th>Relayed By</th>
<th>Size (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>469254</td>
<td>6 minutes</td>
<td>2455</td>
<td>9,183.61 BTC</td>
<td>F2Pool</td>
<td>999.98</td>
</tr>
<tr>
<td>469253</td>
<td>14 minutes</td>
<td>2305</td>
<td>3,889.59 BTC</td>
<td>BTCC Pool</td>
<td>989.22</td>
</tr>
<tr>
<td>469252</td>
<td>15 minutes</td>
<td>2126</td>
<td>15,091.60 BTC</td>
<td>BTC.com</td>
<td>998.21</td>
</tr>
<tr>
<td>469251</td>
<td>24 minutes</td>
<td>2198</td>
<td>60,390.68 BTC</td>
<td>GBMiners</td>
<td>999.25</td>
</tr>
</tbody>
</table>

### NEW TO BITCOIN?

Like paper money and gold before it, bitcoin and ether allow parties to exchange value. Unlike their predecessors, they are digital and decentralized. For the first time in history, people can exchange value without intermediaries which translates to greater control of funds and lower fees.

### SEARCH

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

- **Address / ip / SHA hash**
  - **Search**
Could not verify this certificate because the issuer is unknown.

<table>
<thead>
<tr>
<th>Issued To</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>blockcharin.info</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>&lt;Not Part Of Certificate&gt;</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>&lt;Not Part Of Certificate&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issued By</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>Let's Encrypt Authority X3</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Let's Encrypt</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>&lt;Not Part Of Certificate&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Period of Validity</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Begins On</td>
<td>May 31, 2017</td>
</tr>
<tr>
<td>Expires On</td>
<td>August 29, 2017</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fingerprints</th>
<th></th>
</tr>
</thead>
</table>
LATEST BLOCKS

<table>
<thead>
<tr>
<th>Height</th>
<th>Age</th>
<th>Transactions</th>
<th>Total Sent</th>
<th>Relayed By</th>
<th>Size (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>469763</td>
<td>8 minutes</td>
<td>2093</td>
<td>2,747.18 BTC</td>
<td>BTC.com</td>
<td>998.25</td>
</tr>
<tr>
<td>469762</td>
<td>8 minutes</td>
<td>2365</td>
<td>17,170.63 BTC</td>
<td>F2Pool</td>
<td>999.83</td>
</tr>
<tr>
<td>469761</td>
<td>19 minutes</td>
<td>1846</td>
<td>8,391.48 BTC</td>
<td>F2Pool</td>
<td>999.98</td>
</tr>
<tr>
<td>469760</td>
<td>25 minutes</td>
<td>2322</td>
<td>2,153.08 BTC</td>
<td>BTC.TOP</td>
<td>999.08</td>
</tr>
</tbody>
</table>

NEW TO BITCOIN?

Like paper money and gold before it, bitcoin and ether allow parties to exchange value. Unlike their predecessors, they are digital and decentralized. For the first time in history, people can exchange value without intermediaries which translates to greater control of funds and lower fees.

SEARCH

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...
Could not verify this certificate because the issuer is unknown.

**Issued To**
- Common Name (CN): `blockchraim.info`
- Organization (O): `<Not Part Of Certificate>`
- Organizational Unit (OU): `<Not Part Of Certificate>`

**Issued By**
- Common Name (CN): Let's Encrypt Authority X3
- Organization (O): Let's Encrypt
- Organizational Unit (OU): `<Not Part Of Certificate>`

**Period of Validity**
- Begins On: June 3, 2017
- Expires On: September 1, 2017

**Fingerprints**
The account 18xaP8AmpRDAUiqiXsELtKQFzicC78BnYh was stolen at 2017-11-11 22:41:12 from a blockchain.info wallet. The 2FA was activated and no seed stored on any pc. Also not backup. The 2FA was with google authenticator on a smartphone. The bitcoin is being splitted on two accounts: 13wahvu3FP8LK8P51UmEkhBUhyC7mzkrn3 and 1KDFTGoWXceezxqUk5whjnViPEkCdJeU1V. If you check the movements of these wallets you can see they are doing the same to many accounts. The blockchain support answered with a copy/paste generic email, but not more help. The police is already informed and let us see if they can do something...this is frustrating. How can this happen?
2FA Bypass

