Pinaca

Cyber Offences

Issues & Challenges in Investigation

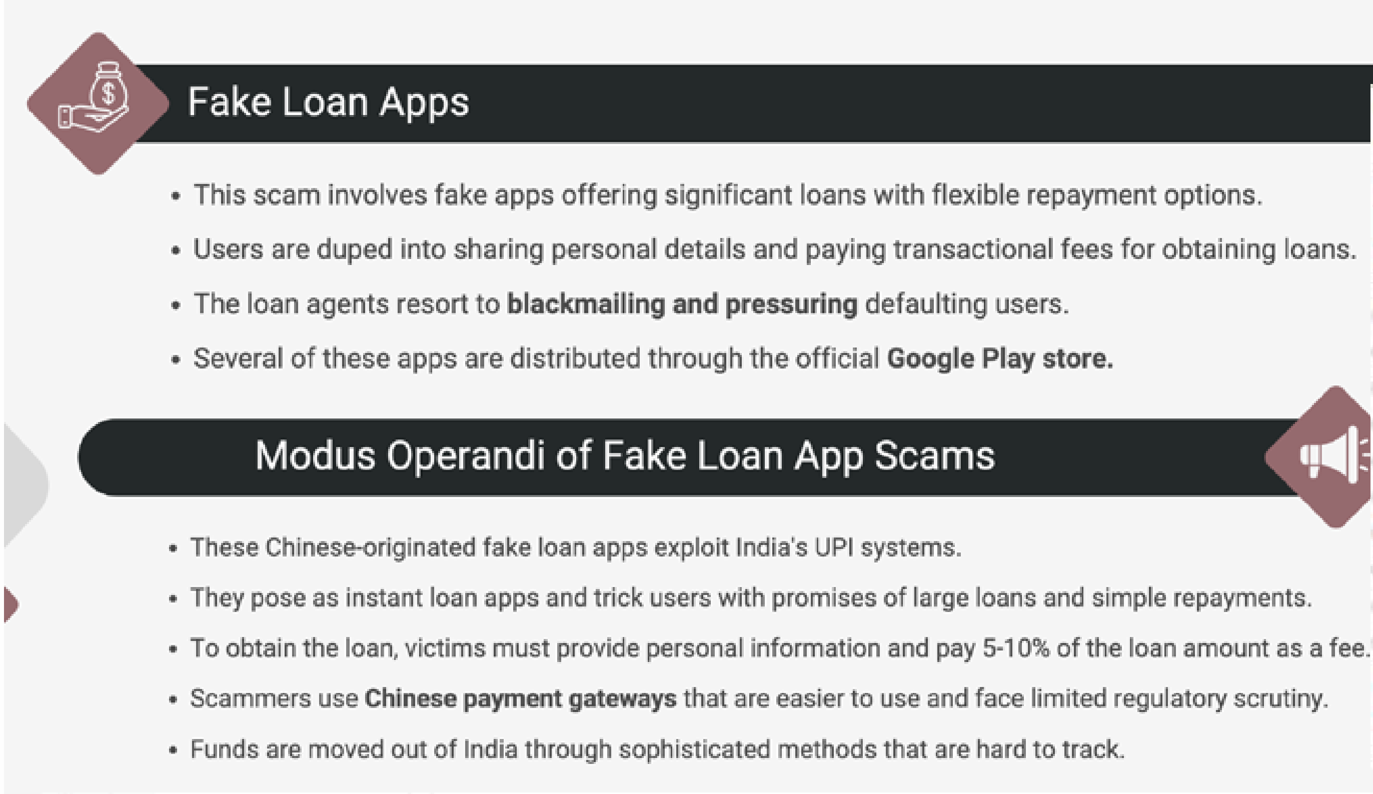
BVS Saikrishna

CEO – Pinaca Group.

Financial Ecosystem of Cybercrime.

- Hackers, State Backed & Organised Crime Cartel
- Financial Specialists (Money Mules, Launderers)
- Dark Web Marketplaces
- Intermediary Networks (Exchanges, Washers & Fraud Rings)

Fake Loan Apps.



Fake Loan Apps

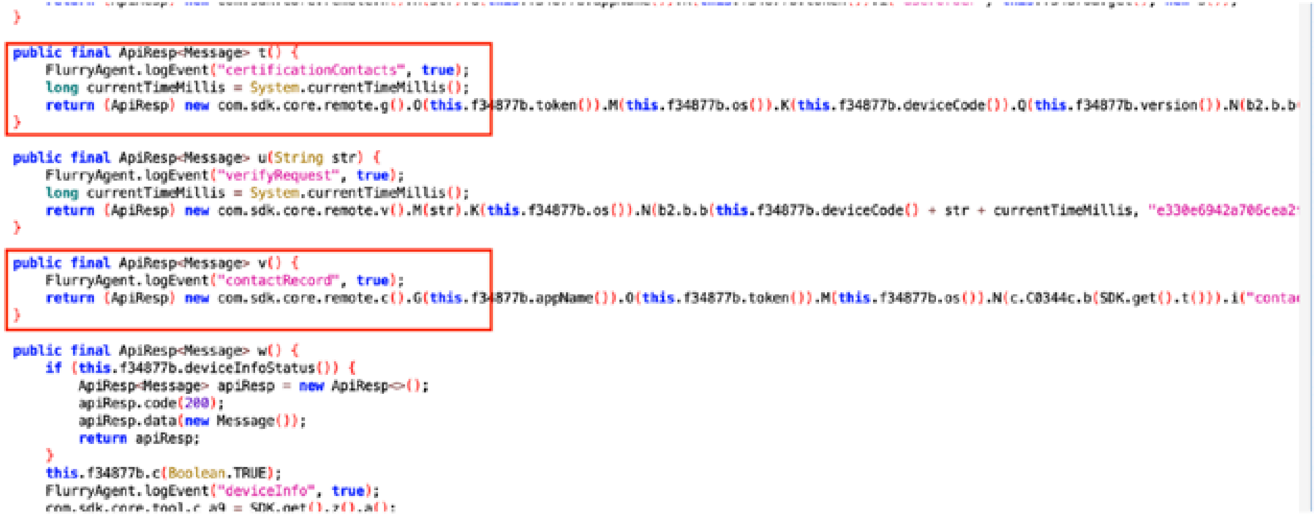
- This scam involves fake apps offering significant loans with flexible repayment options.
- Users are duped into sharing personal details and paying transactional fees for obtaining loans.
- The loan agents resort to **blackmailing and pressuring** defaulting users.
- Several of these apps are distributed through the official **Google Play store.**

Modus Operandi of Fake Loan App Scams

- These Chinese-originated fake loan apps exploit India's UPI systems.
- They pose as instant loan apps and trick users with promises of large loans and simple repayments.
- To obtain the loan, victims must provide personal information and pay 5-10% of the loan amount as a fee.
- Scammers use **Chinese payment gateways** that are easier to use and face limited regulatory scrutiny.
- Funds are moved out of India through sophisticated methods that are hard to track.

Fake Loan Apps.

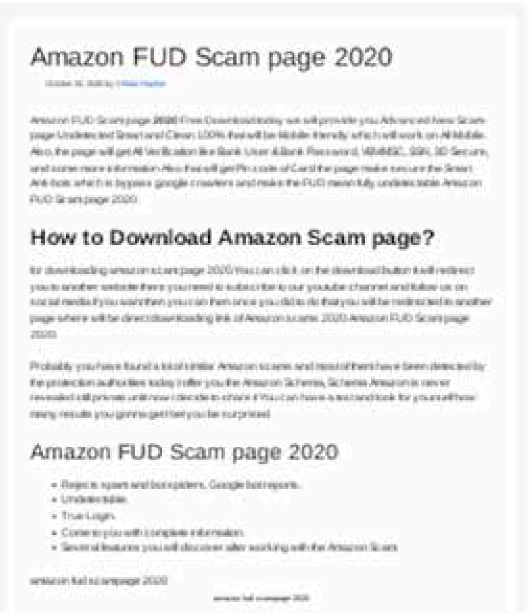
- The apps misuse KYC details such as **Aadhaar and PAN** to open fake bank and crypto exchange accounts.
- They gain full access to the device's **contacts, gallery, SMS, and location**.
- This data is then used for money laundering and phishing scams and sold on the Dark web.
- The data is used to fabricate information, manipulate images, or message close contacts during the blackmail process to embarrass and pressure users into submitting to predatory terms.



```
}

public final ApiResp<Message> t() {
    FlurryAgent.logEvent("certificationContacts", true);
    long currentTimeMillis = System.currentTimeMillis();
    return (ApiResp) new com.sdk.core.remote.g().O(this.f34877b.token()).M(this.f34877b.os()).K(this.f34877b.deviceCode()).Q(this.f34877b.version()).N(b2.b.b
}

public final ApiResp<Message> u(String str) {
    FlurryAgent.logEvent("verifyRequest", true);
    long currentTimeMillis = System.currentTimeMillis();
    return (ApiResp) new com.sdk.core.remote.v().M(str).K(this.f34877b.os()).N(b2.b.b(this.f34877b.deviceCode() + str + currentTimeMillis, "e330e6942a706cea2
}

public final ApiResp<Message> v() {
    FlurryAgent.logEvent("contactRecord", true);
    return (ApiResp) new com.sdk.core.remote.c().G(this.f34877b.appName()).O(this.f34877b.token()).M(this.f34877b.os()).N(c.C0344c.b(SDK.get().t())).i("conta
}

public final ApiResp<Message> w() {
    if (this.f34877b.deviceInfoStatus()) {
        ApiResp<Message> apiResp = new ApiResp<>();
        apiResp.code(200);
        apiResp.data(new Message());
        return apiResp;
    }
    this.f34877b.c(Boolean.TRUE);
    FlurryAgent.logEvent("deviceInfo", true);
    com.sdk.core.tool.c a9 = SDK.get().z().a();
```

Multiple Cyber Scams.

- Several illegal marketplaces and **carding sites on the Dark Web** were also uncovered during our investigation.
- These sites distribute scam pages and clones to popular e-commerce sites in exchange for cryptocurrency.
- Some hackers even provide tutorial videos and live classes to scammers on how to setup and deploy these sites.



Amazon FUD Scam page 2020

October 31, 2020 by [illegible]

Amazon FUD Scam page **2020** Free Download today we will provide you Advanced New Scam page Undetected Smart and Clean. 100% that will be Mobile friendly which will work on All Mobile. Also, the page will get All Verification like Bank User & Bank Password, VBV/MSC, SSN, 3D Secure, and some more information Also that will get Pin code of Card the page make secure the Smart Anti-bots which is bypass google crawlers and make the FUD mean fully undetectable Amazon FUD Scam page 2020.

How to Download Amazon Scam page?

for downloading amazon scam page 2020 You can click on the download button it will redirect you to another website there you need to subscribe to our youtube channel and follow us on social media if you want then you can them once you did to do that you will be redirected to another page where will be direct downloading link of Amazon scame 2020 Amazon FUD Scam page 2020.

Probably you have found a lot of similar Amazon scams and most of them have been detected by the protection authorities today I offer you the Amazon Scheme, Scheme Amazon is never revealed till private until now I decide to share it You can have a test and look for yourself how many results you gonna get bet you be surprised

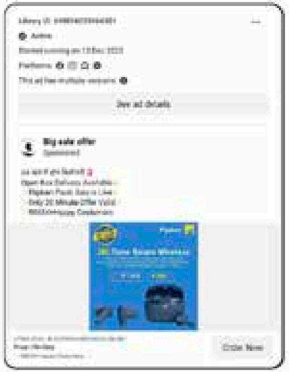
Amazon FUD Scam page 2020

- Rejects spam and bot spiders, Google bot reports.
- Undetectable.
- True Login.
- Come to you with complete information.
- Several features you will discover after working with the Amazon Scam

amazon full scampage 2020

amazon full scampage 2020

Fake Advertisements : Digital Platforms



Library ID: [illegible]

Active

Started running on 13 Dec 2023

Platforms

This ad has multiple versions

See ad details

Big sale offer

Sponsored

24 घंटे में [illegible] डिलीवरी

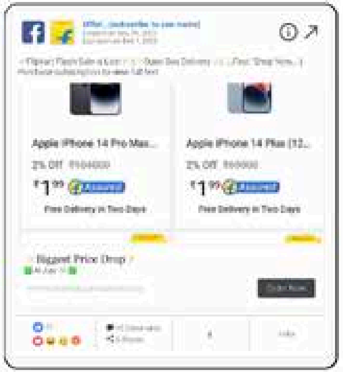
Open Box Delivery Available

Flipkart Flash Sale is Live

Only 20 Minute Offer Valid

[illegible]+Happy Costumers

Order Now



Offer...(subscribe to see name)

Flipkart Flash Sale is Live! ... Open Box Delivery ... Fast Shop Now... | Purchase subscription to view full text

Apple iPhone 14 Pro Max...

2% Off ₹[illegible]

₹1 99 Assured

Free Delivery in Two Days

Apple iPhone 14 Plus (12...

2% Off ₹[illegible]

₹1 99 Assured

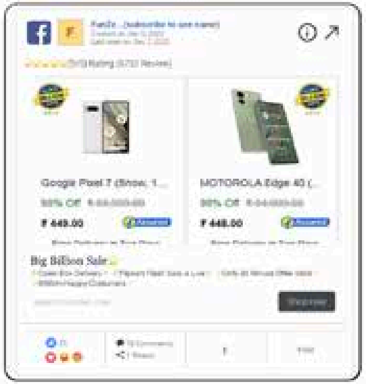
Free Delivery in Two Days

Biggest Price Drop

At Just ₹1

Order Now

Like



FanZe...(subscribe to see name)

[illegible] Rating ([illegible] Review)

Google Pixel 7 (Snow, 1...

99% Off ₹[illegible]

₹ 449.00 Assured

MOTOROLA Edge 40 (...

99% Off ₹[illegible]

₹ 448.00 Assured

Big Billion Sale

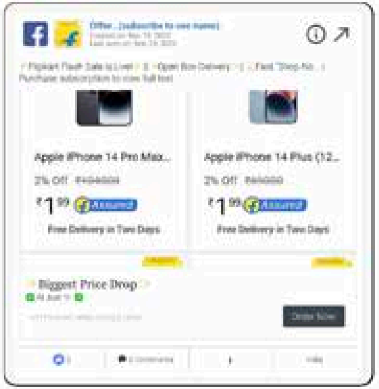
Open Box Delivery ... Flipkart Flash Sale is Live ... Only 20 Minute Offer Valid ... [illegible]+Happy Costumers

Shop now

Comments

Share

Like



Offer...(subscribe to see name)

Flipkart Flash Sale is Live! ... Open Box Delivery ... Fast Shop No... | Purchase subscription to view full text

Apple iPhone 14 Pro Max...

2% Off ₹[illegible]

₹1 99 Assured

Free Delivery in Two Days

Apple iPhone 14 Plus (12...

