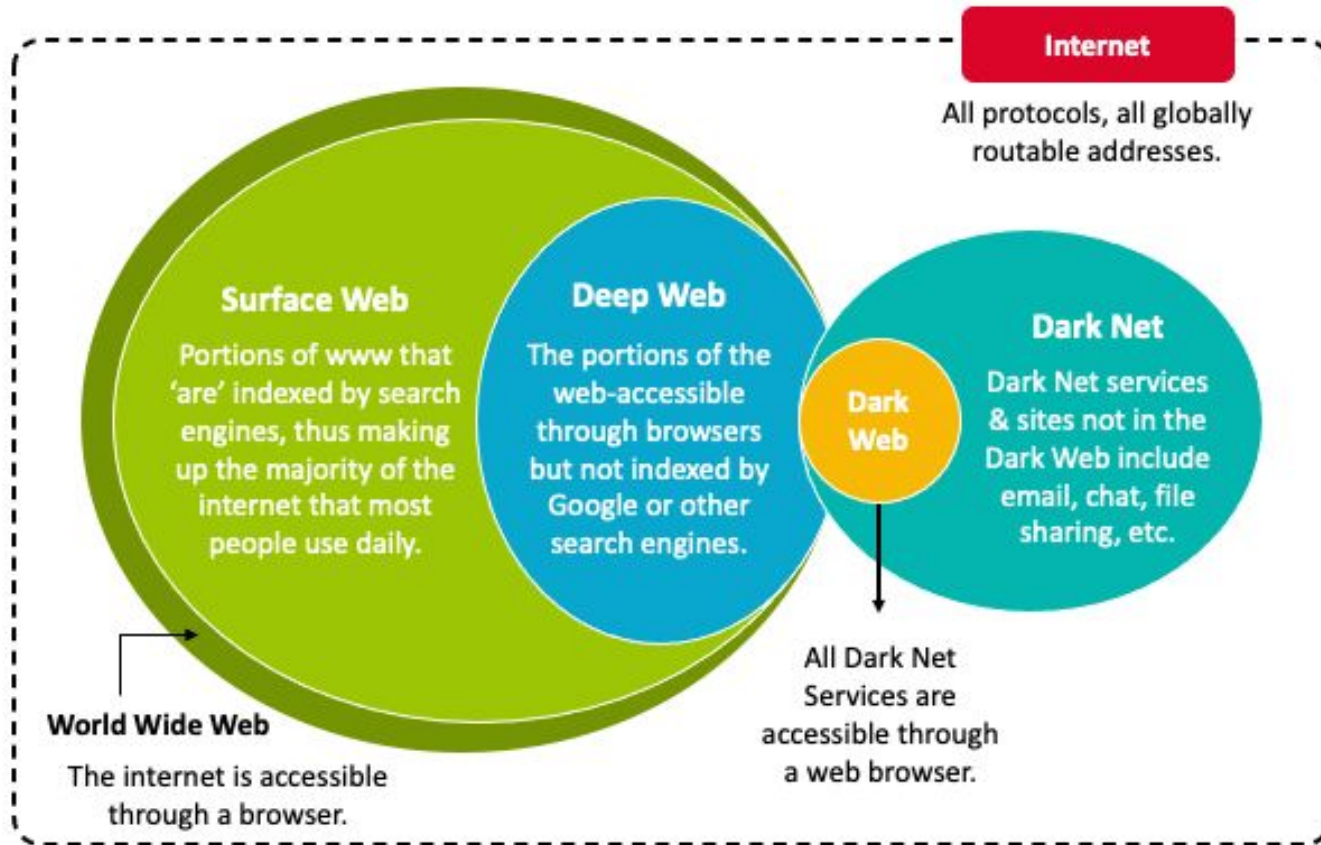


Understanding cybercriminal strategies

By Hieu M. Ngo (aka Hieupc) - NCSC Viet Nam

Co-founder chongluadao.vn



CYBER OF THINGS : EVERYTHING IS DIGITAL

C Factor and all are interrelated

**CYBER
CRIME**

**CYBER
SECURITY**

**CYBER
TERRORISM**



Cyber-Crime Tools Used

- The operators in the Deep Web and Dark Web use tools which ensure the anonymity of their identity, location, transactions, and payments
- **The Onion Routing (ToR)** network provides anonymous browsing and access to the Deep Web sites that are identified as *.**onion**.
- **Freenet, ZeroNet**: peer to peer (P2P) platform for censorship-resistant communication.
- **Invisible Internet Project** (I2P) is a fully encrypted private network layer.
- Use of **Bitcoins** helps keep transactions anonymous as this system does not identify the buyer / seller or payer/payee except as a hash value. In addition bitcoins can be converted to cash in currencies across the world and thus provide an unidentifiable means of stashing and transferring money.



- **Tor** is a special network of computers on the Internet, distributed around the world.
- <https://www.torproject.org>



- **Freenet** : <https://freenetproject.org>
- **ZeroNet** : <https://zeronet.io>
- **I2P** : <https://geti2p.net/en>



- **Bitcoins** are an anonymous, decentralized form of electronic currency
- like "cash" in cyberspace - anonymous.