Victim enters credentials on phishing site

Malicious actor intercepts credentials and forwards to legitimate domain

Victim enters credentials on phishing site

Malicious actor obtains 2FA code

Victim enters 2FA code staying on phishing page

2FA prompt

Malicious actor obtains 2FA code

Login Successful - welcome test22@gmail.com
The account 18xaP8AmpRDAUiqiXsELtKFQzic78BnYh was stolen at 2017-11-11 22:41:12 from a blockchain.info wallet. The 2FA was activated and no seed stored on any pc. Also not backup. The 2FA was with google authenticator on a smartphone. The bitcoin is being split on two accounts: 13wahvu3FP8LK8P51UmEkhBUhyC7mzkrm3 and 1KDFTG0WXceeZxxUK5wHjnVlPeKClJeU1V. If you check the movements of these wallets you can see they are doing the same to many accounts. The blockchain support was with a copy/paste generic email, but not more help. The police is already informed and let us see if they can do something…this is frustrating. How can this happen?
COINHOARDER: Tracking a Ukrainian Bitcoin Phishing Ring DNS Style

This post is authored by Jeremiah O’Connor and Dave Maynor with contributions from Artiom Halub and Austin McBride.

EXECUTIVE SUMMARY

Cisco has been tracking a bitcoin theft campaign for over 6 months. The campaign was discovered internally and researched with the aid of an intelligence sharing partnership with Ukraine Cyberpolice. The campaign was very simple and after initial setup the attackers needed only to continue purchasing Google AdWords to ensure a steady stream of victims. This campaign targeted specific geographic regions and allowed the attackers to amass millions in revenue through the theft of cryptocurrency from victims. This campaign demonstrates just how lucrative these sorts of malicious attacks can be for cybercriminals. Additionally, the revenue generated by these sorts of attacks, can then be reinvested into other cybercriminal operations.

THE COINHOARDER CAMPAIGN

On February 24, 2017, Cisco observed a massive phishing campaign hosted in Ukraine targeting the popular Bitcoin wallet site blockchain.info with a client request magnitude of over 200,000 client queries. This campaign was unique in that adversaries leveraged Google Adwords to poison user search results in order to steal users' wallets. Since Cisco observed this technique, it has become increasingly common in the wild with attackers targeting many different crypto wallets and exchanges via malicious ads.

Cisco identified an attack pattern in which the threat actors behind the operation would establish a “gateway” phishing link that would appear in search results among Google Ads. When searching for crypto-related keywords such as “blockchain” or “bitcoin wallet,” the spoofed links would appear at the top of search results. When clicked, the link would redirect to a “lander” page and serve phishing content in the native language of the geographic region of the victim’s IP address.
Russian bulletproof hosting filled with #phish @coinbase #phishing w/ @globalsign SSL certs and IDNs, xn--conbase-pza[.]com --> coïnbase[.]com, coinbase[.]im @CiscoSecurity @SecurityGuyPhil

Philip Martin @SecurityGuyPhil · 11 Nov 2017
Replying to @jmcoonner415 @coinbase and 2 others
Thanks @jmcoonner415 we’ve been working in takedowns for these domains and certs since they flagged in our systems around 3 AM (PST). Still pending actions from the various involved parties (including @globalsign)

Jeremiah O’Connor @jmcoonner415 · 11 Nov 2017
Outstanding!! You’re the man 😊😊😊

GlobalSign @globalsign · 13 Nov 2017
Thanks for reporting this Jeremiah. I have forwarded this onto our phishing abuse team to have a look at. Hopefully we can get them down asap!