2% Off ₹[illegible]

₹1 99 Assured

Free Delivery in Two Days

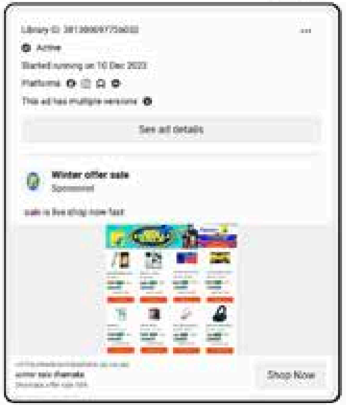
Biggest Price Drop

At Just ₹1

Order Now

Comments

Like



Library ID: 381[illegible]

Active

Started running on 10 Dec 2023

Platforms

This ad has multiple versions

See ad details

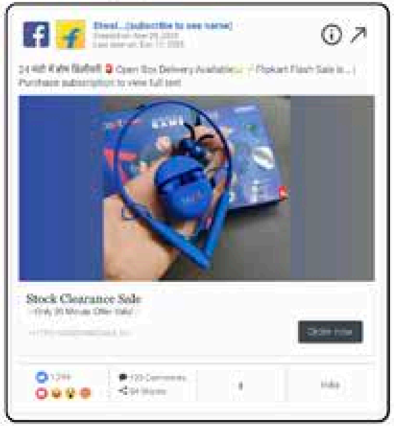
Winter offer sale

Sponsored

sale is live shop now fast

winter sale [illegible]

Shop Now



Deal...(subscribe to see name)

24 घंटे में फ्री डिलीवरी Open Box Delivery Available ... Flipkart Flash Sale is... | Purchase subscription to view full text

Stock Clearance Sale

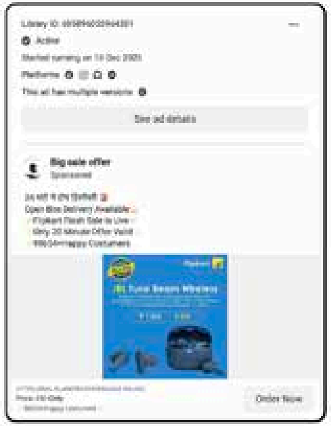
Only 20 Minute Offer Valid

Order now

Comments

Shares

Like



Library ID: [illegible]

Active

Started running on 13 Dec 2023

Platforms

This ad has multiple versions

See ad details

Big sale offer

Sponsored

24 घंटे में [illegible] डिलीवरी

Open Box Delivery Available

Flipkart Flash Sale is Live

Only 20 Minute Offer Valid

[illegible]+Happy Costumers

Price: ₹[illegible] Only

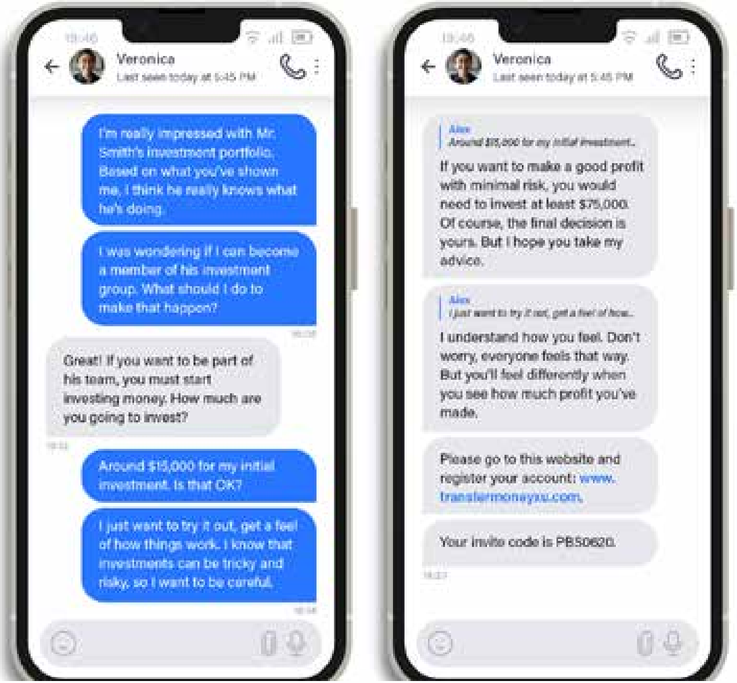
Order Now

Cybercrime Income Sources.

- **Ransomware Payments** : Cryptocurrency ransoms.
- **Data Theft & Sale** : Selling personal/financial data on dark web.
- **Fraud & Phishing**: Stolen credit cards, fake invoices.
- **Botnets & DDoS-for-Hire**: Offering cyberattacks as a service.
- **Cryptojacking**: Illegally mining cryptocurrency.
- **Malware-as-a-Service**: Selling hacking tools.

Cybercrime : Laundering.

- Cryptocurrency Tumbling & Mixing Services
- Cash-Out via Gift Cards & Prepaid Cards
- Money Mules & Social Engineering
- Exploiting Online Gambling & Casinos
- Shell Companies & Fake Businesses
- Peer-to-Peer Crypto Transfers



Veronica
Last seen today at 5:45 PM

I'm really impressed with Mr. Smith's investment portfolio. Based on what you've shown me, I think he really knows what he's doing.

I was wondering if I can become a member of his investment group. What should I do to make that happen?

Great! If you want to be part of his team, you must start investing money. How much are you going to invest?

Around $15,000 for my initial investment. Is that OK?

I just want to try it out, get a feel of how things work. I know that investments can be tricky and risky, so I want to be careful.

Veronica
Last seen today at 5:45 PM

> Alex
> *Around $15,000 for my initial investment...*

If you want to make a good profit with minimal risk, you would need to invest at least $75,000. Of course, the final decision is yours. But I hope you take my advice.

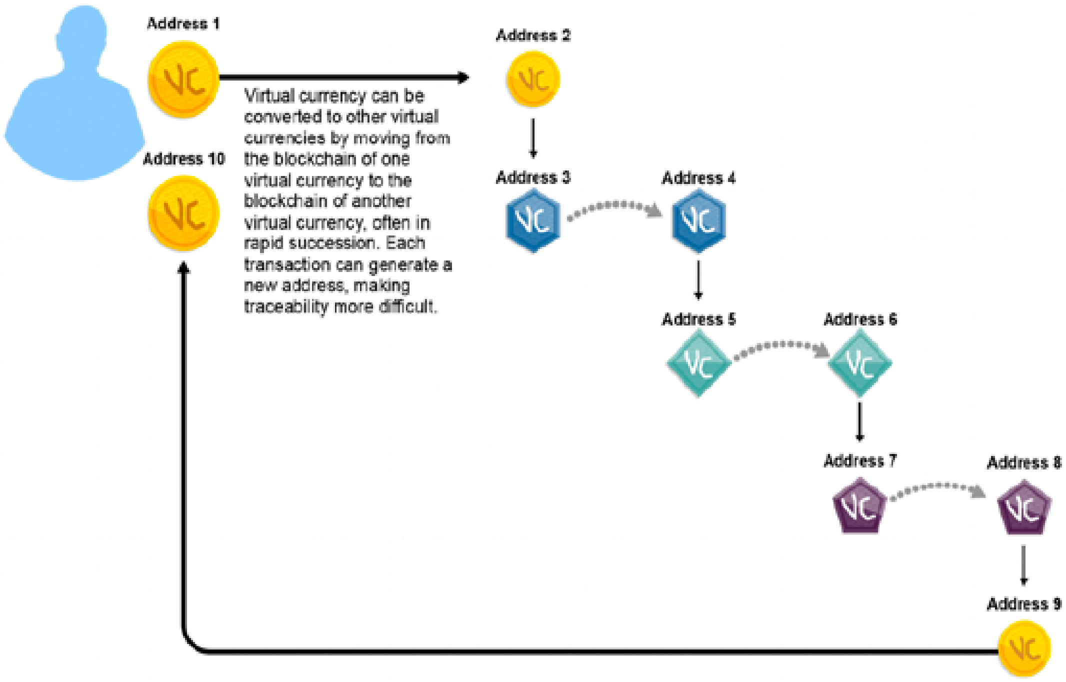
> Alex
> *I just want to try it out, get a feel of how...*

I understand how you feel. Don't worry, everyone feels that way. But you'll feel differently when you see how much profit you've made.

Please go to this website and register your account: www.transfermoneyxu.com.

Your invite code is PB50620.

Blockchain Hopping to avoid detection.



Virtual currency can be converted to other virtual currencies by moving from the blockchain of one virtual currency to the blockchain of another virtual currency, often in rapid succession. Each transaction can generate a new address, making traceability more difficult.

- Mixing Services.
- Privacy Coins.
- Private Chain Theft.
- Weak KYC Regimes.

Axie Infinity Ronin Bridge Hack.
173mn USD.
ETH->BNB Chain->WTH->USDD-> BTTC

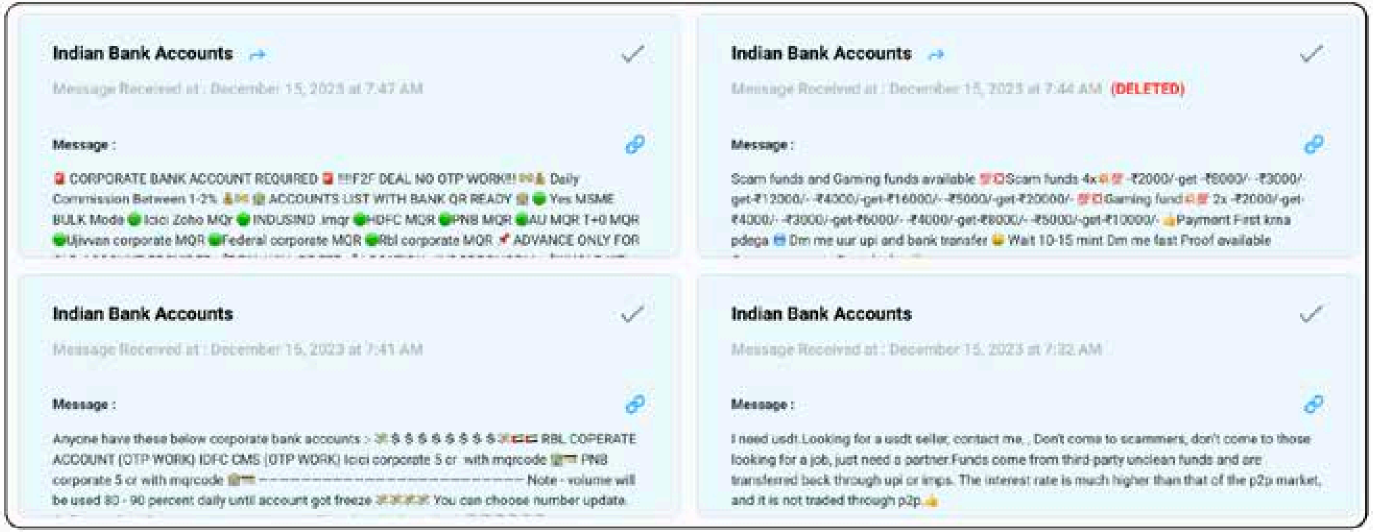
6/9 Private Keys stolen.
Coins Rotated through Tornado Cash.

Using ML for evaluation of Scam Content.

- **Illegal Betting & Investment Scams:**
- We identify URLs & phone numbers linked to fraudulent websites involved in illegal betting and fake investment schemes, providing IB with the data needed to investigate and take down these scams.
- **Fraudulent Google Ads:**
- We track fake customer care numbers and scams, such as work-from-home job offers and recruitment frauds, that impersonate legitimate companies, often tricking victims into revealing personal information or making payments.
- **Telegram and WhatsApp Monitoring:**
- We continuously gather data about Telegram channels, WhatsApp groups, and profiles that are involved in scams and fraud activities to help in identifying key actors in fraudulent networks.
- **UPI & Bitcoin Wallet Intelligences**
- We provide intelligence on UPI IDs and BTC wallets involved in financial fraud or scam activities, assisting in tracking funds and shutting down fraud mechanisms.

Money Mules in India.

- Scammers launder money using mules with accounts in smaller banks with limited investigative resources.
- Mules receive a 1-2% transaction fee for their services in the laundering scheme.
- Over **20 Telegram channels** have been identified for recruiting mules, some sending hundreds of messages daily.
- Scammers promise high commissions and require accounts in banks like **PNB, Yes Bank, and IndusInd Bank**.
- Mules must have a verified KYC details, sometimes **requiring corporate accounts** or high-limit bank accounts.



Indian Bank Accounts

Message Received at : December 15, 2023 at 7:47 AM

Message :

CORPORATE BANK ACCOUNT REQUIRED !!!F2F DEAL NO OTP WORK!! Daily Commission Between 1-2% ACCOUNTS LIST WITH BANK QR READY 🟢 Yes MSME BULK Mode 🟢 Icici Zoho MQr 🟢 INDUSIND .imqr 🟢HDFC MQR 🟢PNB MQR 🟢AU MQR T+0 MQR 🟢Ujjivan corporate MQR 🟢Federal corporate MQR 🟢Rbl corporate MQR 📌 ADVANCE ONLY FOR

Indian Bank Accounts

Message Received at : December 15, 2023 at 7:44 AM (DELETED)

Message :

Scam funds and Gaming funds available Scam funds 4x -₹2000/-get -₹8000/- -₹3000/-get-₹12000/- -₹4000/-get-₹16000/- -₹5000/-get-₹20000/- Gaming fund 2x -₹2000/-get-₹4000/- -₹3000/-get-₹6000/- -₹4000/-get-₹8000/- -₹5000/-get-₹10000/- 👍Payment First krna pdega Dm me uur upi and bank transfer Wait 10-15 mint Dm me fast Proof available

Indian Bank Accounts

Message Received at : December 15, 2023 at 7:41 AM

Message :

Anyone have these below corporate bank accounts :- $ $ $ $ $ $ $ $ RBL COPERATE ACCOUNT (OTP WORK) IDFC CMS (OTP WORK) Icici corporate 5 cr with mqrcode PNB corporate 5 cr with mqrcode ------------------------------ Note - volume will be used 80 - 90 percent daily until account got freeze You can choose number update

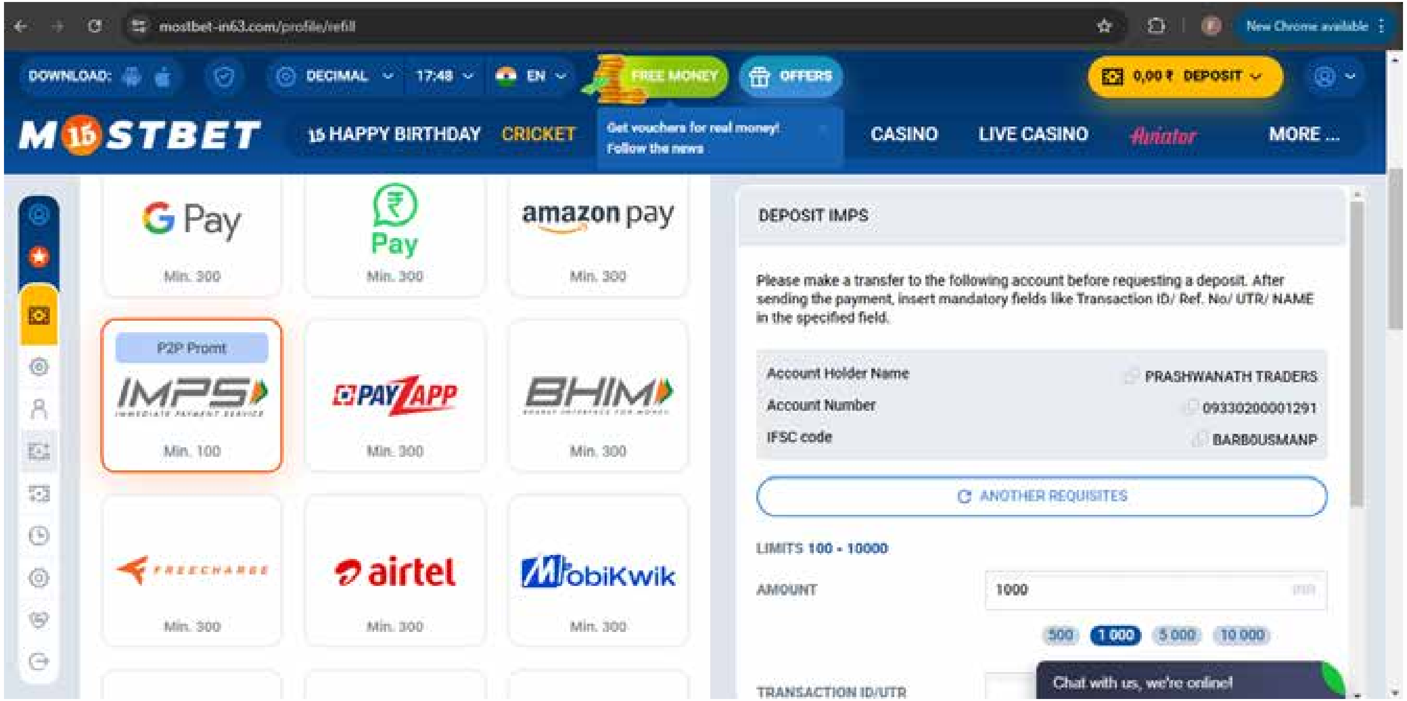
Indian Bank Accounts

Message Received at : December 15, 2023 at 7:32 AM

Message :

I need usdt.Looking for a usdt seller, contact me, , Don't come to scammers, don't come to those looking for a job, just need a partner.Funds come from third-party unclean funds and are transferred back through upi or imps. The interest rate is much higher than that of the p2p market, and it is not traded through p2p.👍

Tracking IFNs



DEPOSIT IMPS

Please make a transfer to the following account before requesting a deposit. After sending the payment, insert mandatory fields like Transaction ID/ Ref. No/ UTR/ NAME in the specified field.