Crooks are smarter – and now it's cheaper than ever!

They can buy malware, attack kits, and even '**Crimeware-as-a-Service**'!

It's as cheap as...



Drive-by Download tool kit rental
\$100/WEEK



Credit card details
\$ 0.50/CARDS



DDoS attacks
\$10/DAY



Stolen gaming accounts
\$10 EACH

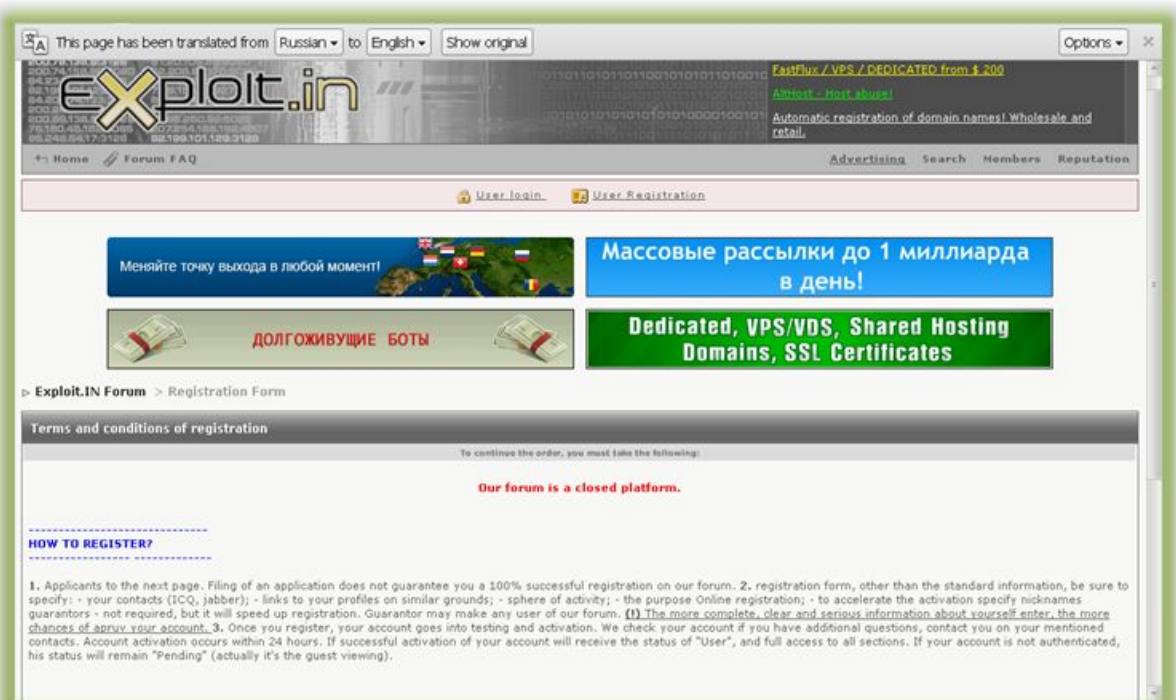


Verified Spam Email Blasts
\$70/MILLION

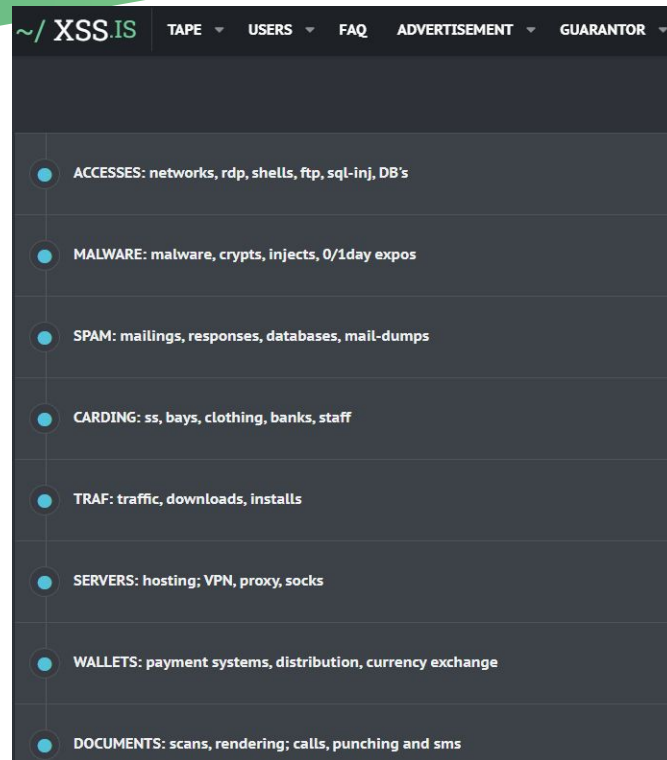
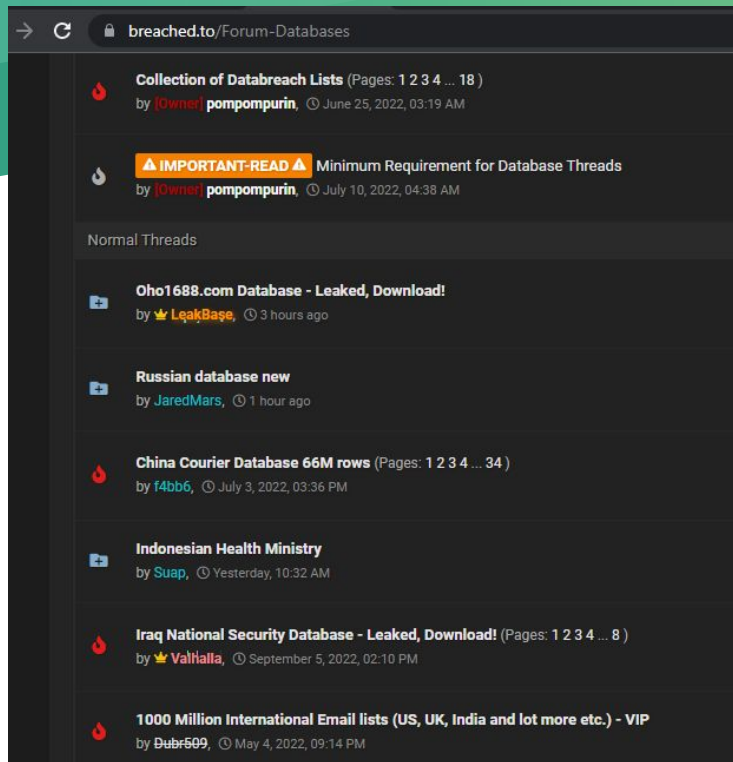
Cyber-crime popular tools