GlobalSign @globalsign · 15 Nov 2017
Update: We have revoked the cert and are considering adding ‘coinbase’ to our phishing filter. @coinbase, we are here for you!
COINBASE ADDS 100K NEW USERS IN JUST 24 HOURS AS BITCOIN PRICES CONTINUE TO CLIMB

Binance: World's top cryptocurrency exchange adds 240,000 users in just one hour

Hong Kong based Binance sees unprecedented growth and even places a temporary ban on new traders

Shaft Musaddique | Thursday 11 January 2018 12:45 GMT | 3 comments

569 shares
Binance - Exchange The World

Create Account | Already Registered? Login

Binance Referral Program
It pays to have friends!
Promotion Starts: 2017.10.27 4:00AM (UTC)

Binance Lists IOSToken (IOST) (01-24)

BNB/BTC
0.0011895 $13.10
Volume: 4,076.12 BTC

TRX/BTC
0.00000609 $0.07
Volume: 10,638.70 BTC

VEN/BTC
0.00063599 $7.00
Volume: 7,498.55 BTC

XRP/BTC
0.00011739 $1.29
Volume: 3,223.24 BTC

Binance Lists PIVX (PIVX) (01-23)

BTC Markets
ETH Markets
USDT Markets

Pair | Last Price | 24h Change | 24h High | 24h Low
--- | --- | --- | --- | ---
IOST/BTC | 0.00000870 / $0.10 | 9.71% | 0.00001355 | 0.00000765
ETH/BTC | 0.094750 / $1,043.20 | 2.64% | 0.095200 | 0.091900
This certificate has been verified for the following uses:

- SSL Client Certificate
- SSL Server Certificate

Issued To
- Common Name (CN): sni182946.cloudflaressl.com
- Organization (O): <Not Part Of Certificate>
- Organizational Unit (OU): Domain Control Validated

Issued By
- Common Name (CN): COMODO ECC Domain Validation Secure Server CA 2
- Organization (O): COMODO CA Limited
- Organizational Unit (OU): <Not Part Of Certificate>

Period of Validity
- Begins On: February 3, 2018
- Expires On: August 12, 2018

Fingerprints
<table>
<thead>
<tr>
<th>Prefix</th>
<th>ASN</th>
<th>Network Owner Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>85.93.0.0/19</td>
<td>AS 12586</td>
<td>ASGHOSTNET, DE 86400</td>
</tr>
<tr>
<td>85.93.20.0/24</td>
<td>AS 57509</td>
<td>LL-INVESTMENT-LTD, BG 86400</td>
</tr>
</tbody>
</table>

Known domains hosted by 85.93.20.58

```
```
Fellow Binancians,

To ensure a safe crypto community, we can’t simply play defense. We need to actively prevent any instances of hacking before they occur, as well as follow through after-the-fact. Even though the hacking attempt against Binance on March 7th was not successful, it was clear it was a large-scale, organized effort. This needs to be addressed.

Binance is offering a $250,000 USD equivalent bounty to anyone who supplies information that leads to the legal arrest of the hackers involved in the attempted hacking incident on Binance on March 7th, 2018.

The first person to supply substantial information and evidence that leads to the legal arrest of the hackers, in any jurisdiction, will receive the equivalent of $250,000 USD in BNB. The exchange rate will be determined at time of transfer.

Please supply detailed information to bounty@binance.com as well as to your local law enforcement agencies.

If your local laws allow, you may remain anonymous.

If multiple sources/segments of data are used to lead to the final legal arrests, the bounty may be split between sources. Binance reserves all rights to split the bounty amount, solely at our discretion.

Furthermore, Binance has currently allocated the equivalent of $10,000,000 USD in crypto reserves for future bounty awards against any illegal hacking attempts on Binance. We have also invited other exchanges and crypto businesses to join our initiative. We welcome their participation.

Thank you for your support and effort in keeping our community safe.