Account Holder Name	PRASHWANATH TRADERS
Account Number	09330200001291
IFSC code	BARB0USMANP

ANOTHER REQUISITES

LIMITS 100 - 10000

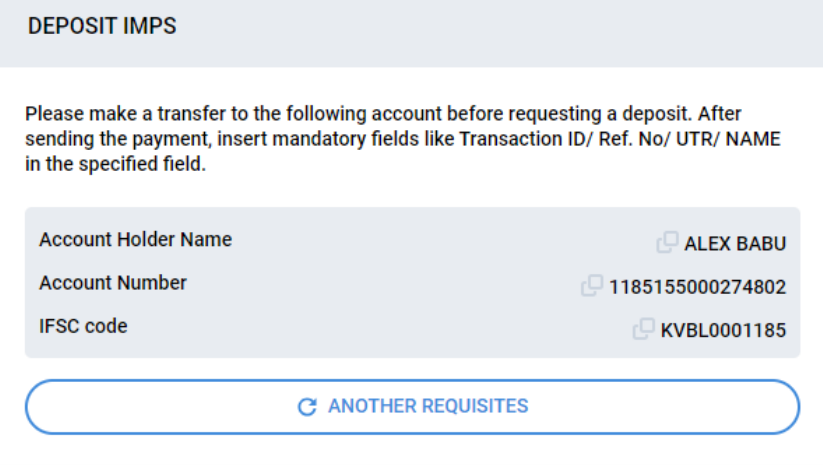
AMOUNT 1000 INR

500 1 000 5 000 10 000

TRANSACTION ID/UTR

Chat with us, we're online!

Money Mule Accounts.

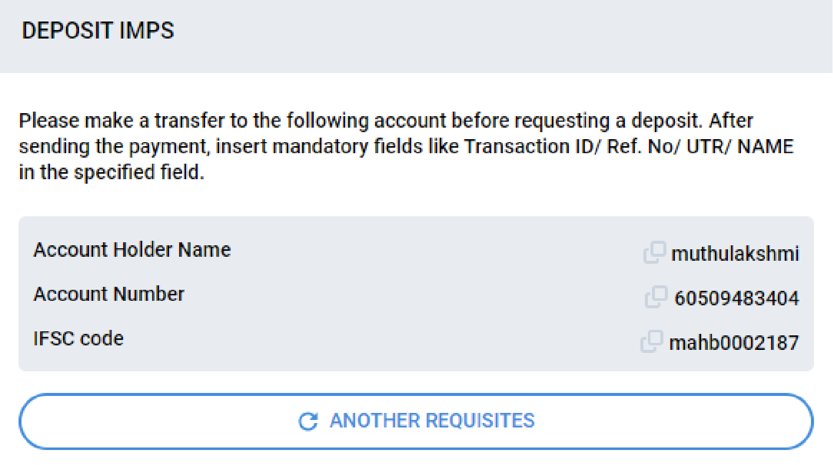


DEPOSIT IMPS

Please make a transfer to the following account before requesting a deposit. After sending the payment, insert mandatory fields like Transaction ID/ Ref. No/ UTR/ NAME in the specified field.

Account Holder Name	ALEX BABU
Account Number	1185155000274802
IFSC code	KVBL0001185

ANOTHER REQUISITES



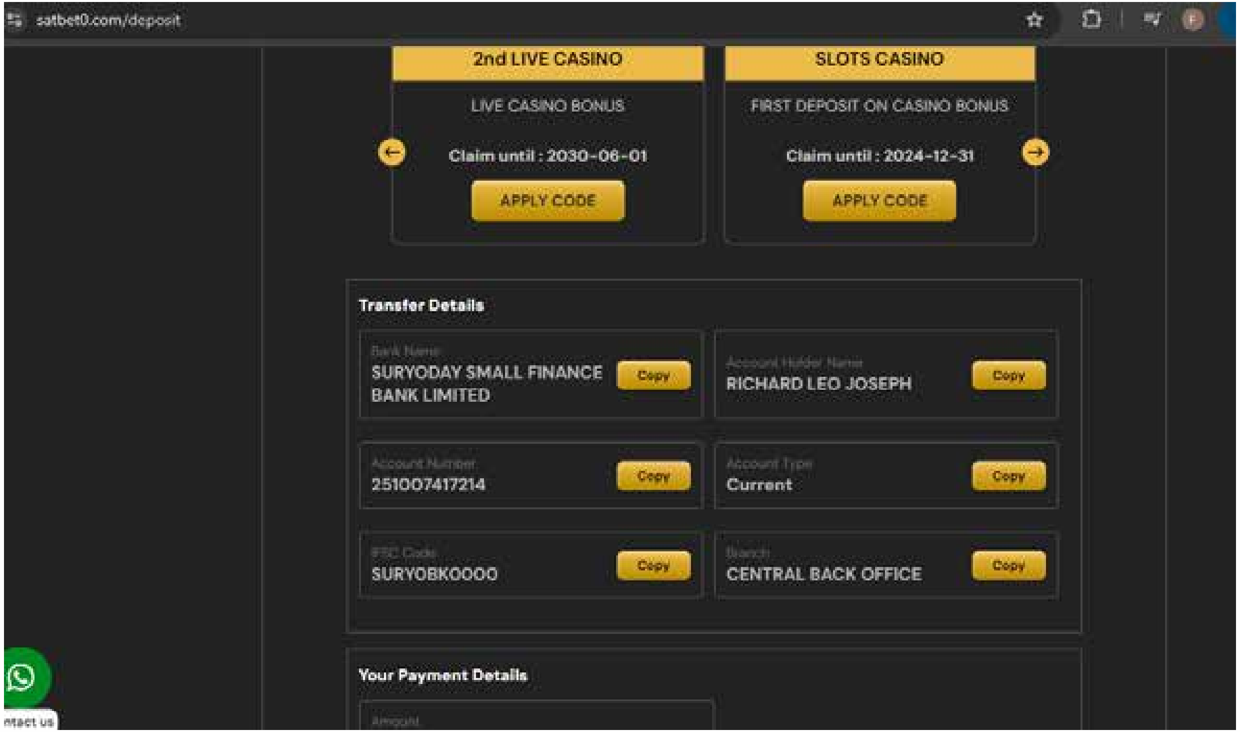
DEPOSIT IMPS

Please make a transfer to the following account before requesting a deposit. After sending the payment, insert mandatory fields like Transaction ID/ Ref. No/ UTR/ NAME in the specified field.

Account Holder Name	muthulakshmi
Account Number	60509483404
IFSC code	mahb0002187

ANOTHER REQUISITES

Money Mule Operators



Transfer Details

Bank Name
SURYODAY SMALL FINANCE BANK LIMITED

Account Holder Name
RICHARD LEO JOSEPH

Account Number
251007417214

Account Type
Current

IFSC Code
SURYOBK0000

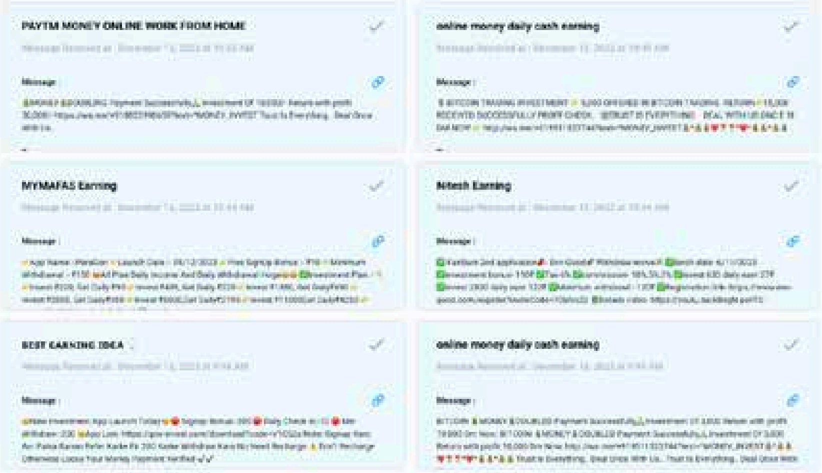
Branch
CENTRAL BACK OFFICE

Your Payment Details

Amount

Fake Investment Scams : Pig Butchering.

- Victims are enticed by high-return promises via fake websites and companies using apps and online payment gateways.
- Personal and banking details are collected through apps for online payments, with fraudulent returns promised.
- Research monitoring **218 Telegram channels** shows a surge in investment scams.



PAYTM MONEY ONLINE WORK FROM HOME

Message Received at : [illegible]

Message :

[illegible]

online money daily cash earning

Message Received at : [illegible]

Message :

[illegible]

MYMAFAS Earning

Message Received at : [illegible]

Message :

[illegible]

Nitech Earning

Message Received at : [illegible]

Message :

[illegible]

BEST EARNING IDEA

Message Received at : [illegible]

Message :

[illegible]

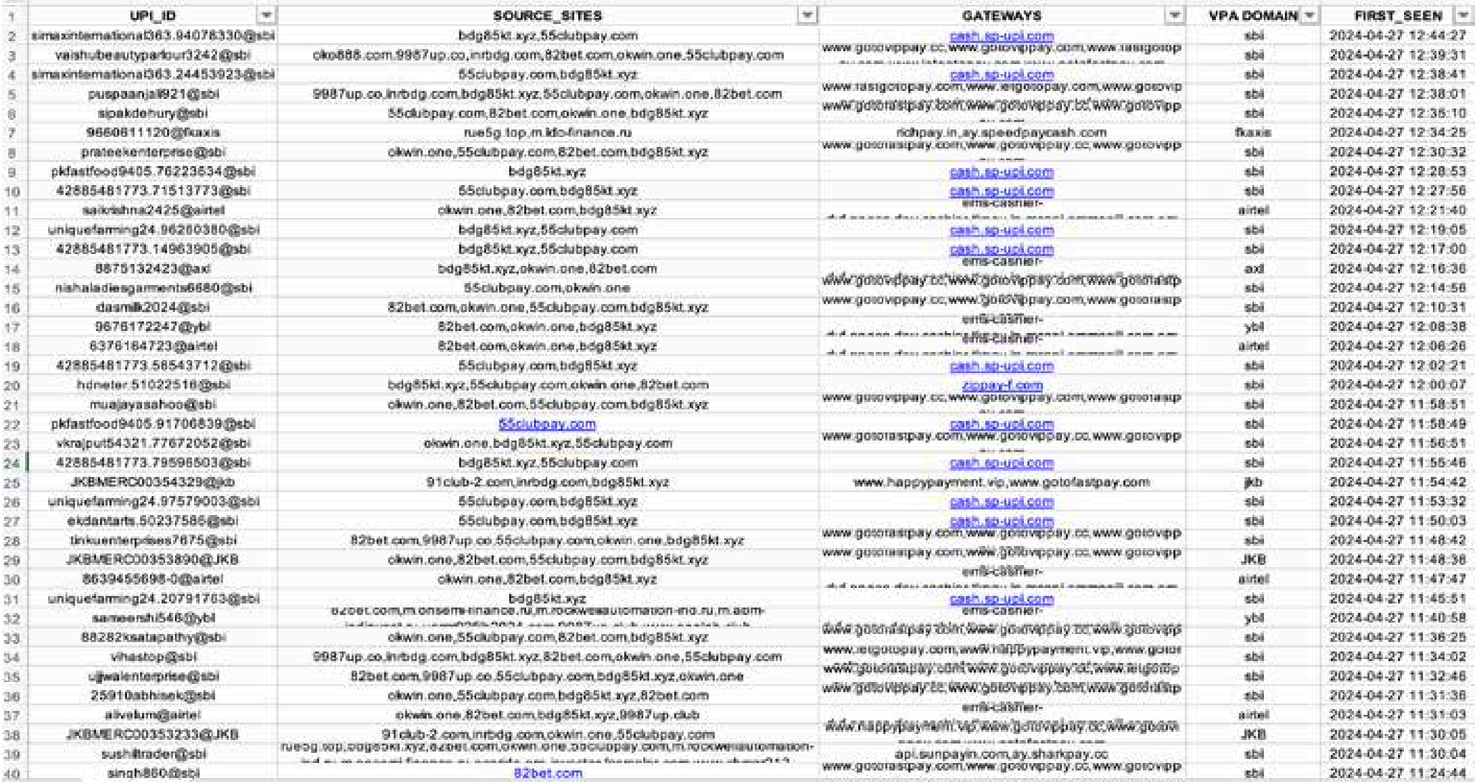
online money daily cash earning

Message Received at : [illegible]

Message :

[illegible]

Suspicious UPI IDs from Fraudulent Groups.



