

Malware as a business model

Platform Criminality

Robert Fischer
Systems Engineer

Jason Mauchley
Account Manager



The Web of Profit

Conservative estimates in The Web of Profit 2018 research show cybercriminal revenues worldwide of at least \$1.5 trillion – equal to the GDP of Russia. In fact, if cybercrime was a country it would have the 13th highest GDP in the world. This \$1.5 trillion figure includes:

- \$860 billion – Illicit/illegal online markets
- \$500 billion – Theft of trade secrets/IP
- \$160 billion – Data trading
- \$1.6 billion – Crimeware-as-a-Service
- \$1 billion – Ransomware

Cybersecurity Ventures predicts cybercrime damages will cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015.

<https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/>

<https://www.thesststore.com/blog/cybercrime-pays-new-study-finds-cybercriminal-revenues-hit-1-5-trillion-annually/>

11 top cybersecurity statistics at-a-glance

- **90% of remote code execution attacks are associated with cryptomining.**
- **92% of malware is delivered by email.**
- **56% of IT decision makers say targeted phishing attacks are their top security threat.**
- **77% of compromised attacks in 2017 were fileless.**
- **The average ransomware attack costs a company \$5 million.**
- **It takes organizations an average of 191 days to identify data breaches.**
- **69% of companies see compliance mandates driving spending.**
- **88% companies spent more than \$1 million on preparing for the GDPR.**
- **25% of organizations have a standalone security department.**
- **54% of companies experienced an industrial control system security incident**
- **61% of organizations have experienced an IoT security incident**

<https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html>

Estimates on the impact of cybercrime

- Cybercrime will cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015
- "Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm"
- Cybercrime will cost the world in excess of \$6 trillion annually by 2021, making it more profitable than the global trade of all major illegal drugs combined.

<https://www.prnewswire.com/news-releases/cyberattacks-are-the-fastest-growing-crime-and-predicted-to-cost-the-world-6-trillion-annually-by-2021-300765090.html>

<https://blogs.cisco.com/financialservices/how-to-prevent-the-bank-robbery-no-one-can-see>

Expected industry response

- Global spending on cybersecurity products and services will exceed \$1 trillion cumulatively from 2017 to 2021
- Average of 3% of capex (capital expenditures) that's focused on IT on security.
 - Versus Cybercriminals found to be reinvesting 20% of their revenues into further crime...
- Cybersecurity unemployment rate effectively zero
 - 6 million jobs globally by 2019
 - 3.5 million unfilled cybersecurity positions by 2021

<https://cybersecurityventures.com/cybersecurity-market-report/>

<https://cybersecurityventures.com/cybersecurity-unemployment-rate/>

<https://blog.paloaltonetworks.com/2016/06/cybersecurity-more-threats-but-also-more-opportunities/>

<https://cybersecurityventures.com/jobs/>

Our Internet

Surface Web

Deep Web

- Comprises 90% of the internet
- Websites whose contents are not searchable by standard search engines
- Accessibly only by querying a search box within a particular website
- Includes dark webpages
- Examples: bank account sites, company intranets and registration-required sites

Dark Web

- Comprises 0.01% of the internet
- Not traceable by third parties
- Protected by encryption technologies
- Small part of the deep web that has been intentionally hidden and is inaccessible through standard web browsers
- Accessible via special browsers such as TOR (The Onion Router) project
- Also known as the Internet's underground
- Examples: Silk Road - a criminal version of eBay (shutdown by FBI twice: 2013 and 2014) and untraceable financial transactions