Binance
Known domains hosted by 185.110.132.214

hitbtc.com myetherwallet.com porloneix.com www.myetherwallet1.domen-hosting.org bitrtrx.com myetherwalletr.com
myetherwallet2.domen-hosting.org wallbtc.com binnance.com blockchain.com blueitrade.net myetherwallet.com myetherwallet.com
www.myetherwallet.domen-hosting.org blockchain.com cpanel.kraken.com myetherwallet1.domen-hosting.org
kucin1.domen-hosting.org myetherwallet5.domen-hosting.org myetherwallet1.domen-hosting.org exmo.me www.exoo1.domen-hosting.org
myetherwallet.com getachub1.domen-hosting.org blueitrade2.domen-hosting.org exmo.me kraken.com kucin1.domen-hosting.org
i-myetherwallet.org bitfinex.com ns1.handhost.com blockchain.com ethereumwallet.com exmo.com hitbtc.com
exmp.im webmail.exmo.com exmo.com erxmo.com exmd.com myetherwallet.com myetherwallet.com wallbtc.com exmc.com mycrypt.com
poloneix.com binnance.com blockchain.com exmo.me myetherwallet.com bitrtrx.com mycrypt.com mynncrypto.com
blockchain.com freewallet.com karken.com warlbt.com 1myetherwallet.net binnance.com dinanne.com hitbtc.com myetherwallet24.ru
bleitrade.com myetherwalletru.com mynetriewallet.ru webmail.exmd.org kraken.eu localethereum.com mycrypt.com
webmail.exmd.org kraken.com net myetherwallet-c.com binnance.com bitrtrx.org exno.eu myetherwallet0.com binnance.com blockchain.net
binnance.com myetherwallet.ru.com wallbtc.com cpanel.blockchain.net exmo.net kraken.com krakke.com krakken.com myetherwalletru.com
qolonex.com porloneix.com webdisk.porloneix.com binnance.com cpanel.karne.co exmp.su hitbtc.com 0myetherwallet.com mycrypt.com
blockchain.com info 1myetherwallet.com i-myetherwallet.info mycrypt.org myetherwallet.com hitbtc.com.ru com myetherwallet.org myetherwallet.org
poloneix.com webdisk.localethereum.com binnance.com bitrtrx.org myetherwallet.info polymex.com
bitrtrx.com exmd.org ng.exmp.org bittrex.com blockchain.info blockchaininfo.com mycrypt.org myetherwallet.info myetherfun
myetherwallet-c.com webdisk.blockchain.info mycrypt.com myetherwallet.com blockchain.org binance.com e-cex.com
1-myetherwallet.info cpanel.binance.com liqji.com binnance.com cpanel.poloneix.com exno.eu bitrtrx.org liqji.com su myetherwallet-t.com
porloneix.com webmail.poloneix.co 1-myetherwallet.info cpanel.bitcortex.com bitcortex.com exmp.org kraken.com exno.co myetherwallet.com
myetherwalletru.info gethub.org exmo.co xn--myetherwlet-3kb80f.com block-chaininfo.com cpanel.exmo.co binnance.com erxmo.me
exmo.com myetherwallet.com blockchain.info bitrtrx.com liqji.com su polymex.com exmo.co kraken.com wallbtc.com wallbtc.com
wallbtc.com liqji.com su bitrtrx.com myetherwallet.com liqji.com su blockchain.com kraken.com webdisk.kraken.com handhost.com myetherwallet.org blockchain.com
cpanel.exmd.org kraken.com myetherwallet.org myetherwallet.info xn--myetherwallet-seb.com myetherwallet.com exno.com myetherwallet.info
karke.com myetherwallet.fun kracken.ru.com liqji.com su myetherwallet.info webdisk.exmp.co blockchaininfo.com cn-blockchain.com exmd.co
exmp.co
<table>
<thead>
<tr>
<th>Prefix</th>
<th>ASN</th>
<th>Network Owner Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>176.119.0/24</td>
<td>AS 58271</td>
<td>VSERVER-AS, UA 86400</td>
</tr>
</tbody>
</table>