1	UPI_ID	SOURCE_SITES	GATEWAYS	VPA DOMAIN	FIRST_SEEN
2	simaxinternational363.94078330@sbi	bdg85kt.xyz,55clubpay.com	cash.sp-upi.com	sbi	2024-04-27 12:44:27
3	vaishubeautyparlour3242@sbi	oko888.com,9987up.co,inrbdg.com,82bet.com,okwin.one,55clubpay.com	www.gotovippay.cc,www.gotovippay.com,www.fastgotop	sbi	2024-04-27 12:39:31
4	simaxinternational363.24453923@sbi	55clubpay.com,bdg85kt.xyz	cash.sp-upi.com	sbi	2024-04-27 12:38:41
5	puspaanjali921@sbi	9987up.co,inrbdg.com,bdg85kt.xyz,55clubpay.com,okwin.one,82bet.com	www.fastgotopay.com,www.letgotopay.com,www.gotovip	sbi	2024-04-27 12:38:01
6	sipakdehury@sbi	55clubpay.com,82bet.com,okwin.one,bdg85kt.xyz	www.gotofastpay.com,www.gotovippay.cc,www.gotovipp	sbi	2024-04-27 12:36:10
7	9660611120@fkaxis	rue5g.top,m.lido-finance.ru	richpay.in,ay.speedpaycash.com	fkaxis	2024-04-27 12:34:25
8	prateekenterprise@sbi	okwin.one,55clubpay.com,82bet.com,bdg85kt.xyz	www.gotofastpay.com,www.gotovippay.cc,www.gotovipp	sbi	2024-04-27 12:30:32
9	pkfastfood9405.76223634@sbi	bdg85kt.xyz	cash.sp-upi.com	sbi	2024-04-27 12:28:53
10	42885481773.71513773@sbi	55clubpay.com,bdg85kt.xyz	cash.sp-upi.com	sbi	2024-04-27 12:27:56
11	saikrishna2425@airtel	okwin.one,82bet.com,bdg85kt.xyz	ems-cashier-	airtel	2024-04-27 12:21:40
12	uniquefarming24.96260380@sbi	bdg85kt.xyz,55clubpay.com	cash.sp-upi.com	sbi	2024-04-27 12:19:05
13	42885481773.14963905@sbi	bdg85kt.xyz,55clubpay.com	cash.sp-upi.com	sbi	2024-04-27 12:17:00
14	8875132423@axl	bdg85kt.xyz,okwin.one,82bet.com	ems-cashier-	axl	2024-04-27 12:16:36
15	nishaladiesgarments6680@sbi	55clubpay.com,okwin.one	www.gotovippay.cc,www.gotovippay.com,www.gotofastp	sbi	2024-04-27 12:14:56
16	dasmilk2024@sbi	82bet.com,okwin.one,55clubpay.com,bdg85kt.xyz	www.gotovippay.cc,www.gotovippay.com,www.gotofastp	sbi	2024-04-27 12:10:31
17	9676172247@ybl	82bet.com,okwin.one,bdg85kt.xyz	ems-cashier-	ybl	2024-04-27 12:08:38
18	6376164723@airtel	82bet.com,okwin.one,bdg85kt.xyz	ems-cashier-	airtel	2024-04-27 12:06:26
19	42885481773.56543712@sbi	55clubpay.com,bdg85kt.xyz	cash.sp-upi.com	sbi	2024-04-27 12:02:21
20	hdneter.51022516@sbi	bdg85kt.xyz,55clubpay.com,okwin.one,82bet.com	zippay-f.com	sbi	2024-04-27 12:00:07
21	muajayasahoo@sbi	okwin.one,82bet.com,55clubpay.com,bdg85kt.xyz	www.gotovippay.cc,www.gotovippay.com,www.gotofastp	sbi	2024-04-27 11:58:51
22	pkfastfood9405.91706839@sbi	55clubpay.com	cash.sp-upi.com	sbi	2024-04-27 11:58:49
23	vkrajput54321.77672052@sbi	okwin.one,bdg85kt.xyz,55clubpay.com	www.gotofastpay.com,www.gotovippay.cc,www.gotovipp	sbi	2024-04-27 11:56:51
24	42885481773.79596503@sbi	bdg85kt.xyz,55clubpay.com	cash.sp-upi.com	sbi	2024-04-27 11:55:46
25	JKBMERC00354329@jkb	91club-2.com,inrbdg.com,bdg85kt.xyz	www.happypayment.vip,www.gotofastpay.com	jkb	2024-04-27 11:54:42
26	uniquefarming24.97579003@sbi	55clubpay.com,bdg85kt.xyz	cash.sp-upi.com	sbi	2024-04-27 11:53:32
27	ekdantarts.50237586@sbi	55clubpay.com,bdg85kt.xyz	cash.sp-upi.com	sbi	2024-04-27 11:50:03
28	tinkuenterprises7675@sbi	82bet.com,9987up.co,55clubpay.com,okwin.one,bdg85kt.xyz	www.gotofastpay.com,www.gotovippay.cc,www.gotovipp	sbi	2024-04-27 11:48:42
29	JKBMERC00353890@JKB	okwin.one,82bet.com,55clubpay.com,bdg85kt.xyz	www.gotofastpay.com,www.gotovippay.cc,www.gotovipp	JKB	2024-04-27 11:48:36
30	8639455698-0@airtel	okwin.one,82bet.com,bdg85kt.xyz	ems-cashier-	airtel	2024-04-27 11:47:47
31	uniquefarming24.20791763@sbi	bdg85kt.xyz	cash.sp-upi.com	sbi	2024-04-27 11:46:51
32	sameershi546@ybl	82bet.com,m.onsemi-finance.ru,m.rockwellautomation-ind.ru,m.aom-	ems-cashier-	ybl	2024-04-27 11:40:58
33	88282ksatapathy@sbi	okwin.one,55clubpay.com,82bet.com,bdg85kt.xyz	www.gotofastpay.com,www.gotovippay.cc,www.gotovipp	sbi	2024-04-27 11:36:25
34	vihastop@sbi	9987up.co,inrbdg.com,bdg85kt.xyz,82bet.com,okwin.one,55clubpay.com	www.letgotopay.com,www.happypayment.vip,www.gotof	sbi	2024-04-27 11:34:02
35	ujjwalenterprise@sbi	82bet.com,9987up.co,55clubpay.com,bdg85kt.xyz,okwin.one	www.gotofastpay.com,www.gotovippay.cc,www.letgotop	sbi	2024-04-27 11:32:46
36	25910abhisek@sbi	okwin.one,55clubpay.com,bdg85kt.xyz,82bet.com	www.gotovippay.cc,www.gotovippay.com,www.gotofastp	sbi	2024-04-27 11:31:36
37	alivelum@airtel	okwin.one,82bet.com,bdg85kt.xyz,9987up.club	ems-cashier-	airtel	2024-04-27 11:31:03
38	JKBMERC00353233@JKB	91club-2.com,inrbdg.com,okwin.one,55clubpay.com	www.happypayment.vip,www.gotovippay.cc,www.gotofa	JKB	2024-04-27 11:30:05
39	sushiltraden@sbi	rue5g.top,bdg85kt.xyz,82bet.com,okwin.one,55clubpay.com,m.rockwellautomation-	api.sunpayin.com,ay.sharkpay.cc	sbi	2024-04-27 11:30:04
40	singh860@sbi	82bet.com	www.gotofastpay.com,www.gotovippay.cc,www.gotovipp	sbi	2024-04-27 11:24:44

Tracking of threats FY 24.

The following data was gathered by analyzing 100K+ Telegram messages, providing deep insights into coordinated scam operations:

- **93,210 fake Google ads** targeting customer care and job scams.
- **80,839 WhatsApp phone** numbers involved in fraud and scam activities.
- **45,548 URLs of scam** websites, involving illegal betting and fraudulent investment schemes.
- **9,751 Telegram channels** mentioned in channels promoting scam activities.
- **595 WhatsApp URLs** (profiles and groups) connected to fraudulent activities.
- **1,685 scam-related phone** numbers identified across platforms.
- **48 UPI IDs** associated with fraudulent transactions.
- **125 Bitcoin wallets** involved in scam operations.

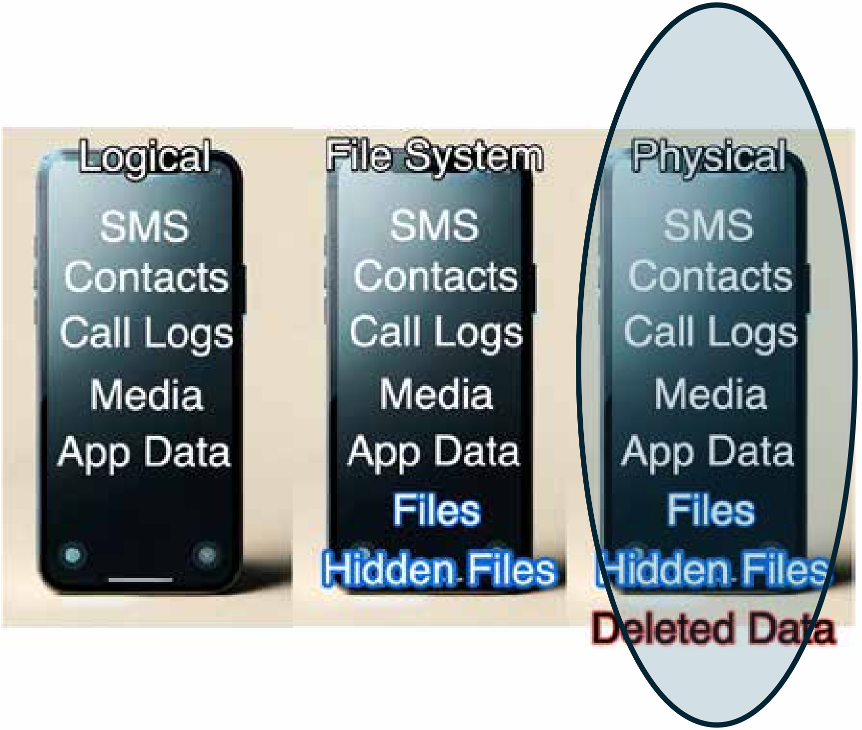
Challenges.

- **Technical & Legal Challenges:**
  - Anonymity of blockchain transactions.
  - Domestic jurisdiction issues.
  - Advanced money laundering techniques.
  - Concept of Organised Crime
- **Regulatory Efforts:**
  - Anti-money laundering (AML) policies.
  - Blockchain analytics & tracing tools.
  - Better Forensics.
  - Collaborative global law enforcement efforts.

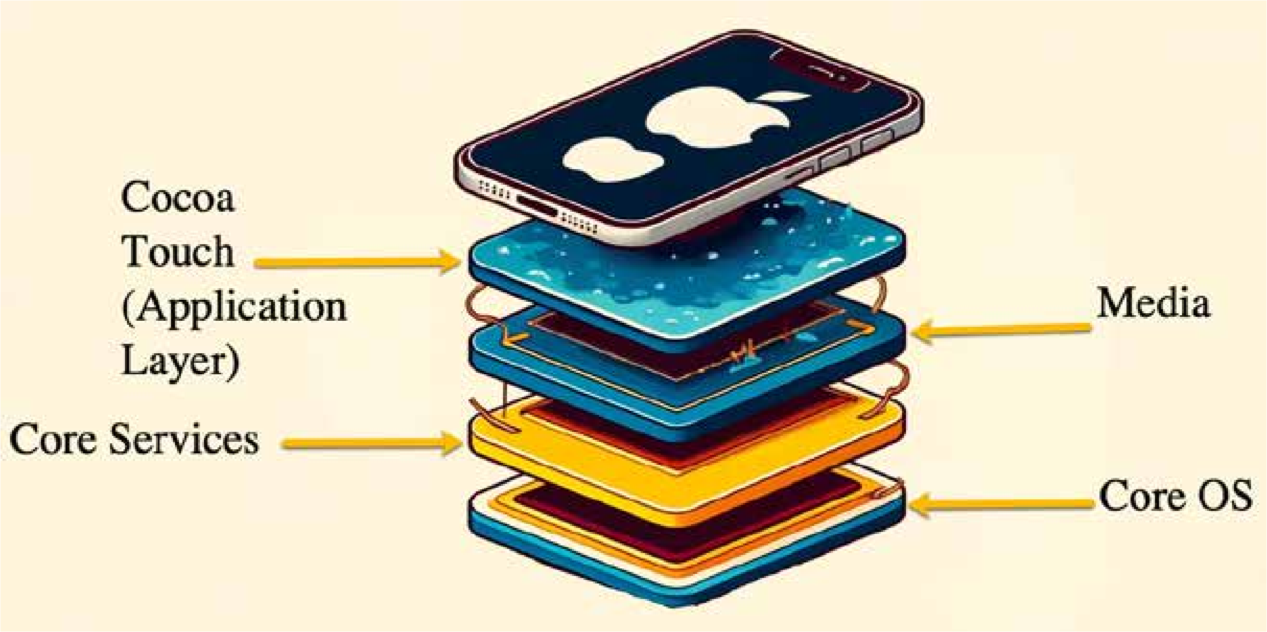
Challenges in Forensics: Mobile Forensics.

Mobile Forensics

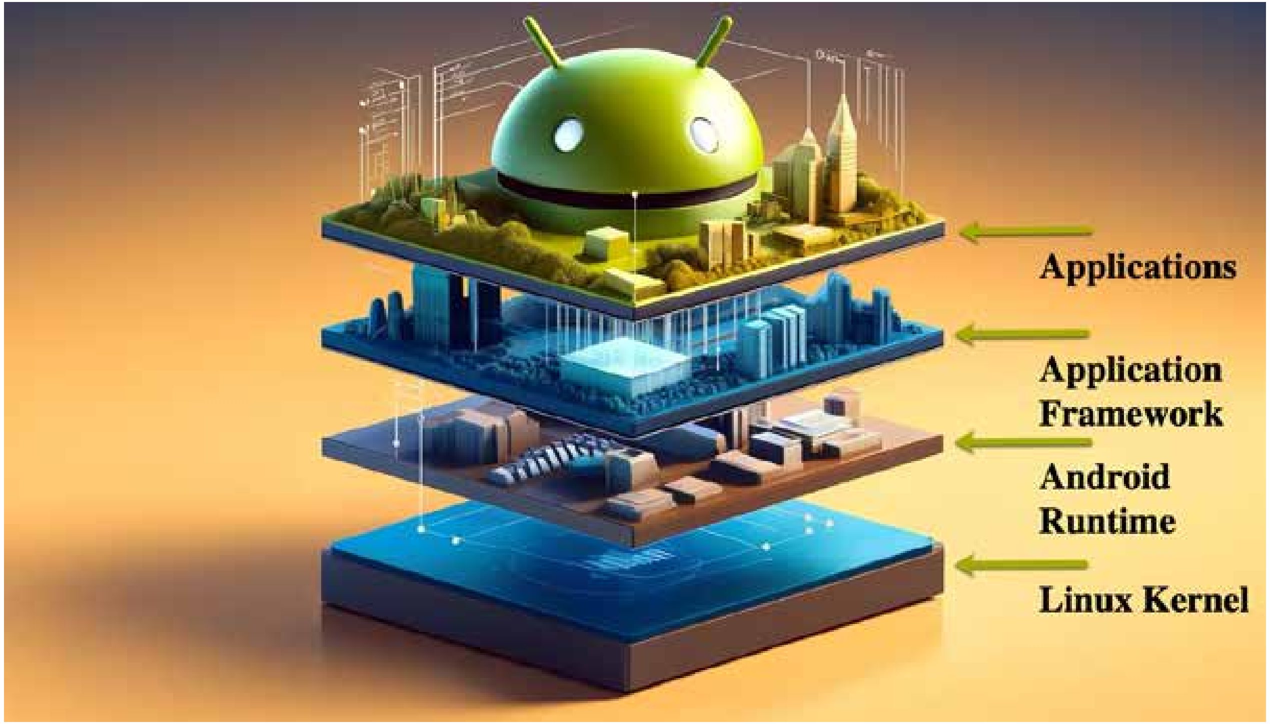
- Several commercial tools are available when you need to perform forensic acquisition and analysis of mobile devices. Some of the most popular vendors include the following:
  - Belkasoft
  - Cellebrite
  - Magnet Forensics
  - MSAB
  - Oxygen Forensics



iOS Running.

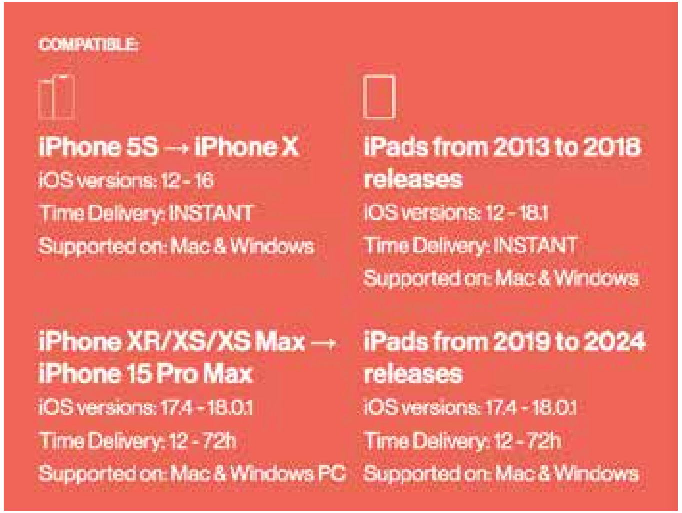


Android Running



Finding Bugs.

- **Checkm8** is a jailbreak exploit for iOS devices that uses a **boot ROM** vulnerability. This security flaw is hardware-based, meaning it can't be patched through iOS updates. It grants you access to the operating system's core, bypassing restrictions and installing software not sanctioned by Apple.
- The Checkm8 exploit is compatible with several Apple devices. It affects devices with chipsets A5 to A11, including iPhones from the 4S to the X, several iPad models, several Apple TV iterations, and some iPod touch models.