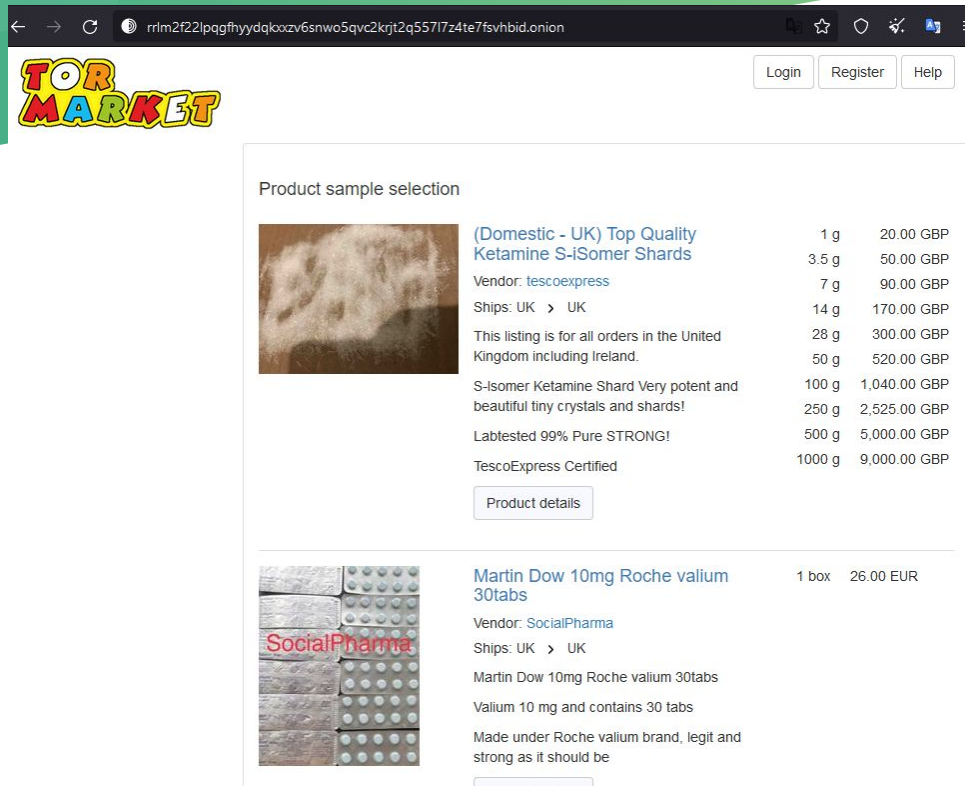
Cyber-crime popular tools



Cyber-crime popular tools




Cyber-crime popular tools



The screenshot shows a web browser window with the TOR MARKET website. The browser's address bar displays a long alphanumeric string. The website has a green header with the TOR MARKET logo and navigation links for Login, Register, and Help. The main content area is titled 'Product sample selection' and features two product listings. The first listing is for '(Domestic - UK) Top Quality Ketamine S-Isomer Shards' with a price list ranging from 20.00 GBP for 1g to 9,000.00 GBP for 1000g. The second listing is for 'Martin Dow 10mg Roche valium 30tabs' priced at 26.00 EUR per box. Both listings include vendor information, shipping details, and product descriptions.