Known domains hosted by 176.119.1.88

www.bing-analytics.stream  
www.win-rar-software.com  
xn--mymoneo-v63c.com  
bing-analytics.stream  
sheapshift.com  
win-rar-software.com  
www.xn--mymoneo-v63c.com  
www.xn--mythwallet-srbc.com  
win-rar-affiliate.review  
win-rar-download.com  
www.bing-analytics.online  
xn--mythwallet-srbc.com

Known domains hosted by 176.119.5.227

xn--mononero-81d.com  
xn--yoneo-e1bb9q.com  
www.adobeiservice.center  
xn--yoneo-e1bb9q.com  
xn--mononero-81d.com  
xn--mononaddress-deb.org  
www.xn--mymoneo-f63c.com  
adobeiservice.center  
xn--monoroadress-deb.org  
www.doubleclick-analytics.me  
www.client342x34-doubleclick-analytics.bid  
www.client342x234-doubleclick-analytics.bid  
client342x234-doubleclick-analytics.bid  
www.client2fsf9g-doubleclick-analytics.bid  
www.xn-hpshif-2dd2993e.com  
xn-shpshif-5055f.com  
www.clientxf9g-doubleclick-analytics.bid  
www.xn-shapshif-3b.llo  
xn--shapshif-3b.llo  
www.clientxog9g-doubleclick-analytics.bid  
www.xn--mymoneo-y5c3c.com  
xn--shapshif-3b.llo  
clientxf9g-doubleclick-analytics.bid  
www.client342x34-doubleclick-analytics.bid  
xn--shapshif-8k7d.com  
xn-shpshif-ox0d7i.com  
www.xn--ymoner-2s7b49b.com  
www.xn--ymoner-2s7b49b.com

Known domains hosted by 176.119.5.229

www.client342x234-doubleclick-analytics.bid  
www.clientxf9g-doubleclick-analytics.bid  
www.client2fsf9g-doubleclick-analytics.bid  
www.login-to-office365.com  
www.clientss3f9g-doubleclick-analytics.bid  
www.clientxf9g-doubleclick-analytics.bid  
www.doubleclick-analytics.bid  
www.clientxf9g-doubleclick-analytics.bid  
www.clientofsf9g-doubleclick-analytics.bid  
www.doubleclick-analytics.bid  
www.doubleclick-analytics.bid  
www.xn--mytherwalle-3qb7278g.com  
login-to-office365.com  
www.xn--mytherwalle-ek5f.com  
clientxf9g-doubleclick-analytics.bid  
www.clientx929g-doubleclick-analytics.bid  
www.clientxf029g-doubleclick-analytics.bid  
xn--mytherwalle-3qb7278g.com  
www.client342x34-doubleclick-analytics.bid  
doubleclick-analytics.bid  
doubleclick-analytics.online  
xn--mytherwalle-ek5f.com

Blockchain is the world’s most popular digital wallet. We are on a mission to build a more open, accessible, and fair financial future, one piece of software at a time.

LOG IN
SIGN UP

#1 DIGITAL WALLET
100 MILLION+ TRANSACTIONS
27 MILLION+ WALLETS
Could not verify this certificate because the issuer is unknown.

**Issued To**
- Common Name (CN): sni40538.cloudflaresssl.com
- Organization (O): <Not Part Of Certificate>
- Organizational Unit (OU): Domain Control Validated
- Serial Number: 00:F5:DA:F8:9C:84:13:C0:5B:AD:01:17:8E:04:06:35:3C

**Issued By**
- Common Name (CN): COMODO ECC Domain Validation Secure Server CA 2
- Organization (O): COMODO CA Limited
- Organizational Unit (OU): <Not Part Of Certificate>