COMPATIBLE:

iPhone 5S → iPhone X
iOS versions: 12 - 16
Time Delivery: INSTANT
Supported on: Mac & Windows

iPads from 2013 to 2018 releases
iOS versions: 12 - 18.1
Time Delivery: INSTANT
Supported on: Mac & Windows

iPhone XR/XS/XS Max → iPhone 15 Pro Max
iOS versions: 17.4 - 18.0.1
Time Delivery: 12 - 72h
Supported on: Mac & Windows PC

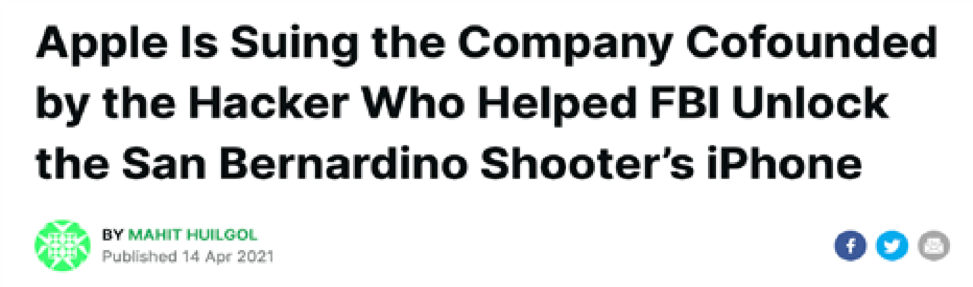
iPads from 2019 to 2024 releases
iOS versions: 17.4 - 18.0.1
Time Delivery: 12 - 72h
Supported on: Mac & Windows

Belkasoft Evidence Center X

Troubles from Apple & Android.

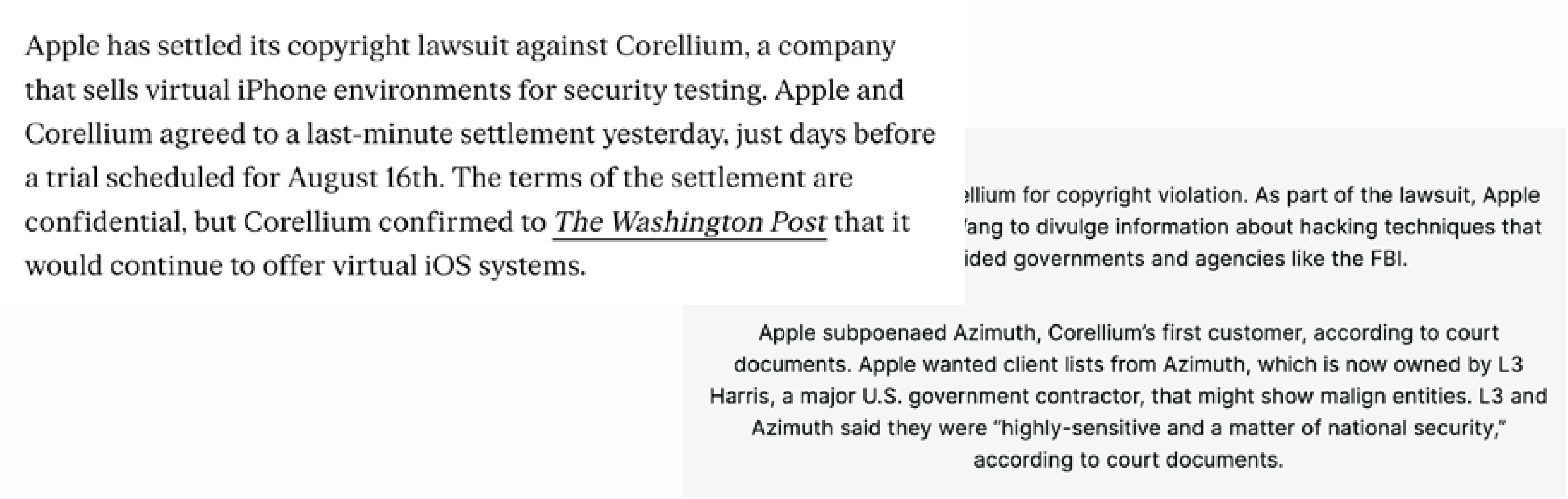
- Apple's USB Restricted Mode (introduced in iOS 11.4.1) is designed to protect user privacy, but as a forensic examiner, it creates a major obstacle.
- After one hour of the phone being locked, USB data transfer is blocked, hindering your ability to extract data.
- Similar limitations from Android as well.

Suites from Apple.



Apple Is Suing the Company Cofounded by the Hacker Who Helped FBI Unlock the San Bernardino Shooter's iPhone

BY MAHIT HUILGOL
Published 14 Apr 2021



Apple has settled its copyright lawsuit against Corellium, a company that sells virtual iPhone environments for security testing. Apple and Corellium agreed to a last-minute settlement yesterday, just days before a trial scheduled for August 16th. The terms of the settlement are confidential, but Corellium confirmed to *The Washington Post* that it would continue to offer virtual iOS systems.

ellium for copyright violation. As part of the lawsuit, Apple
'ang to divulge information about hacking techniques that
ided governments and agencies like the FBI.

Apple subpoenaed Azimuth, Corellium's first customer, according to court documents. Apple wanted client lists from Azimuth, which is now owned by L3 Harris, a major U.S. government contractor, that might show malign entities. L3 and Azimuth said they were "highly-sensitive and a matter of national security," according to court documents.

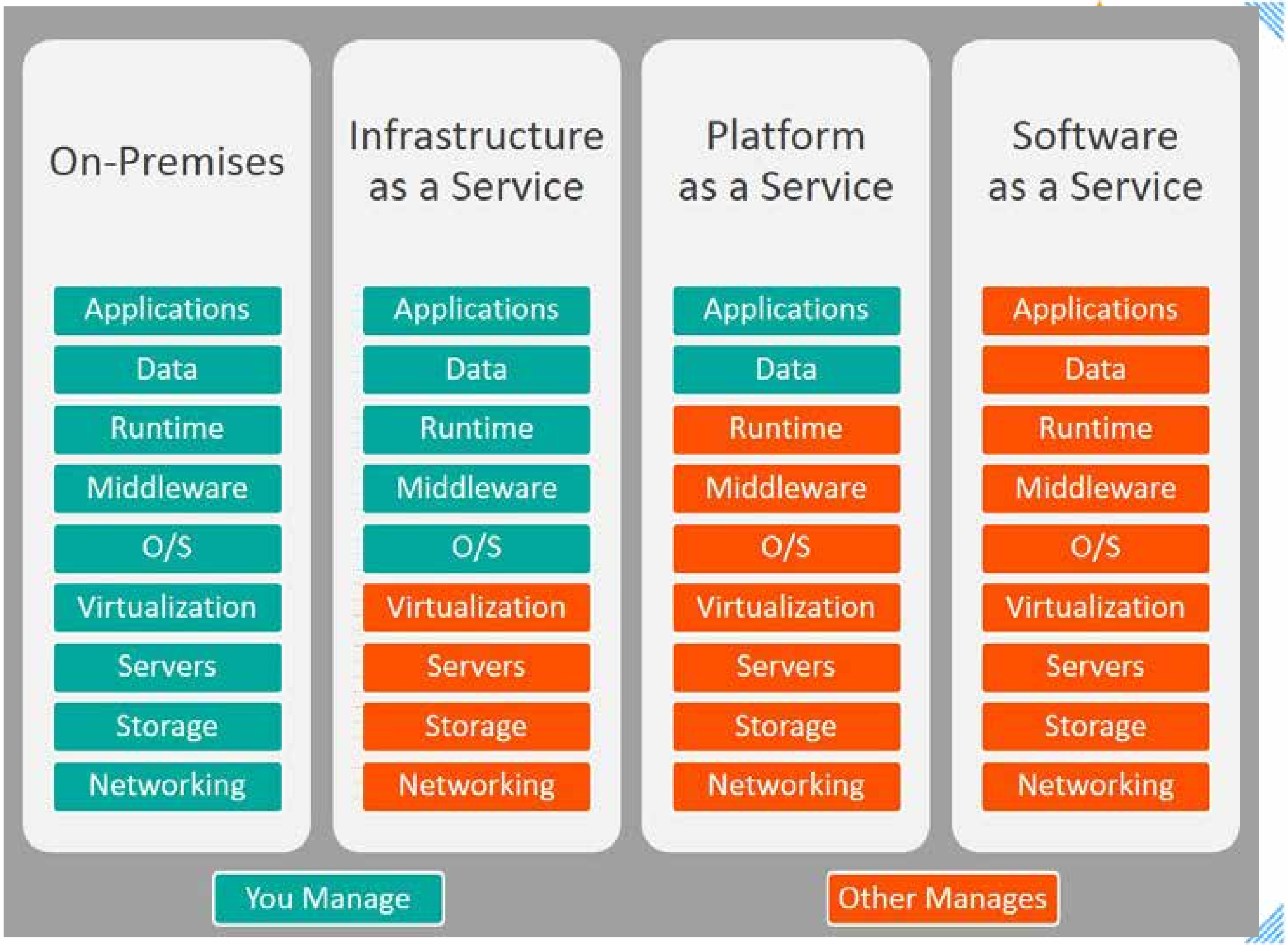
Cellebrite

- With Cellebrite **Universal Forensics Extraction Device** (**UFED**) (https://cellebrite.com), you gain access to a vast array of mobile devices.
- This tool lets you gather digital evidence from smartphones, SIM cards, and SD cards. Throughout the acquisition process, the integrity of the data is preserved.
- There are several methods for data acquisition, such as **full file system** (**FFS**) and physical extractions, which ensure that you have the flexibility and resources needed.

Cloud Forensics

Applications for Income Tax : Brief Background.

Master Sheet on Cloud based offerings.

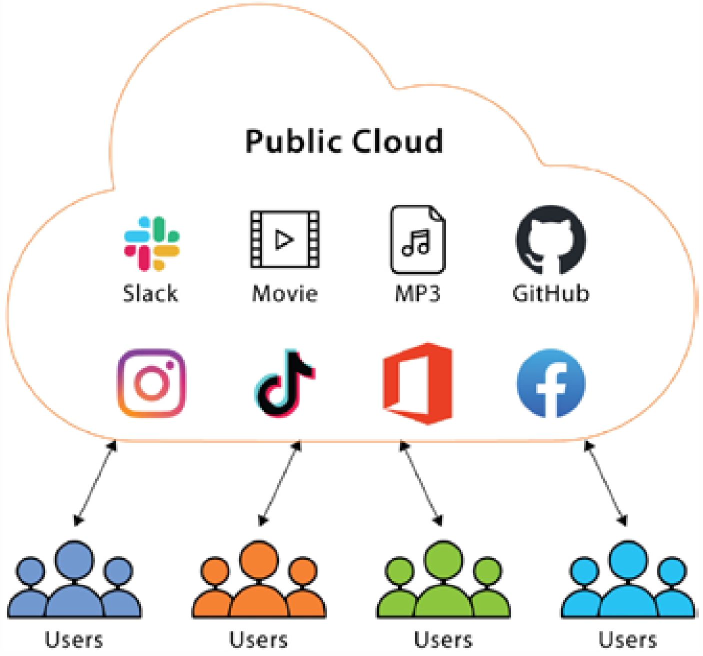


On-Premises	Infrastructure as a Service	Platform as a Service	Software as a Service
🟩 Applications	🟩 Applications	🟩 Applications	🟥 Applications
🟩 Data	🟩 Data	🟩 Data	🟥 Data
🟩 Runtime	🟩 Runtime	🟥 Runtime	🟥 Runtime
🟩 Middleware	🟩 Middleware	🟥 Middleware	🟥 Middleware
🟩 O/S	🟩 O/S	🟥 O/S	🟥 O/S
🟩 Virtualization	🟥 Virtualization	🟥 Virtualization	🟥 Virtualization
🟩 Servers	🟥 Servers	🟥 Servers	🟥 Servers
🟩 Storage	🟥 Storage	🟥 Storage	🟥 Storage
🟩 Networking	🟥 Networking	🟥 Networking	🟥 Networking