Cybercrime platform service examples

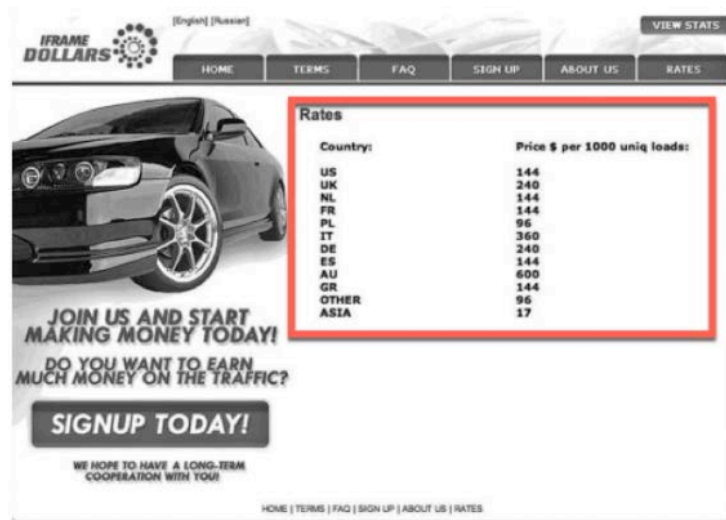
- Zero-day Adobe exploits, up to \$30,000
- Zero-day iOS exploit, \$250,000
- Malware exploit kit, \$200-\$600 per exploit
- Blackhole exploit kit, \$700 for a month's leasing, or \$1,500 for a year
- Custom spyware, \$200
- SMS spoofing service, \$20 per month
- Hacker for hire, around \$200 for a “small” hack

<https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/>

IFRAME Dollars

- How much are your hosts worth?

294 ■ *Cyber Fraud: Tactics, Techniques, and Procedures*



The screenshot shows the IFRAME DOLLARS website interface. At the top, there is a navigation menu with links for HOME, TERMS, FAQ, SIGN UP, ABOUT US, and RATES. A 'VIEW STATS' button is located in the top right corner. The main content area features a large image of a black Bentley Continental GT on the left. To the right of the car is a table titled 'Rates' with two columns: 'Country:' and 'Price \$ per 1000 uniq loads:'. The table lists the following data:

Country:	Price \$ per 1000 uniq loads:
US	144
UK	240
NL	144
FR	144
PL	96
IT	360
DE	240
ES	144
AU	600
GR	144
OTHER	96
ASIA	17

Below the table, there is a promotional message: 'JOIN US AND START MAKING MONEY TODAY! DO YOU WANT TO EARN MUCH MONEY ON THE TRAFFIC? SIGNUP TODAY! WE HOPE TO HAVE A LONG-TERM COOPERATION WITH YOU!'. At the bottom of the page, there is a footer with the same navigation links: HOME | TERMS | FAQ | SIGN UP | ABOUT US | RATES.

Figure 8.12 IFrameDollars last known payout rates.

<https://unit42.paloaltonetworks.com/threat-brief-whats-driving-shift-cryptocurrency-mining-malware/>

Please don't forget IoT... Think 5G revolution (5G attack surface...)



Projections show 75.44 billion IoT devices worldwide by 2025

IoT Attacks Escalating with a 217.5% Increase in Volume

<https://www.bleepingcomputer.com/news/security/iot-attacks-escalating-with-a-2175-percent-increase-in-volume/>

<https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

Some examples of IoT attacks

- **The Mirai Botnet (aka Dyn Attack)**
 - DDOS attack takes down chunks of the 'net
 - Compromised IoT via default account/pwd via automated searches
- **Hackable Cardiac Devices from St. Jude**
 - implantable cardiac devices have vulnerabilities, that exploited, could deplete the battery or administer incorrect pacing or shocks.
- **Jeep hack**
 - Vulnerabilities that allowed research attackers total control of SUV via vehicle's CAN bus from Sprint cellular network
- **“My friend Cayla”**
 - de facto "spying device"
 - Banned by German regulators
- **CrashOverRide**
 - SCADA malware against electrical power grids
 - State sponsored

<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>

<https://phys.org/news/2017-02-germany-internet-connected-spying-doll-cayla.html>

<https://thehackernews.com/2017/06/electric-power-grid-malware.html>

Straightforward IoT security

- “Devices that cannot have their software, passwords, or firmware updated should never be implemented.
- Changing the default username and password should be mandatory for the installation of any device on the Internet.
- Passwords for IoT devices should be unique per device, especially when they are connected to the Internet.
- Always patch IoT devices with the latest software and firmware updates to mitigate vulnerabilities.”