Product sample selection



[\(Domestic - UK\) Top Quality Ketamine S-Isomer Shards](#)

Vendor: [tescoexpress](#)

Ships: UK > UK

This listing is for all orders in the United Kingdom including Ireland.


S-Isomer Ketamine Shard Very potent and beautiful tiny crystals and shards!

Labtested 99% Pure STRONG!

TescoExpress Certified

[Product details](#)

| | |
|--------|--------------|
| 1 g | 20.00 GBP |
| 3.5 g | 50.00 GBP |
| 7 g | 90.00 GBP |
| 14 g | 170.00 GBP |
| 28 g | 300.00 GBP |
| 50 g | 520.00 GBP |
| 100 g | 1,040.00 GBP |
| 250 g | 2,525.00 GBP |
| 500 g | 5,000.00 GBP |
| 1000 g | 9,000.00 GBP |



[Martin Dow 10mg Roche valium 30tabs](#)

Vendor: [SocialPharma](#)

Ships: UK > UK

Martin Dow 10mg Roche valium 30tabs

Valium 10 mg and contains 30 tabs

Made under Roche valium brand, legit and strong as it should be

[Product details](#)

1 box

26.00 EUR

Cyber-crime popular tools

The screenshot displays the 'genesis' marketplace interface, specifically the 'Bots' section. The left sidebar contains navigation links: Dashboard, Genesis Wiki, News, Bots (highlighted), Generate FP, Orders, Purchases, Payments, Tickets, Software, Profile, Invites, and Logout. The main content area shows a list of bots for sale, each with a unique ID, a list of associated resources, the operating system, and the price.

| BOT NAME/ID | RESOURCES KNOWN / OTHER | COUNTRY / HOST | PRICE |
|--|---|--|-------|
| C87E0F9CE840F636165FB8AB40E857E 2021-09-06 18:31:11 2021-09-07 17:57:07 | Google, Facebook, auth.riotgames.com, classroom.worldbookonline.com, lms.asknlearn.com, sign-up-api.riotgames.com, chesstempo.com, genyo.com.ph, lsm-campus-erp.com, slz02.scholasticid..., ...other 19 | US 69.250... Windows 10 Codename 19H2 Insider Preview Build 18363 | 11.00 |
| 0927F1CD2DA7321EA34E9051959C4E3D 2021-09-06 19:30:56 2021-09-07 17:57:07 | Windows 8.1 Pro | PL 89.64... | 5.00 |
| 547389A651AE78E45FC7AB9A75A0913E 2021-09-05 23:47:46 2021-09-07 17:57:07 | Google, Amazon, cracked.to, giphy.com, Twitter, Live, PayPal, f95zone.to, osu.ppy.sh, ...other 10 | BG 88.80... Windows 10 Pro | 20.00 |
| FB19EB0DCE741CDO89B8FA02CE3A5B7 2021-09-07 16:33:58 2021-09-07 17:57:07 | Twitter, LinkedIn, Cloudflare, smarthoster.uk, app.crisp.chat, Google, Pinterest, PayPal, Fiverr, Instagram, accounts.livechat.com, ...other 31 | HU 37.234... Windows 10 Pro | 17.00 |
| 2E7CE277B692725E4F97860A14E05C62 | Messenger, Zoom, Eprice, Libero, Ebay, Google | IT | 165 |

Cyber-crime Telegram the new darkweb



Cyber-crime popular tools

KelvinSecurity
1,407 members

Pinned message
Notification: Our fanpage on Facebook closes definitively after Facebook present...

@brokedegenerate Inbox 20:15

April 28

Sentinel
ZoneAlarmLPE

Exploit for LPE in ZoneAlarm Antivirus/Firewall.

Combination of weak permissions in C:
\\ProgramData\\CheckPoint\\ZoneAlarm\\Data and self-protection
bypass (self-protection driver failed to protect sensitive files from
modification when file is accessed over UNC path) leads to LPE
allowing any local user to elevate privileges to SYSTEM account.

<https://github.com/Wh04m1001/ZoneAlarmLPE>

GitHub
GitHub - Wh04m1001/ZoneAlarmLPE: Exploit for LPE in
ZoneAlarm Antivirus/Firewall
Exploit for LPE in ZoneAlarm Antivirus/Firewall. Contribute to
Wh04m1001/ZoneAlarmLPE development by creating an accou...