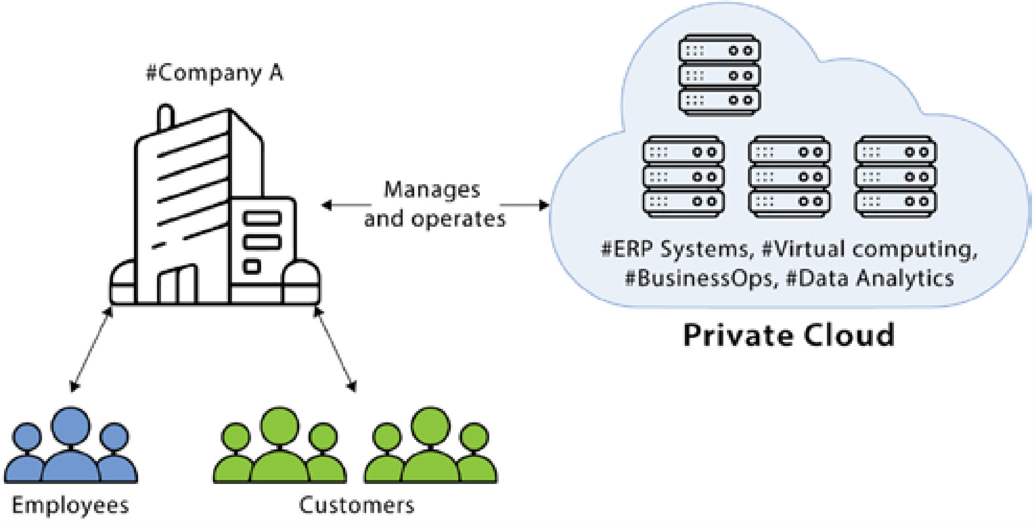
🟩 You Manage

🟥 Other Manages

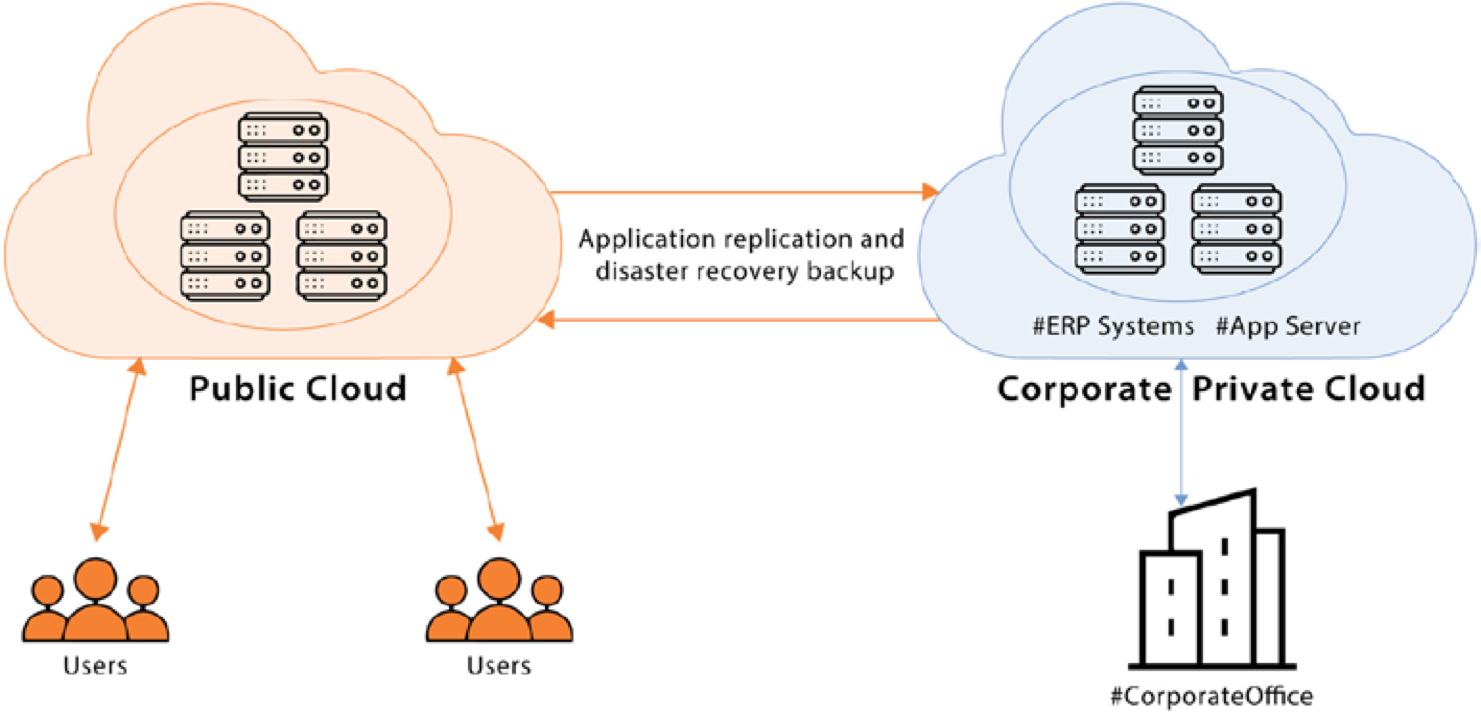
Public Cloud



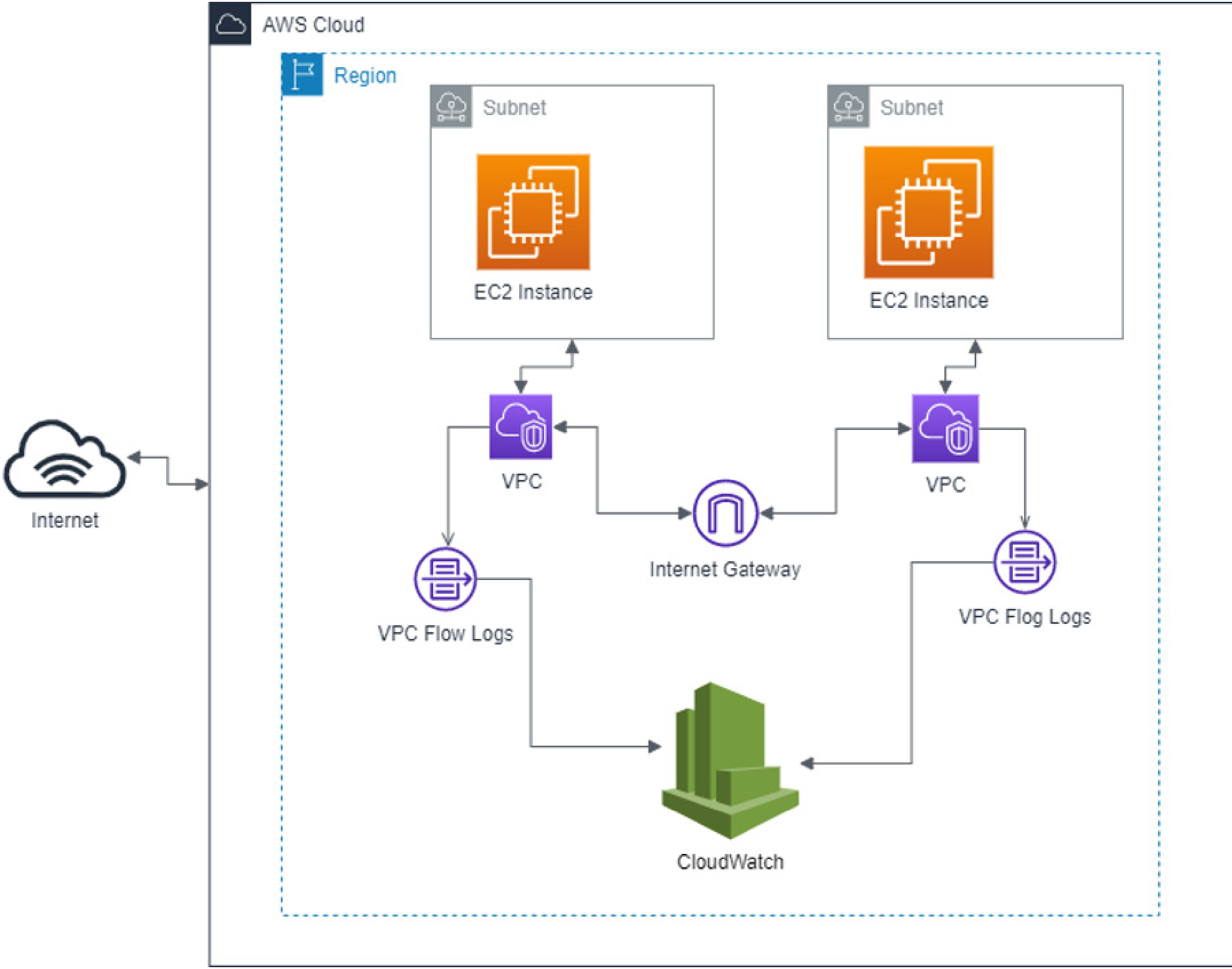
Private Cloud


#Company A
Manages
and operates
#ERP Systems, #Virtual computing,
#BusinessOps, #Data Analytics
Private Cloud
Employees
Customers

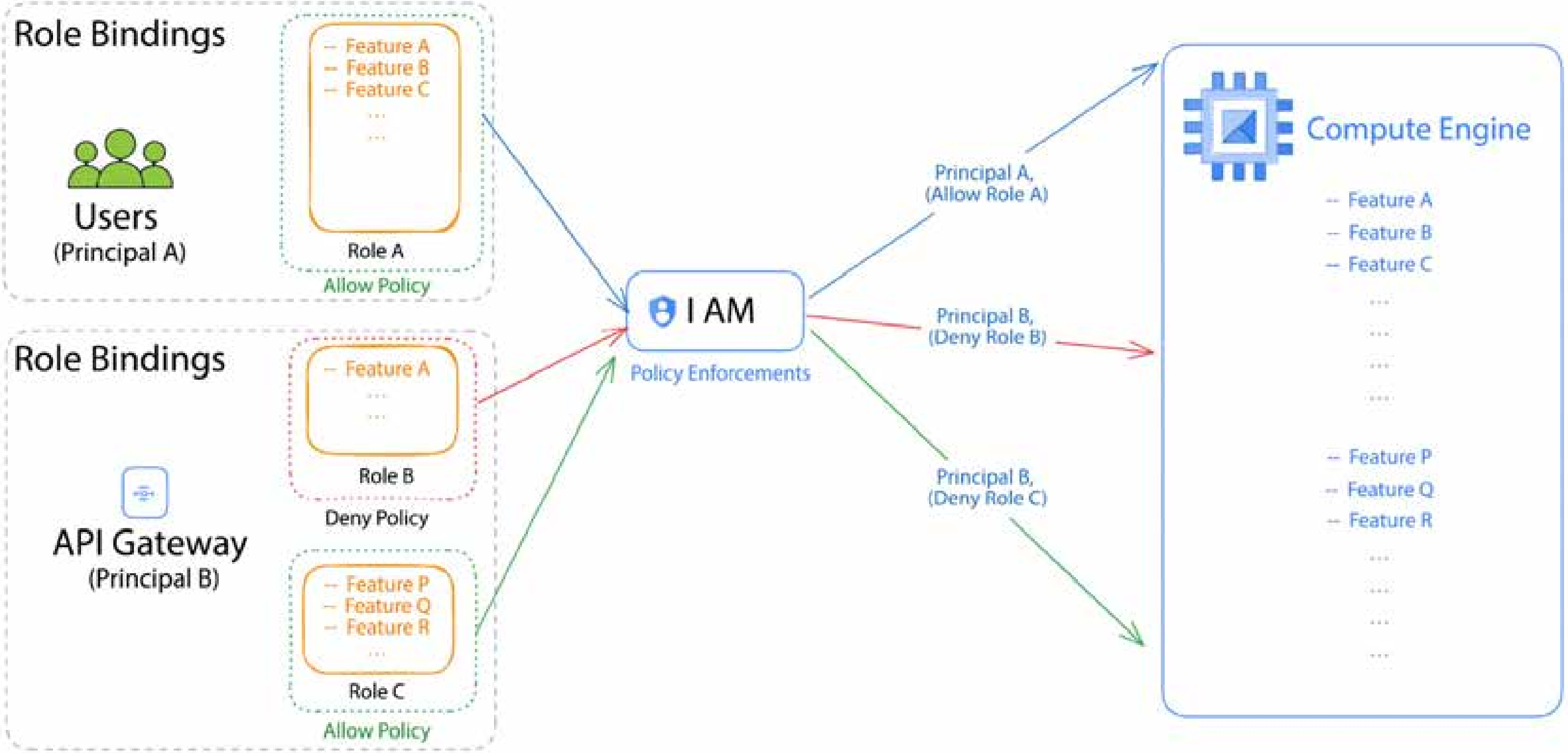
Hybrid Cloud



Mining through Logs.



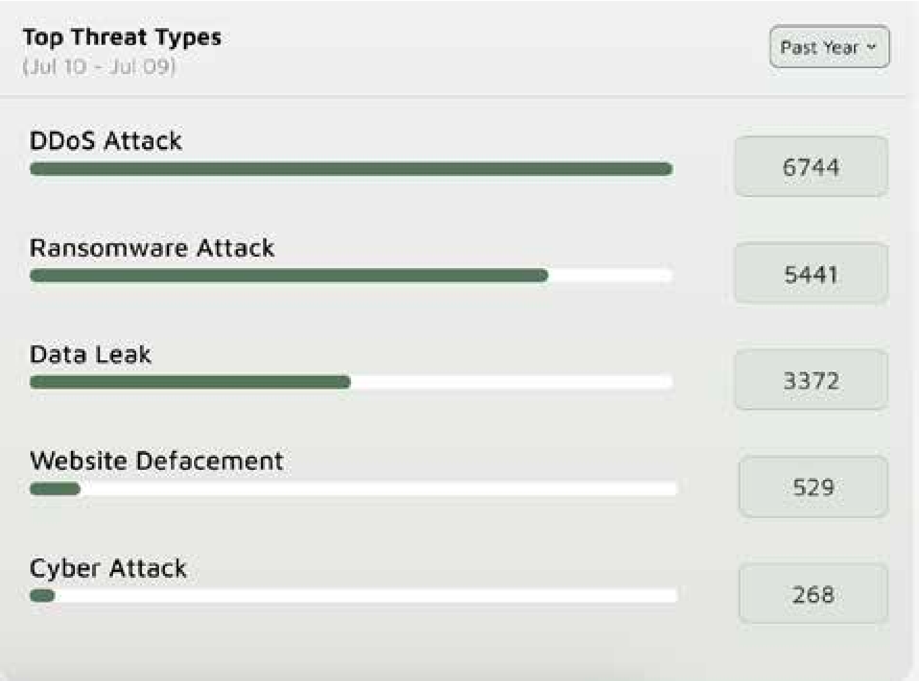
Complex Linkages.



Current Threats in Cybersecurity.

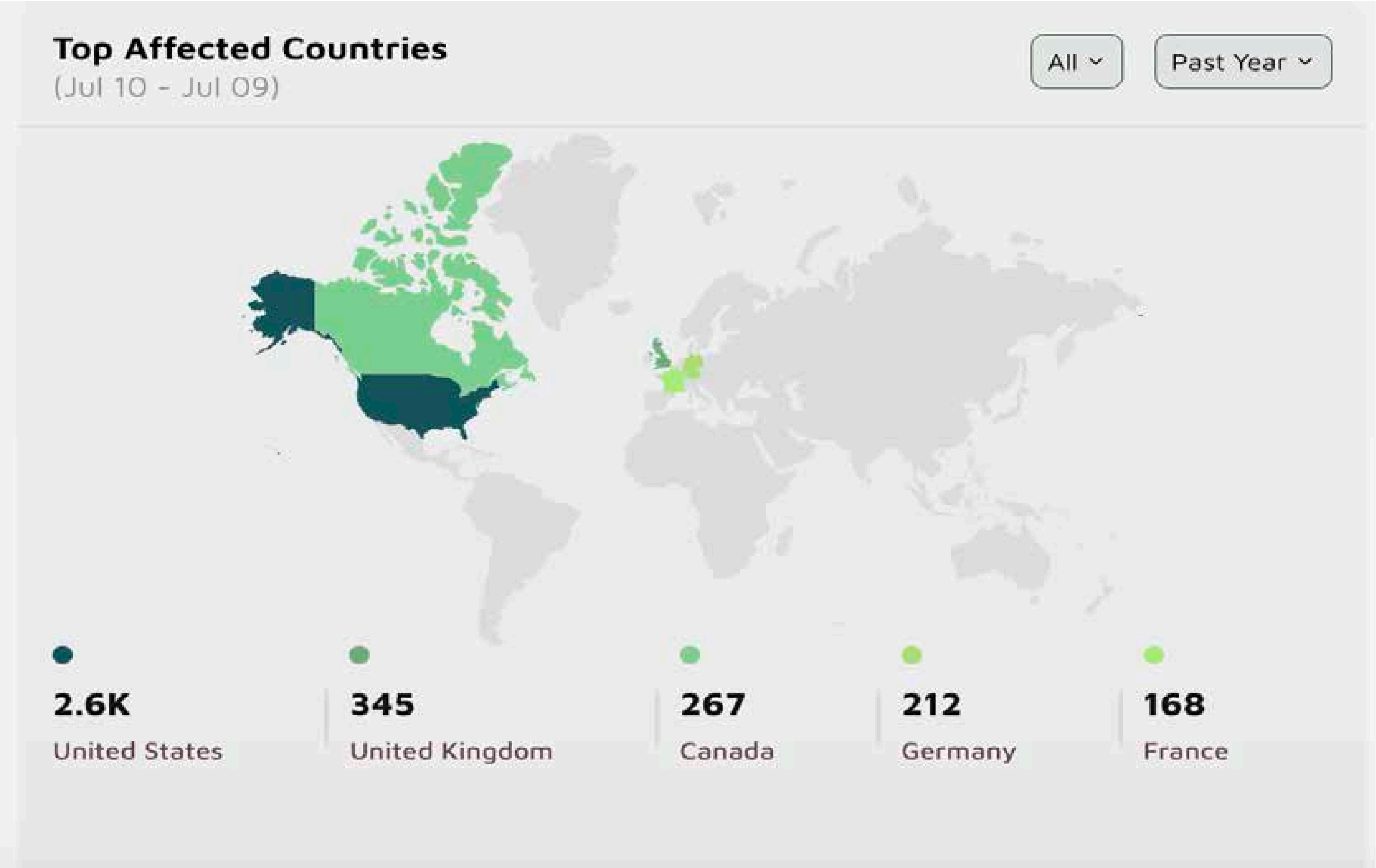
- Phishing
- Ransomware
- Insider threats
- Sophisticated fraud schemes
- State Actors
- Activists

Defending from the APT Groups.