<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>

Ransomware today



CryptoLocker **Your Personal files are encrypted!** English

Your personal files encryption produced on this computer: photos, videos, documents, etc. Encryption was produced using a unique public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that **nobody** and **never** will be able to restore files.

Private key will be destroyed on
2015-05-08 20:16:08

To obtain the private key for this computer, which will automatically decrypt files, you need pay 1 Bitcoin (~225 USD)

You can easily delete this software, but you must know that without it, you will never be able to get your original files back.

Disable your antiviruses to prevent the removal of this software.

For more information on how to buy and send bitcoins, click 'Pay with Bitcoin'. To open a list of encoded files, click 'Show Files'.

Do not delete this list, it will be used for decryption. And do not move your files.

Time left
167:49:22

Received: 0.00 BTC
Checking wallet...



Your files are encrypted by CTB-Locker

Your files are encrypted with strong encryption. Databases and other important files have been encrypted with strong encryption generated for this computer.

Encrypted on a secret Internet server and nobody can decrypt your files without a private key.

submit the payment. If you do not send money within provided time your files will be permanently encrypted and no one will be able to recover them.

Number of files that have been encrypted:
1000

Your files are encrypted

To get the key to decrypt files you have to pay **750 USD/EUR**. If payment is not made before **42h 48m 35s** decrypting files will increase **2** times and will be **1500 USD/EUR**.



WARNING

We have encrypt your files with CryptoLocker virus


! Your important files (including those on the network disk(s), USB, etc): photos, videos, documents etc, were encrypted with CryptoLocker virus. The only way to get your files back is to buy our decryption software.

Caution: Removing of CryptoLocker will not restore access to your encrypted files. The only way to save your files is to buy a decryption software. Otherwise, your files will be lost.

[Click here to buy decryption software](#)

Our website should also be accessible from one of these links:
<http://cehitmefogal@the.locker.net/buy.php?i=mdf>
<http://cehitmefogal@the.dos2k10r.org/buy.php?i=mdf>
<http://cehitmefogal@the.dos2k10r.org/buy.php?i=mdf>
<http://cehitmefogal@the.onion.cab/buy.php?i=mdf>

Frequently Asked Questions



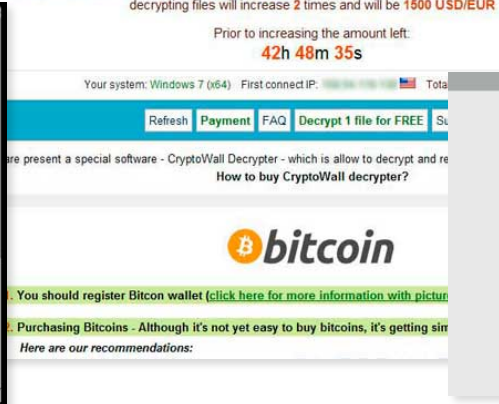
We present a special software - **Locky Decrypter** - which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.
2. You should register BitCoin wallet (simplest online wallet OR some other methods of creating wallet)
3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [LocalBitcoins.com \(WU\)](#) - Buy Bitcoins with Western Union
- [Coincafe.com](#) - Recommended for fast, simple service.



All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC = 415 USD

HEADME_F0W_DECRYPT.txt

Your computer has been locked and all your files has been encrypted with 2048-bit RSA encryption.

Instruction for decrypt:

1. Go to **DOWNLOAD FOR BROWSER AND OPEN THIS LINK** **IF NOT WORKING JUST**
2. Use **YOUR ID FOR AUTHENTICATION**
3. Pay 1 BTC (~410.635) for decryption pack using bitcoins (wallet is your ID for authentication - **IF NOT WORKING JUST**)
4. Download decrypt pack and run

----> Also at **DOWNLOAD FOR BROWSER AND OPEN THIS LINK** you can decrypt 1 file for FREE to make sure decryption is working.

Also we have ticket system inside, so if you have any questions - you are welcome.
We will answer only if you able to pay and you have serious question.