Wh04m1001/
ZoneAlarmLPE

Exploit for LPE in ZoneAlarm Antivirus/Firewall

Al 1 Contributor 0 Issues 23 Stars 5 Forks

0:39

INTERNET INFECTION
843 subscribers

522 deathNote, 10:37 AM

INTERNET INFECTION
share & support us

320 deathNote, 10:37 AM

INTERNET INFECTION
All Adobe Products 2020 cracked

These may have viruses as i didn't check, scan on virustotal or use in VM

Adobe Photoshop 2020
<http://www.mediafire.com/file/q95zb5lrlutcgj/Adobe.Photoshop.2020.v21.0.2.57.exe/file>

Adobe Illustrator 2020
<https://www.mediafire.com/file/dyhtj37arw2rfvw/Adobe.Illustrator.2020.v24.0.1.341.exe/file>

Adobe InDesign 2020
http://www.mediafire.com/file/l6akoiad9othwm3/Adobe_InDesign_2020.exe/file

Adobe Bridge 2020
http://www.mediafire.com/file/2t7fjiw7jj0slpo/Adobe_Bridge_CC_2020.exe/file

2:51

56 Chats SMSRanger bot

/start 2:50 AM ✓

Please Provide your phone number e.g
+12345 2:50 AM

smsrangerbot @smsrangerbot /help 2:50 AM ✓

/help - show commands available
/pp - enable PayPal mode
/acc - enable Account mode
/pay - enable Apple/Google Pay mode
/email - enable Email mode
/bank - enable Bank mode
/carrier - enable Carrier mode 2:50 AM

/bank 2:51 AM ✓

Please Provide your phone number e.g
+12345 2:51 AM

smsrangerbot +14165774117 2:51 AM ✓

Ok. your request will expire in 1 minute. (company of the service e.g: TD Bank)

request will expire in 1 minute. 2:51 AM

smsrangerbot td canada trust 2:51 AM ✓

Calling +14165774117 from +18559275269 as: td canada trust 2:51 AM @smsrangerbot

On Call (+14165774117) 2:51 AM

Cyber-crime popular tools

EternityTeam



!—SOFT—!

Ransomware - 490\$

Miner - 110\$

Stealer - 300\$

Clipper - 90\$

Worm - 390\$

Naked Pages Announcement

READ THIS AND UNDERSTAND PLEASE!!

YOU BUY LICENSE 200\$

AND YOU CAN USE OUR APP WHICH COMES WITH THE FOLLOWING PAGES

Chase + email access cookies(No gmail)
BOA True login + email access cookies(No gmail)
Citi + email access cookies(No gmail)
Citizen + email access cookies(No gmail)
Huntington + email access cookies(No gmail)

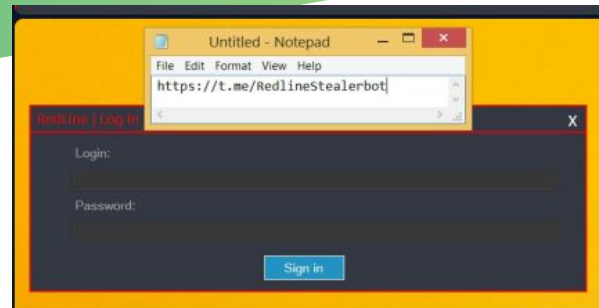
Office(With 2fa bypass and cookies)
proton(+2fa bypass and cookies)
Slack(+2fa bypass and cookies)
53rd
Outlook(+2fa bypass and cookies)
Yahoo + 2fa bypass + cookies
Aol + 2fa bypass + Cookies

TO GET GMAIL COOKIES SUPPORT YOU PAY EXXTRA 1K\$

YOU GET ACCESS TO THE FOLLOWING PAGES ALSO

google (+ 2fa support, phone prompt support, gsuite & edu support)
ALL BANK PAGES WITH GMAIL COOKIES SUPPORT

With all our app features/antibot



Redline for Lifetime

Code: LIFE003000003

Displaying a list of logs with fields: ID, HWID, IP, OS, BuildID, Country, LogDate, Comment
Save all logs to the specified folder.
Check the necessary cookies in the logs.

Files from the file grabber
Statistics on the total number
Logins and passwords, Autofill data, Credit cards, Files from file grabbers
Create/Edit tasks
Clear log list

AND MUCH MUCH MORE.

Telegram only Allows 500 words that's why can't explain more here.

\$ 900 USD

Downloadable product (file)

5:21 PM

Add to cart

Cyber-crime popular tools

Brady
Forwarded from JokerLogs | Reborn

 @joker_reborn - 400 FILES \$ I LIKE YOU POPS.rar
311.5 MB

 Over Monthly 150k-250k New Logs 2022

 BANK,FB,GPAY,CRYPTO,GAMING


- MEGA CLOUD + FREE ACCOUNTS PRO
- Weekly 20k-40k PCS logs
- Geo USA, EU, MIX, Targeted
- Working cookies
- Crypto Wallets
- Free soft for checked your site/link
- Free soft search crypto wallets
- Free soft checked logs google/fb/youtube/twitter


 Current private logs cloud cost:

-  1 month - \$600
-  2 months - \$1000
-  Lifetime - \$5000


THOR ⚡ | FREE LOGS CLOUD
772 subscribers


Unread messages

THOR ⚡ | FREE LOGS CLOUD
 THOR FREE LOGS.zip
258.5 MB
👍 3 👎 0 👁 677 10:27 PM

THOR ⚡ | FREE LOGS CLOUD
 THOR FREE LOGS.rar
472.3 MB
👍 5 👎 0 👁 719 11:35 PM

September 7









THOR ⚡ | FREE LOGS CLOUD
 THOR FREE LOGS.rar
56.7 MB
👍 2 👎 2 👁 671 10:30 PM

THOR ⚡ | FREE LOGS CLOUD
 THOR FREE LOGS.rar
109.7 MB
👍 2 👎 2 👁 709 10:43 PM

September 9

LOGID-3769170.zip

File Commands Tools Favorites Options Help

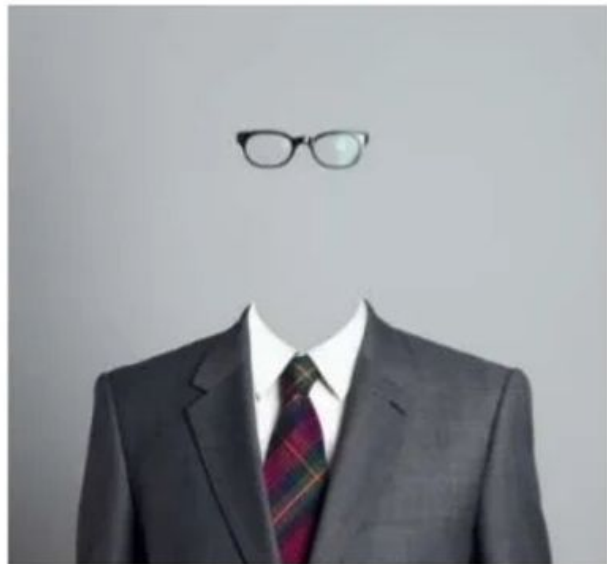
 Add  Extract To  Test  View  Delete  Find  Wizard  Info

↑ LOGID-3769170.zip - ZIP archive, unpacked size 1,049,946 bytes

Name

- ..
- Autofills
- Cookies
- DomainDetects.txt
- ImportantAutofills.txt
- InstalledBrowsers.txt
- InstalledSoftware.txt
- Passwords.txt
- Screenshot.jpg
- UserInformation.txt