Top Threat Types
(Jul 10 - Jul 09)

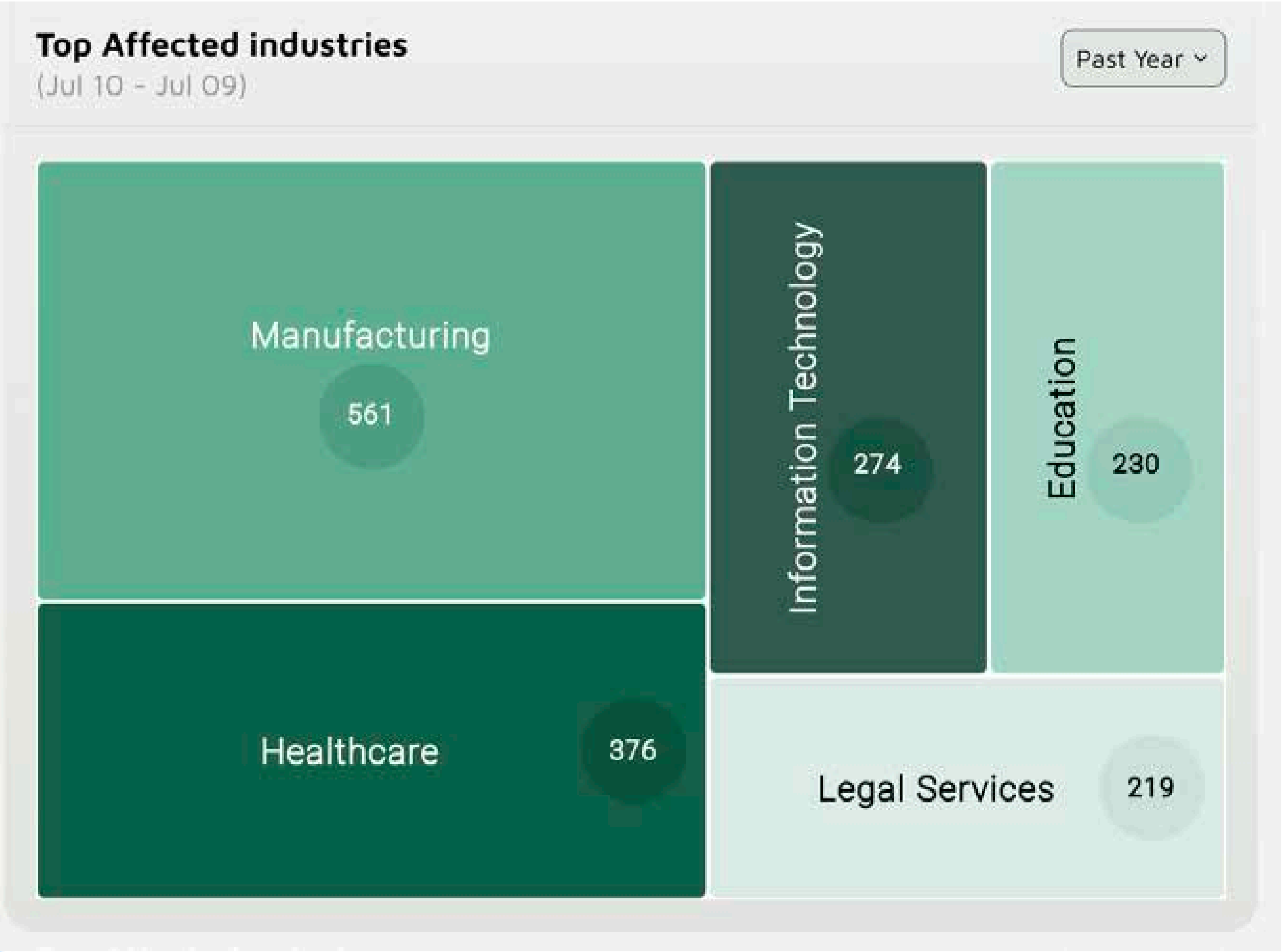
DDoS Attack	6744
Ransomware Attack	5441
Data Leak	3372
Website Defacement	529
Cyber Attack	268



Top Affected Countries

(Jul 10 - Jul 09)

2.6K	345	267	212	168
United States	United Kingdom	Canada	Germany	France

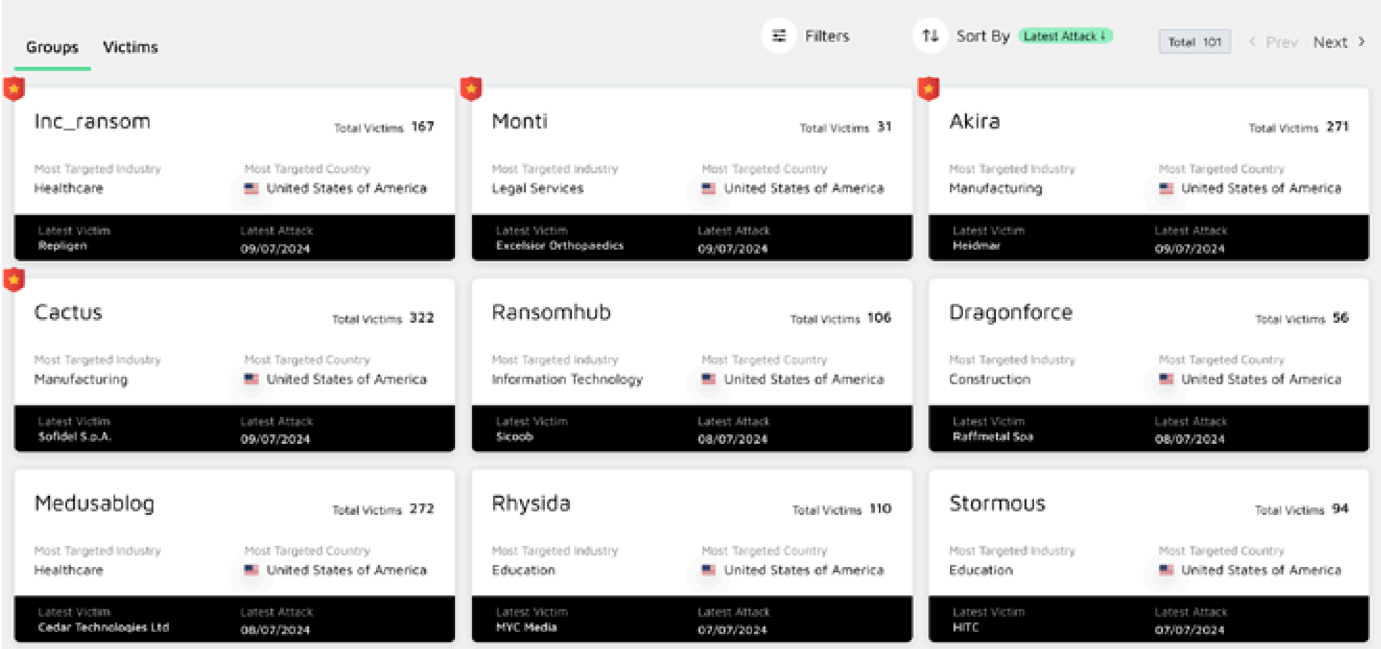


Top Affected industries

(Jul 10 - Jul 09)

Based on tracking of the APT Groups activities by the Saptang Labs Threat Intel Team.

Current Active Ransomware Groups.



Inc_ransom
Total Victims 167
Most Targeted Industry: Healthcare
Most Targeted Country: United States of America
Latest Victim: Repligen
Latest Attack: 09/07/2024

Monti
Total Victims 31
Most Targeted Industry: Legal Services
Most Targeted Country: United States of America
Latest Victim: Excelsior Orthopaedics
Latest Attack: 09/07/2024

Akira
Total Victims 271
Most Targeted Industry: Manufacturing
Most Targeted Country: United States of America
Latest Victim: Heidmar
Latest Attack: 09/07/2024

Cactus
Total Victims 322
Most Targeted Industry: Manufacturing
Most Targeted Country: United States of America
Latest Victim: Sofidel S.p.A.
Latest Attack: 09/07/2024

Ransomhub
Total Victims 106
Most Targeted Industry: Information Technology
Most Targeted Country: United States of America
Latest Victim: Sicoob
Latest Attack: 08/07/2024

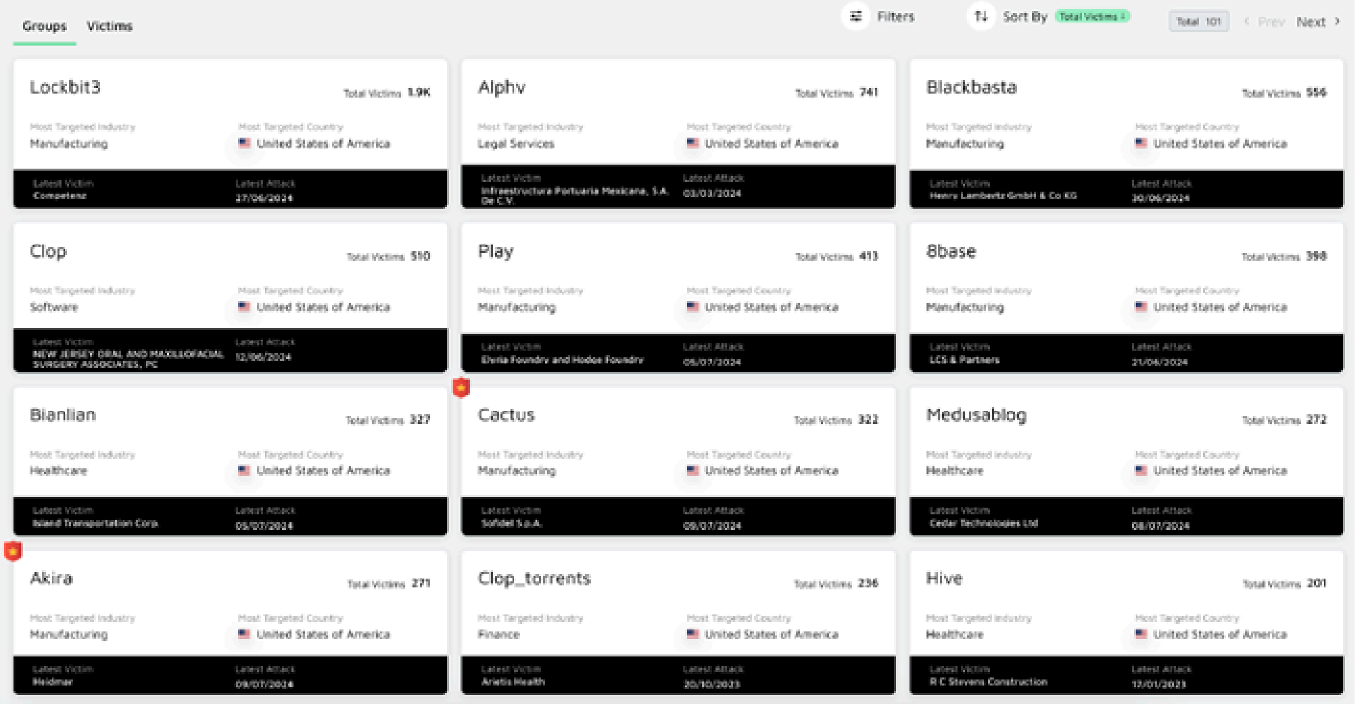
Dragonforce
Total Victims 56
Most Targeted Industry: Construction
Most Targeted Country: United States of America
Latest Victim: Raffmetal Spa
Latest Attack: 08/07/2024

Medusablog
Total Victims 272
Most Targeted Industry: Healthcare
Most Targeted Country: United States of America
Latest Victim: Cedar Technologies Ltd
Latest Attack: 08/07/2024

Rhysida
Total Victims 110
Most Targeted Industry: Education
Most Targeted Country: United States of America
Latest Victim: MYC Media
Latest Attack: 07/07/2024

Stormous
Total Victims 94
Most Targeted Industry: Education
Most Targeted Country: United States of America
Latest Victim: HITC
Latest Attack: 07/07/2024

Most Dangerous Ransomware Groups.



Sort By Total Victims

Total 101

Lockbit3 Total Victims 1.9K
Most Targeted Industry: Manufacturing
Most Targeted Country: United States of America
Latest Victim: Competenz
Latest Attack: 27/06/2024

Alphv Total Victims 741
Most Targeted Industry: Legal Services
Most Targeted Country: United States of America
Latest Victim: Infraestructura Portuaria Mexicana, S.A. De C.V.
Latest Attack: 03/03/2024

Blackbasta Total Victims 556
Most Targeted Industry: Manufacturing
Most Targeted Country: United States of America
Latest Victim: Henry Lambertz GmbH & Co KG
Latest Attack: 30/06/2024

Clop Total Victims 510
Most Targeted Industry: Software
Most Targeted Country: United States of America
Latest Victim: NEW JERSEY ORAL AND MAXILLOFACIAL SURGERY ASSOCIATES, PC
Latest Attack: 12/06/2024

Play Total Victims 413
Most Targeted Industry: Manufacturing
Most Targeted Country: United States of America
Latest Victim: Elveria Foundry and Hodge Foundry
Latest Attack: 05/07/2024

8base Total Victims 398
Most Targeted Industry: Manufacturing
Most Targeted Country: United States of America
Latest Victim: LCS & Partners
Latest Attack: 21/06/2024

Bianlian Total Victims 327
Most Targeted Industry: Healthcare
Most Targeted Country: United States of America
Latest Victim: Island Transportation Corp.
Latest Attack: 05/07/2024

Cactus Total Victims 322
Most Targeted Industry: Manufacturing
Most Targeted Country: United States of America
Latest Victim: Sofidel S.p.A.
Latest Attack: 09/07/2024

Medusablog Total Victims 272
Most Targeted Industry: Healthcare
Most Targeted Country: United States of America
Latest Victim: Cedar Technologies Ltd
Latest Attack: 08/07/2024

Akira Total Victims 271
Most Targeted Industry: Manufacturing
Most Targeted Country: United States of America
Latest Victim: Heidmar
Latest Attack: 09/07/2024

Clop_torrents Total Victims 236
Most Targeted Industry: Finance
Most Targeted Country: United States of America
Latest Victim: Arietis Health
Latest Attack: 20/10/2023

Hive Total Victims 201
Most Targeted Industry: Healthcare
Most Targeted Country: United States of America
Latest Victim: R C Stevens Construction
Latest Attack: 17/01/2023

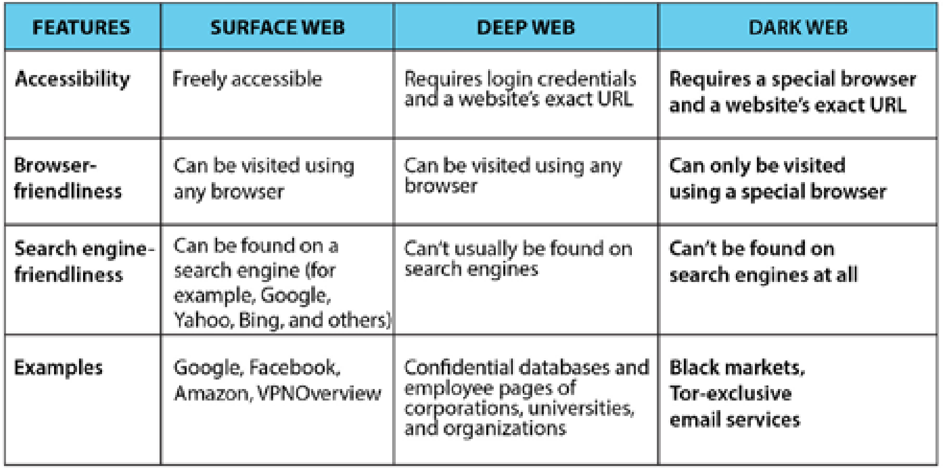
Challenges to Investigation.

Cyberspace

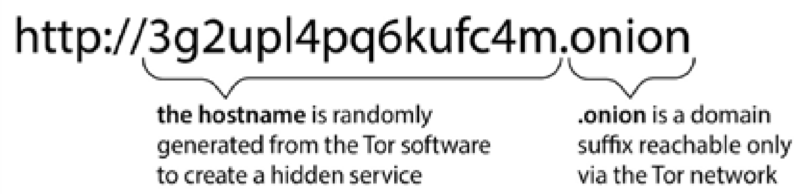
Disruptor-in-chief.

- Underlying basis for all transformations.
- A **global** domain within the **information environment** consisting of the **interdependent** networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
- **Implications : Information Revolution.**
  - Global, Anonymous, Rapid & Cheap Communication Framework
  - Form Groups, Coordinate, Cleanup at will.
  - Secured Encrypted Communications & Financial Networks.

Operating through Deepweb & Darkweb.