IMPORTANT: WE ARE ACCEPT ONLY(!) BITCOINS

HOW TO BUY BITCOINS:
<https://localbitcoins.com/guides/how-to-buy-bitcoins>
[https://en.bitcoin.it/wiki/Buying_Bitcoins_\(the_newbie_version\)](https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version))



150+ ransomware families

THE RISE OF RANSOMWARE



150+ RANSOMWARE FAMILIES IN THE WILD



<https://www.paloaltonetworks.com/solutions/initiatives/ransomware.html>

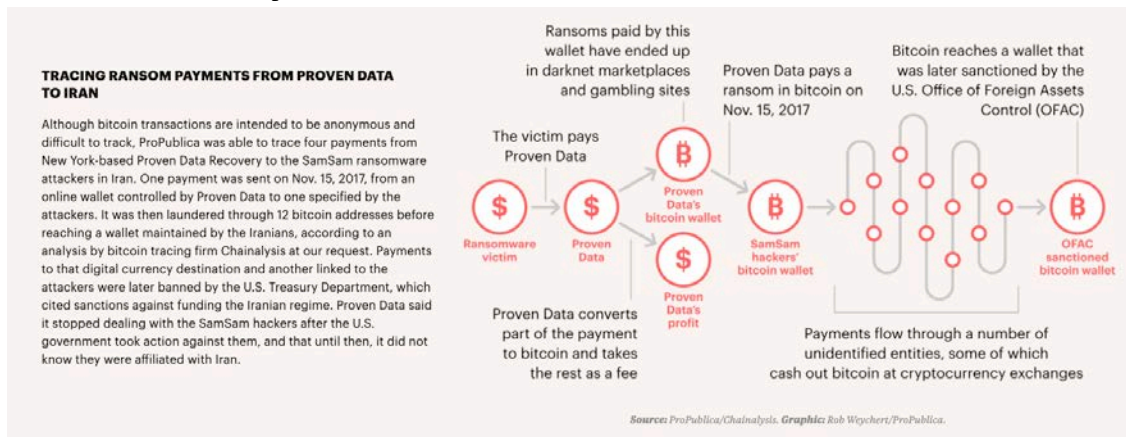


Ransomware today

- Multiple cryptovariants exist today, riding off the success of CryptoLocker
- Use of different attack vectors, such as malicious macros and exploit kits
- More sophisticated tactics, such as using anonymous networks like TOR or I2P for command and control, CAPTCHAs for limited access to payment systems, and language localization efforts
- Attacks are largely victim agnostic
- Multiple platforms targeted, including Android and OS X
- Ransomware as a Service now exists

Is the enemy of my enemy really my friend?

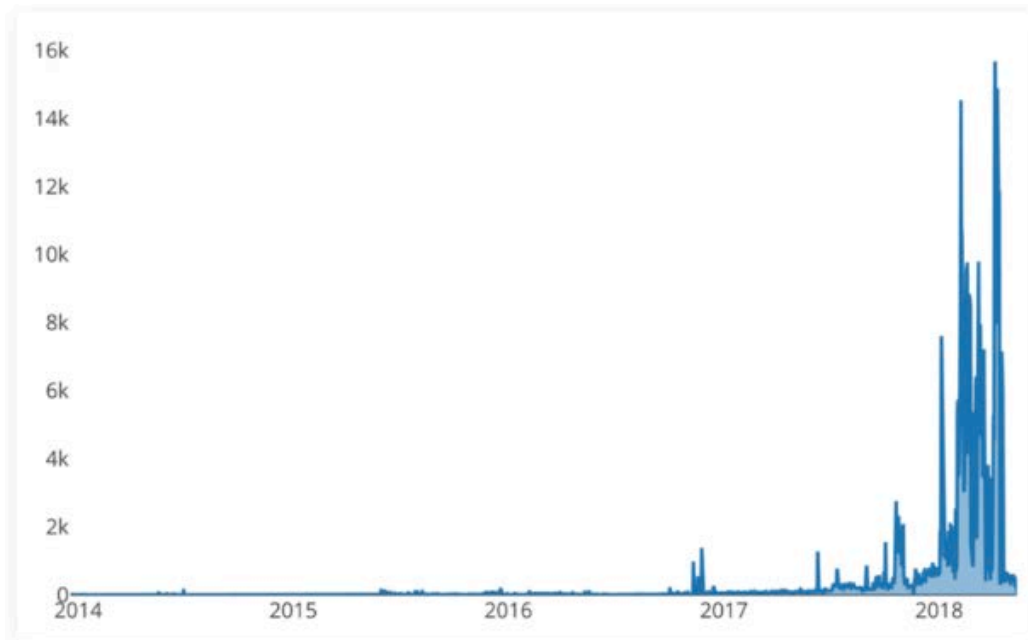
- MonsterCloud
- ProvenData
 - ProPublica was able to trace four payments from New York-based Proven Data Recovery to the SamSam ransomware attackers in Iran