**Period of Validity**
- Begins On: August 13, 2018
- Expires On: February 19, 2019

**Fingerprints**
<table>
<thead>
<tr>
<th>Prefix</th>
<th>ASN</th>
<th>Network Owner Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.45.64.0/21</td>
<td>AS 50673</td>
<td>SERVERIUS–AS, NL 86400</td>
</tr>
<tr>
<td>37.252.14.0/23</td>
<td>AS 50673</td>
<td>SERVERIUS–AS, NL 86400</td>
</tr>
</tbody>
</table>

Known domains hosted by 5.45.69.74


Known domains hosted by 37.252.14.242

<table>
<thead>
<tr>
<th>Prefix</th>
<th>ASN</th>
<th>Network Owner Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>181.174.166.0/24</td>
<td>AS 52469</td>
<td>Offshore Racks S.A, PA 86400</td>
</tr>
</tbody>
</table>

**Known domains hosted by 181.174.166.198**

meyetherwallct.com myehtcrwallet.com myehtewallet.com mychterwallct.com www.mycythevxrvallet.com myehtervvallet.com
meychwrallet.com mychterwallet.com myehtewalletct.com mychterwalletct.com www.mycythevxrvallet.com myehtervvallet.com

**Known domains hosted by 181.174.166.98**

index-tradenet.com my-etherwalllogin.com idexmarkets-official.com my-etherwallsecure.com idex-marketsin.com idexmarket-logins.com
indexmarkets-login1.com icex.market idex-marketsecure.com myether-walletsecure.com idexmarket-official.com myeth-walletlogin.com
idex-marketslogin.com myetherwallet-official.com myetherwallets-official.com ides.market hitbtcsite.com mythewalletts.com etherdealtain.com
hitbtclogin.com idwx.market idex.market idez.market ided.market

**Known domains hosted by 190.14.37.17**

advertise-google-adwords.com adwords-adverts.org advertise-google-ads.com adwords-google-adverts.com antiddos4.today
advertising-google-adwords.com google-adwords.company www.tipprbtc.org advertising-adwords-google.com tipprbtc.org
Domains Associated with jimmyluis@tutanota.com

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Security Categories</th>
<th>Content Categories</th>
<th>Last Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>baitaddress.org</td>
<td>Phishing</td>
<td></td>
<td>Current</td>
</tr>
<tr>
<td>xn--ymoner-2s7b49b.com</td>
<td>Phishing</td>
<td></td>
<td>Current</td>
</tr>
<tr>
<td>xn--btaddress-g5a.org</td>
<td></td>
<td></td>
<td>Current</td>
</tr>
<tr>
<td>xn--cinbse-zc8bxn.com</td>
<td></td>
<td></td>
<td>Current</td>
</tr>
<tr>
<td>xn--coibase-r13c.com</td>
<td></td>
<td></td>
<td>Current</td>
</tr>
<tr>
<td>xn--litevalt-x1b.net</td>
<td></td>
<td></td>
<td>Current</td>
</tr>
</tbody>
</table>

Showing 6 of 6 results
#Necurs is now trying to scam peoples’ cryptocurrencies. The mymyetherwallet[.]com domain was registered today.

```
---
cosmi@cosmina.ro
To: j7997a93b@jaeson.net
New transaction

You have a new transaction on your Ethereum Wallet.
Login to check your balance:
https://mymyetherwallet.com/#view-wallet-info
---
```

3:14 PM - 17 Oct 2017

1 Retweet 4 Likes 2 Comments 1 Reply 4 Likes
The first Android Clipper was updated and says Hi to Dr.Web

Spreads via scam coin web sites with updated targets list. Clipper replaces user clipboard of digital wallet number for attacker's:
-BTC
-Steam
-XMR
-ETH
-LTC
-Payeer wallet

news.drweb.com/show/?i=12739&…
kudos @jmoconnor415
MEGA Chrome Extension Hacked - Detailed Timeline of Events

by SerHack

TLDR;

On 4 September at 14:30 UTC, an unknown attacker managed to hack into MEGA's Google Chrome web store account and upload a malicious version 3.39.4 of an extension to the web store, according to a blog post published by the company. Upon installation or auto-update, the malicious extension asked for elevated permissions to access personal information, allowing it to steal login/register credentials from ANY websites like Amazon, Github, and Google, along with online wallets such as MyEtherWallet and MyMonero, and Idex.market cryptocurrency trading platform. The
!!! WARNING !!!!! PLEASE PAY ATTENTION!!