Dark Web characteristics



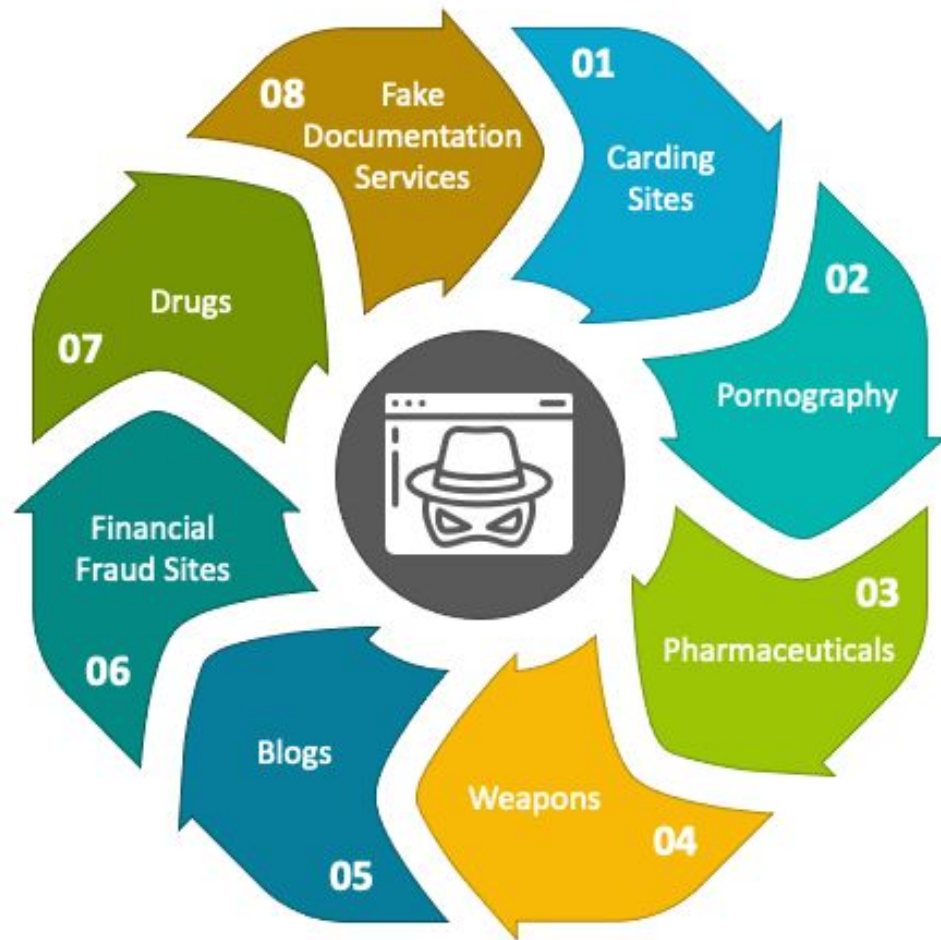
Anonymous



Special access software



Associated with illegal activities

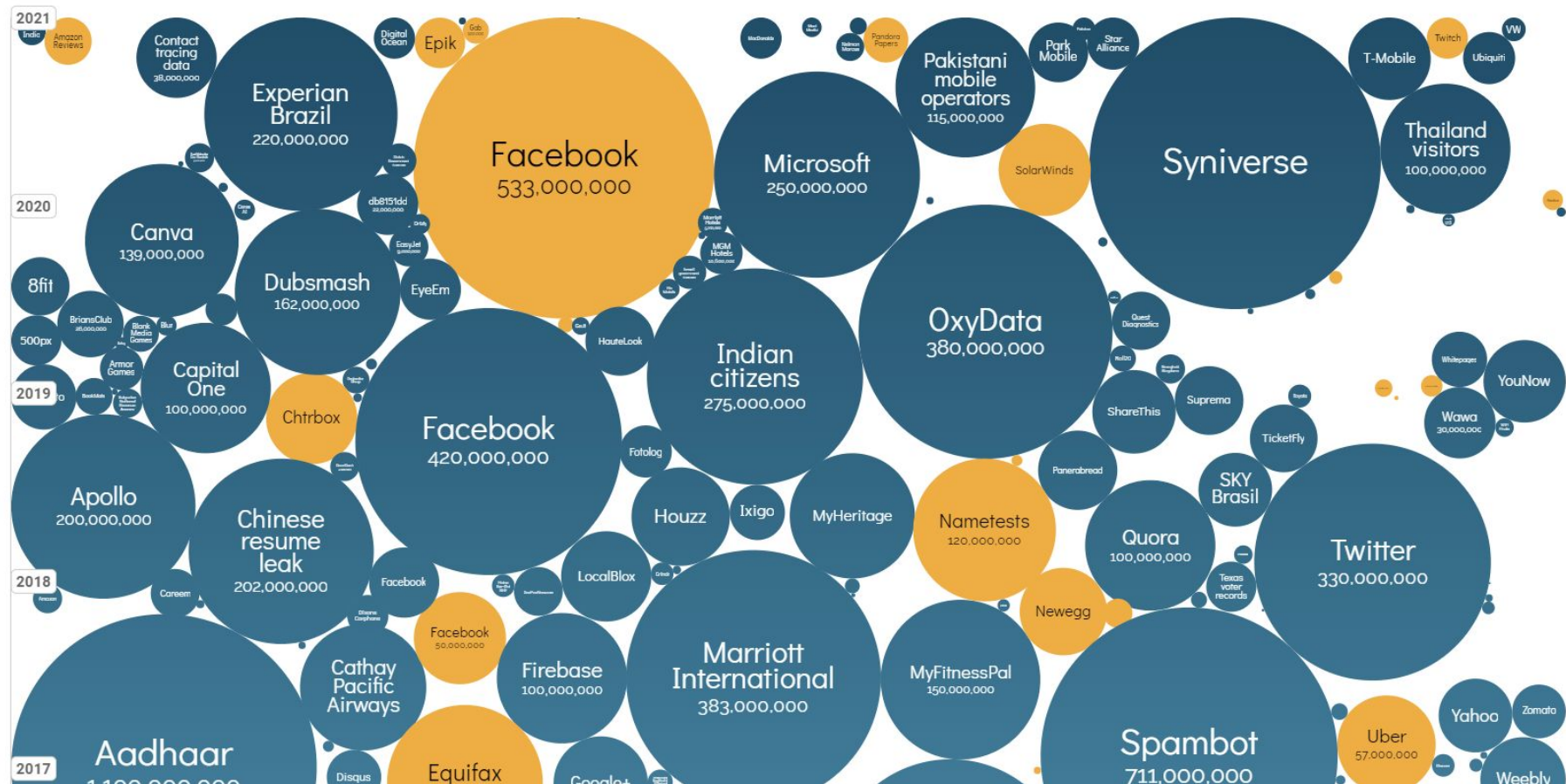


interesting
story

UPDATED: Oct 2021

filter

search...



CRITICAL INFORMATION INFRASTRUCTURES (CII)

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. Most commonly associated with the term are facilities for:



EDUCATION



WATER



DEFENCE



TELECOMMUNICATION



FINANCIAL



GOVERNMENT



HOSPITAL



INDUSTRY



ENERGY



TRANSPORTATION

6 Tips on How to Avoid Ransomware Attacks

Cybercriminals want your important files. Here's how to prevent them from being taken hostage.

1 Avoid Suspicious Links

If you don't know who's sending a link - or if you doubt the person is actually who they claim to be - don't click that link. It's likely infected.

2 Pause Before Sending Personal Information

Often, a cyberattack is obvious in hindsight. Before filling out personal information, ask yourself whether the form you're using is legitimate.

3 Install Firewalls and Antivirus Software

These basic technologies are an effective line of defense against cyberattacks.

4 Quickly Patch Vulnerabilities

It's easy to ignore software update messages, but the consequences of not patching can be brutal.