<https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/>

Growth in crypto miners

- Unit42 researcher
- WildFire samples
- Does not include JavaScript type activities



What is the most commonly mined cryptocurrency?

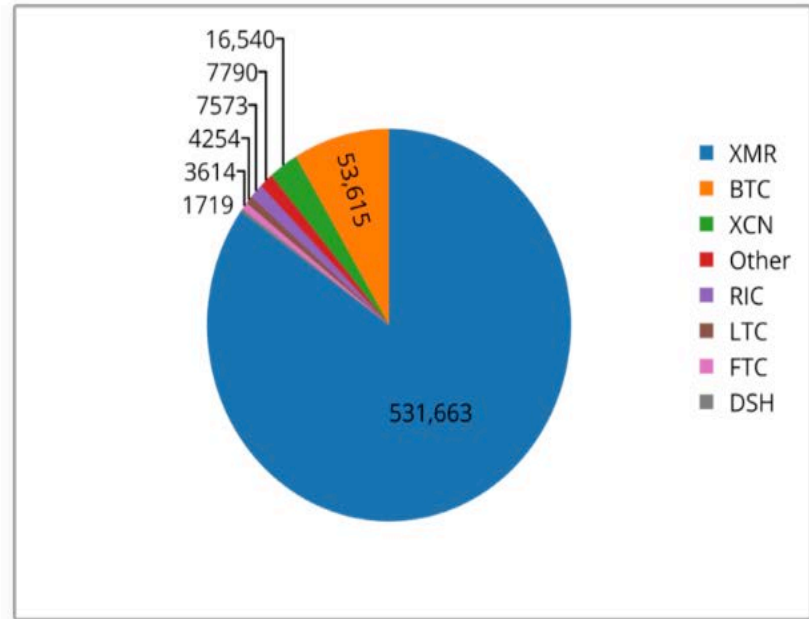
Based on roughly 470,000 unique with WildFire reports and associated PCAP data Cryptocurrency targeted

- Wallet and email addresses used when connecting to mining pools
- Mining pool

This ultimately led me to collecting the following high-level information:

- 629,126 Samples
- 3,773 Emails used to connect with mining pools
- 2,995 mining pool URLs
- 2,341 Monero (XMR) wallets
- 981 Bitcoin (BTC) wallets
- 131 Electroneum (ETN) wallets
- 44 Ethereum (ETH) wallets
- 28 Litecoin (LTC) wallets

When looking at a breakdown of what cryptocurrencies are being targeted by mining malware, we see an incredible monopoly of the Monero cryptocurrency.