LATEST VERSION OF MEGA CHROME EXTENSION WAS HACKED.

Version: 3.39.4

It catches your username and password from Amazon, GitHub, Google, Microsoft portals!! It could catch #mega #extension #hacked@x0rz

10:16 AM - Sep 4, 2018
1,424  1,744 people are talking about this

17.23 UTC on 4th September 2018
The official Twitter account of Monero (XMR) posted a warning, to steer clear of MEGA.

PSA: The official MEGA extension has been compromised and now includes functionality to steal your Monero:
reddit.com/r/Monero/comments...

10:23 AM - Sep 4, 2018

Don't use MEGA Chrome Extension version ...
The MEGA Chrome extension is updated with functionality to steal your...
reddit.com
CRYPTOCURRENCY MEETS LAW ENFORCEMENT AT EUROPOL’S 5TH VIRTUAL CURRENCIES CONFERENCE

21 June 2018

News Article

Largest ever European law enforcement cryptocurrency event brought together some 300 participants

Between 19-21 June 2018, over 300 participants from 40 countries convened in The Hague for the 5th Virtual Currencies Conference organised by Europol’s European Cybercrime Centre (EC3) to discuss one of the hottest topics of this year: virtual currencies, and how to foster the legitimate use of this virtual monetary system often abused by hackers, international drug dealers and the money movers of organised crime.

While the majority of participants came from law enforcement agencies and public prosecutors’ offices, key experts from financial institutions and the IT industry were also present. The event gathered policy makers, academics, and representatives from civil society to exchange views, foster dialogue and share best practices.
Individuals in crypto attacks are much “softer” targets than going after established financial institutions. Criminals from all realms, organized crime and nation-state are taking notice of this. As crypto asset technologies develop and enable millions to become their own bank. It is important to keep in mind that when you’re your own bank, security is imperative!

We are witnessing a restructuring of the criminal economy and the methodology to launder their newly stolen digital assets. Anti-money laundering laws coming into play just moving 1 BTC making converting large amounts of crypto to fiat currencies no easy task. Criminals will have to figure out how to convert their money to FIAT via other means without tipping off law enforcement agencies of their fraudulent identity.
3. Ukraine, Netherlands, Eastern Europe, Russia is a hot bed for many types of financial attacks and home to known bulletproof hosting providers. In 2017 we have witnessed a substantial rise specifically in crypto targeting in the region.
В Україні необхідно визначитися зі статусом криптовалюти», - Сергій Демедюк (ФОТО)

Спеціалісти з кіберполіції повідомляють, що де-факто, за всіма ознаками криптовалюта може відноситись до електронних коштів - одиниць вартісті, які зберігаються на електронному пристрої і приймаються, як засіб платежу. У той же час контроль за її транзакціями забезпечується криптографічним захистом.

Відтак, незважаючи на те, що по своїй сутності існування й обіг криптовалюти базується на основах фінансової піраміди, кіберполіція підтримує ідею легалізації криптовалюти в Україні, а також процесу її майнінгу (цьонайменше, що прирівняти її до електронних коштів). Також підтримується і ідея використання технології Blockchain у державному та приватному секторах.
Conclusion
Enjoy! The Process
LOVE TO LEARN
WORK HARD
BUT REMEMBER TO
HAVE FUN!!
Questions?

@jmoconnor415
jeoconnno@cisco.com
You can enroll today to learn more @ http://bit.ly/introsecurity