5 Educate Your Employees

All the defenses in the world are meaningless if your employees don't know how to spot a threat. Teach them how to identify and avoid common cyberattacks, including ransomware.

6 Test Your Employees

Education without testing is like... well, education without testing. Check whether the information's sticking with annual phishing tests.





LEAKED DATA

[CONDITIONS FOR PARTNERS AND CONTACTS >](#)

12D 19H 2M 48 S

...
...
...
...
...

MORE →



3D 14H 57M 48 S

...
...
...
...
...

MORE →



3D 14H 35M 48 S

...
...
...
...
...

MORE →



3D 14H 29M 48 S

...
...
...
...
...



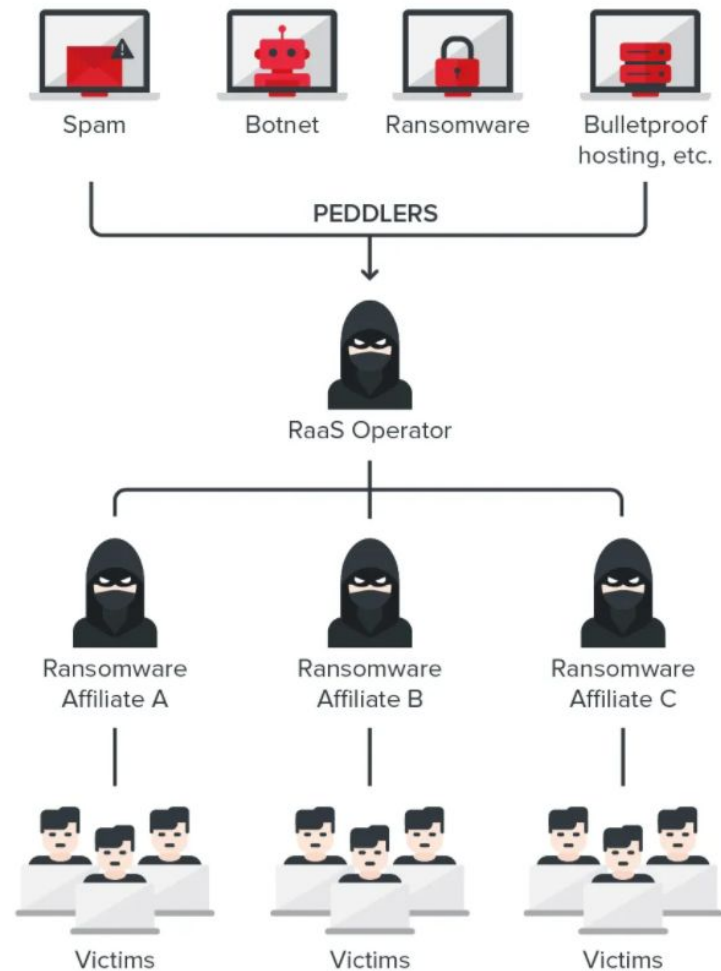
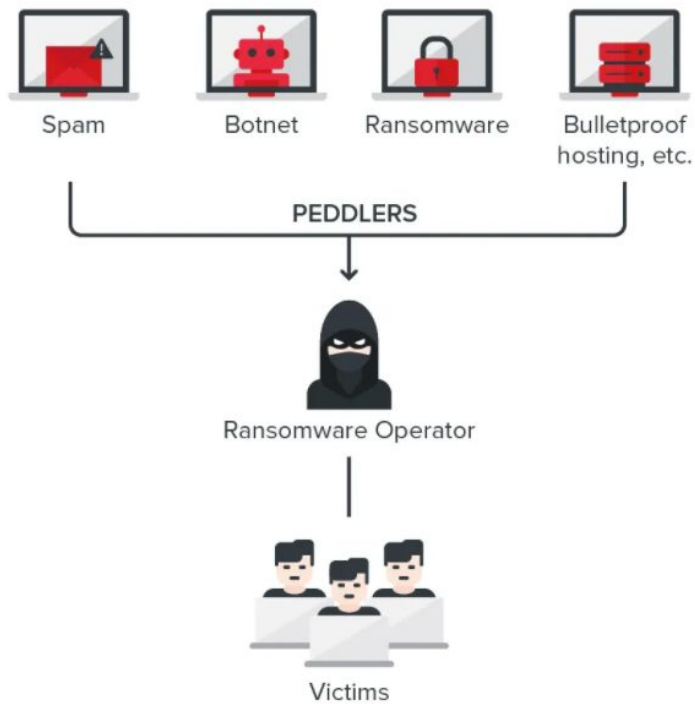
3D 1H 15M 48 S

...
...
...
...
...



PUBLISHED FILES

...
...
...
...
...



Key Takeaways

- Dark web is more about the technology than the content
- Much of the content is legal and legitimate
- Tor is by far the most popular access technology
- It is very difficult to make a site 100% anonymous
- The dark web can present a risk to legitimate users and companies
- Simple security measures can deter all but the most determined attackers

Thank you

<https://ncsc.gov.vn>

<https://chongluadao.vn>