A little more about this Monero miner research

- By design, wallet owner's pwd required to query balance
- By design, Monero recommends running in a 'pool'
- Query's against pools of the found wallets used to determine XMR mined

Market Rates: 2019-02-04 at 13:21 UTC

1	=	42.94
Monero (XMR) ▾		US Dollar (USD) ▾

Wallet	Mined Monero (XMR)
496ePyKvPBRWEoQiqFEaL8frWuR9XuxNj98p69ZQRxmdZZHd5KVSS24bkYY93ASAxKPxN9XmnmeCxHz9NUdvvs8eE5BP24A	88,448.53
49s5yfpFvEX8a2MBQDYxHpECwm3PVEYBq5E3i3wfZuZzbaRcgy3HVx6Qf2sJQHju5BcvF8V EohoW86VmP19nuz3YAcvLdUh	79,576.81
44N9sqilzFYX7ciXSdzYt7uBjPWLXv8Enief4icti55fdpmwmgAYF5cjb8nZRFVj2ZDzWdJdE Vi5uMDvTrYbH3Mr4DYH	56,344.09
42yJMfdGHQnJN5XEUIHydTFFPzzuhUn7xEbL89V5Zkkfch7zxaZCJhyEfe8txQmL6JY5Z1cX GtKeKbuNav7tarp7EoxsJtA	32,885.95
42NCdZTv3WDJvJTd4ny51SXQIKhUyprE9zrP5BsjJu9aeWqwunHK7aHFR9ya8gJf2REyYw BMDxMjjiAVPMBqsVHQje91y	26,359.34
44cwDVn9cQsUqb9nroJm98am2CvT8aUoKKU3ctaKatQSN0ZWC9cFyZjXg1udRXT6XVDjX7 DxThP7QYb9WwGCsNTT3XzPgUk	23,300.37
46GGhVFZq8yKkVvqsxq9Qd1vyf9BWzWPUcgExpTcPqzqczXexskd93FJ6F9q3e7H46jTnGh XqdDu1pJcvD8PpGRP2qRg5	22,519.95
42ychz53apvgs3EHMoeAyGQM3pp7EiKTLTBu1RaBj8njVfykF4v8HdPNyzAfdTDUGZfoLJM dh9Wa4u1Bm2t3f7a5FSwS4U	21,389.34
46hoCjuFZBITmqJ456NSnM3ynWt5KJYJVE8U2wUx2TVwFGmLMYNz2c4L3mQ9PRQEdVT hcHWzU3eKKFwAtELczfJuLPn9hd	20,693.71
471c2w7dyMMe51cDTKSgqoHPpg6uW6A222W6ePHXeXhwEVq5bPunnrCqCbGR3GVUXXM Z47twKtzBEokarwADLYDqPaLefXQMm	19,994.71

Total: 798613.33 XMR

Tesla

- Cloud infrastructure compromised
- Started at open Kubernetes console
 - Found storage pwds here
 - Spread to more hosted infrastructure
 - Was own miner instance (StratumBitcoin) rather than browser based
 - Tougher to ID

<https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/>

Internet accessible servers

- Monero miners on Jenkins servers
 - Leveraged a known vulnerability ([CVE-2017-1000353](#))
 - Install miner software on internet connected Jenkins servers
- Oracle WebLogic servers
 - Leveraged a known vulnerability (CVE-2017-10271)
 - Uses vuln to run powershell and download miner software
 - Eternal blue and mimikatz for lateral movement (one option)
- Apache CouchDB
 - Leveraged known vulnerabilities
 - Apache CouchDB JSON Remote Privilege Escalation Vulnerability (CVE-2017-12635)
 - Apache CouchDB _config Command Execution (CVE-2017-12636)

What can we ALL do to slow down this epidemic

- **Use MFA/2-factor auth**
 - Tokens, authenticator apps, even text if that is all that is supported (SIM highjacking risk exists though)
- **Do not become complacent/Be Present**
- **Use strong password at home and the office**
 - Pass phrases are great. Easier to remember and harder to crack
- **Manage social media settings/Be careful what you post on social media**
- **Be diligent when using emails: Never click on links in email. Don't open attachments.**
 - Try the 'o' hover trick. Usually shows you the full link so you can verify
- **At UNM forward any suspicious work emails to**
- **Pick up the phone**
- **Have "The Talk" with your kids**
- **Learn what is out there about yourself- <https://ojin.org/2019/04/08/how-to-dox-yourself/> and how to request info to be removed**

<https://www.dhs.gov/how-do-i-protect-myself-cyber-attacks>