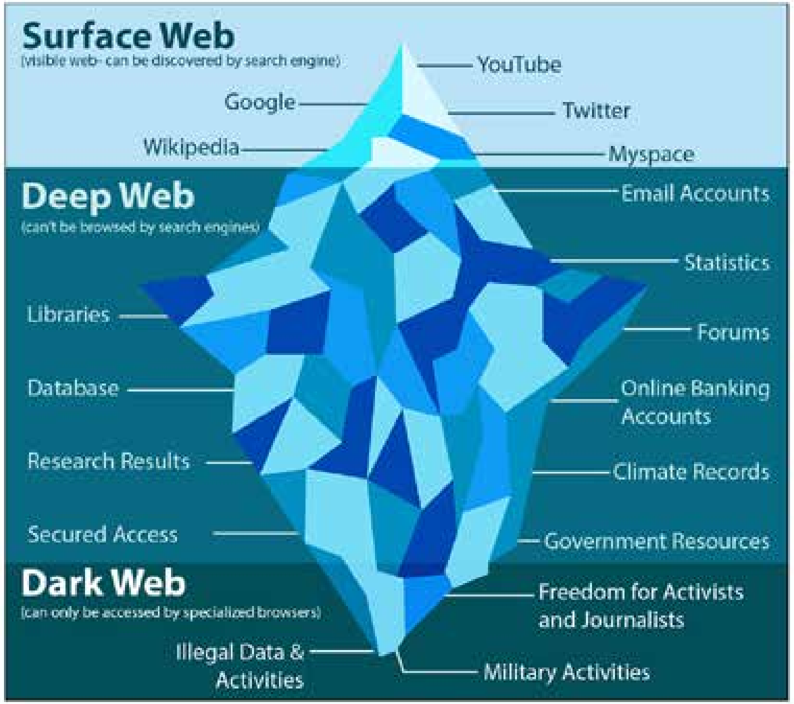
FEATURES	SURFACE WEB	DEEP WEB	DARK WEB
Accessibility	Freely accessible	Requires login credentials and a website's exact URL	**Requires a special browser and a website's exact URL**
Browser-friendliness	Can be visited using any browser	Can be visited using any browser	**Can only be visited using a special browser**
Search engine-friendliness	Can be found on a search engine (for example, Google, Yahoo, Bing, and others)	Can't usually be found on search engines	**Can't be found on search engines at all**
Examples	Google, Facebook, Amazon, VPNOverview	Confidential databases and employee pages of corporations, universities, and organizations	**Black markets, Tor-exclusive email services**



$$\text{http://}\underbrace{\text{3g2upl4pq6kufc4m}}\underbrace{\text{.onion}}$$

the hostname is randomly generated from the Tor software to create a hidden service

.onion is a domain suffix reachable only via the Tor network



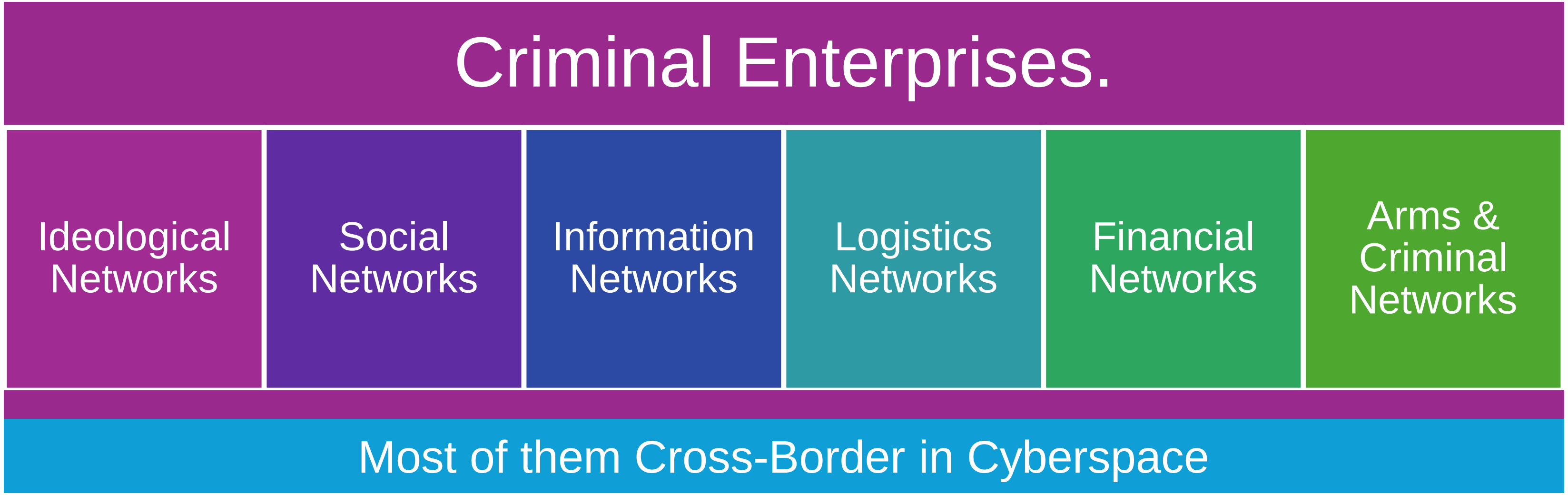
Challenges to Traditional Investigations

- **Anonymous VOIP communications**: WhatsApp, Telegram & Signal.
- **Fintech, Crypto Challenge** : Banks & Financial Intermediaries have no clue.
- **Cloud/Complex ERP Solutions** : Tough to discover & no ready-made audit solutions.
- **Availability of expertise for extraction of anti-forensic solutions**: Secret Apps

Quick Situational Analysis.

- Unable to Observe.
  - Cartels or Groups gone underground.
  - Coordination of the activities is invisible.
  - Impact of the adversarial actions is too quick to notice.
  - Post-mortem data collected is too large to analyze for lessons.
- Unable to Orient on what limited data we see.
  - Old Systems and conclusions based on limited observations are indecisive and curtail operations – limiting exposure and solutions.
  - Institutional Capabilities to counter are not growing fast enough – Operational and financial autonomy.
  - Agility is missing - mechanisms for co-opting technological solutions is too slow or non-existent.
  - New Technological advances are being adapted by adversaries with out our knowledge.

Comprehensive Nature of Crime.



Criminal Enterprises.

Ideological Networks

Social Networks

Information Networks

Logistics Networks

Financial Networks

Arms & Criminal Networks

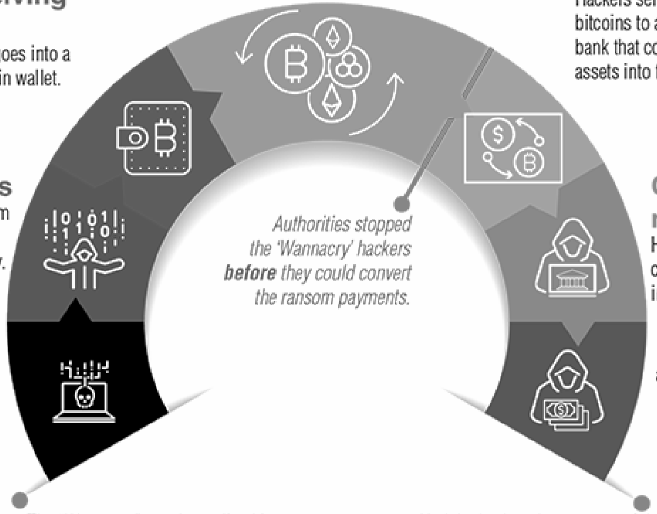
Most of them Cross-Border in Cyberspace

Challenges in Forensics.

- **Technology to acquire data is fast falling behind.**
  - Most of the Platforms (Apple/Android) are closing doors available for forensic analysis.
  - Most of the popular platforms like Cloud etc. require a totally different approach.
- **Frequent Updates to Software**
  - Most of the anti-malware and anti-backdoor features of the operating systems are also making forensics difficult and fast changing field.
  - These changes also make forensics a very expensive, time consuming and complex job.
- **Unfavorable Legal Consequences**
  - Companies like Apple and others are suing forensic operators.
- **Lack of Financial Support for the Forensics**
  - Forensic Products and Software Building is a highly qualified job and not well paid.

Case Study: Bitcoin Tracking.

Bitcoin: Challenges - Dark Web Markets.



Virus
Computers are infected with a virus, disabling businesses, even hospitals, until a ransom is paid.

Ransom payments
Victims pay the hackers a ransom in Bitcoin to decrypt their computer & resume their activity.

Hackers' receiving wallet
Each ransom payment goes into a publicly identified bitcoin wallet.

Layering
Multiple transactions convert the payments from one virtual asset into another to remove all links to the crime.

Virtual Asset Service Provider
Hackers send the 'cleaned' bitcoins to a service provider or bank that converts the virtual assets into fiat money.

Conversion into regulated currency
Hackers receive the bitcoins in the currency of their choice, ready to invest in a bank.

and spend.

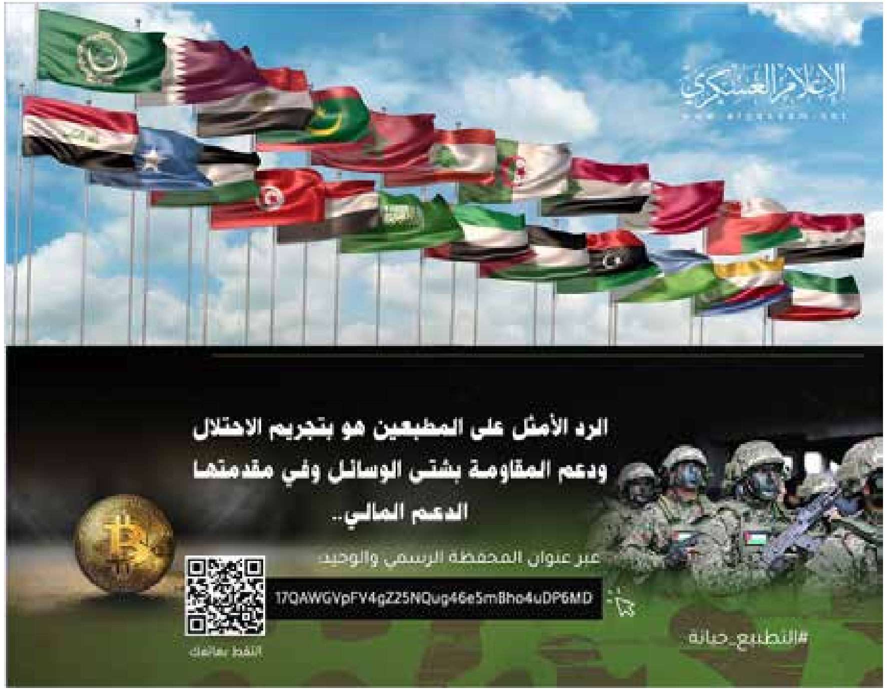
*Authorities stopped the 'Wannacry' hackers **before** they could convert the ransom payments.*

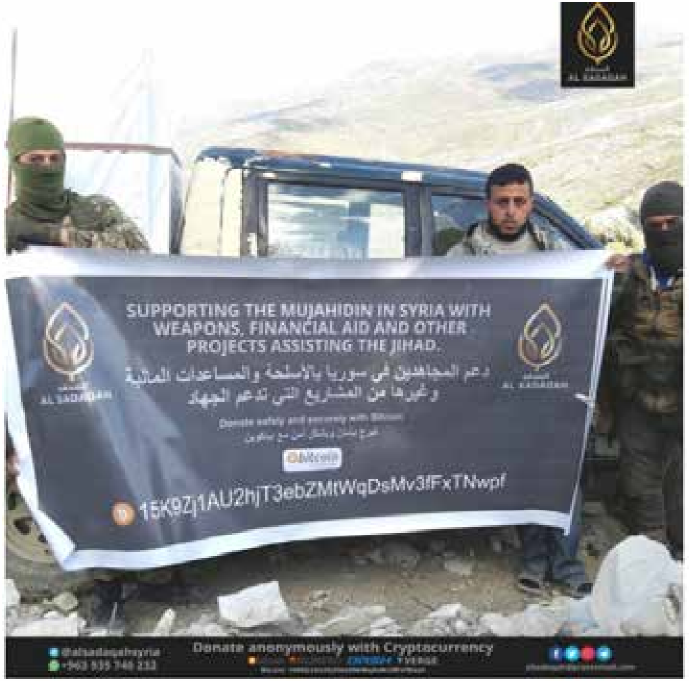
The "Wannacry" attack paralised its victims' source of income, health care and other vital services, resulting in a total damage of USD 8 billion

Had the hackers been successful, they would have received a fraction of the amount of damage they caused: USD 100 million

Darkweb Market Volumes

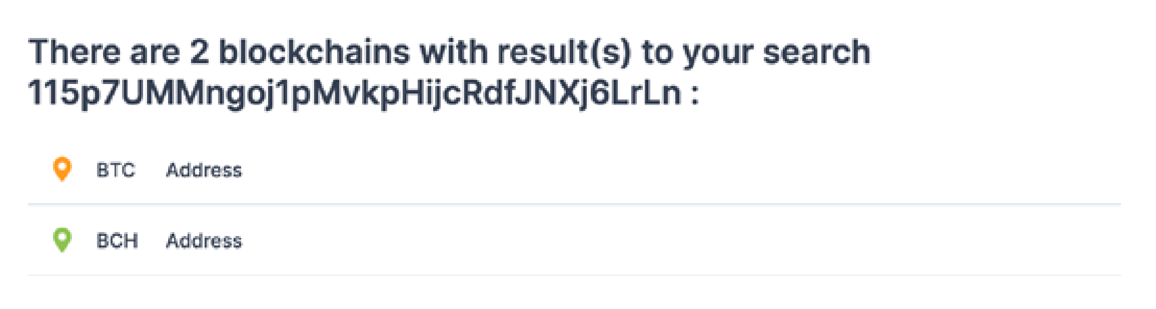
ENTITY	INCOMING TXS	OUTGOING TXS	VOLUME Rx	Volume $	VOLUME SENT	BALANCE ($)	Balance $
AGORA MARKET	9,27,433	2,18,801	7,15,297.00	35,76,48,49,969	-715,190.50107668 Ƀ	106.4983113	53,24,916
BLACK BANK MARKET	54,569	24,678	40,214.14	2,01,07,07,221	-40,210.70776257 Ƀ	3.43666386	1,71,833
BLUE SKY MARKETPLACE	39,657	20,116	11,841.62	59,20,81,037	-11,838.67577739 Ƀ	2.94496109	1,47,248
CANNABIS ROAD	8,182	4,033	1,672.78	8,36,38,998	-1,672.74260709 Ƀ	0.03734735	1,867
EVOLUTION MARKET	79,804	4,102	17,344.38	86,72,19,106	-17,326.10993625 Ƀ	18.27218345	9,13,609
HYDRA MARKET	75,22,150	6,91,254	4,73,121.74	23,65,60,87,090	-472,530.60143079 Ƀ	591.1403707	2,95,57,019
MIDDLE EARTH MARKETPLACE	1,06,675	36,178	1,62,745.85	8,13,72,92,323	-162,745.84315319 Ƀ	0.00330245	165
PANDORA OPENMARKET	77,869	30,910	22,879.23	1,14,39,61,730	-	0	-
SHEEP MARKETPLACE	66,539	21,462	65,255.79	3,26,27,89,548	-65,236.11638139 Ƀ	19.67457546	9,83,729
SILK ROAD	7,92,534	1,63,762	58,74,694.75	2,93,73,47,37,324	-5,874,601.98756129 Ƀ	92.75891157	46,37,946
SILK ROAD 2	5,09,394	1,50,800	2,02,029.08	10,10,14,53,953	-201,850.35427714 Ƀ	178.7247887	89,36,239


الإعلام العسكري
www.alqassam.net
الرد الأمثل على المطبعين هو بتجريم الاحتلال
ودعم المقاومة بشتى الوسائل وفي مقدمتها
الدعم المالي..
عبر عنوان المحفظة الرسمي والوحيد
17QAWGVpFV4gZ25NQug46e5m8ho4uDP6MD
التقط بهاتفك
#التطبيع_خيانة


AL SADAQAH
SUPPORTING THE MUJAHIDIN IN SYRIA WITH
WEAPONS, FINANCIAL AID AND OTHER
PROJECTS ASSISTING THE JIHAD.
دعم المجاهدين في سوريا بالأسلحة والمساعدات المالية
وغيرها من المشاريع التي تدعم الجهاد
Donate safely and securely with Bitcoin
تبرع بأمان وبشكل آمن مع بتكوين
bitcoin
15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf
@alsadaqahsyria
+963 935 746 232
Donate anonymously with Cryptocurrency

Moving into Crypto : ISIS & Al-Qassam Brigade.

Bitcoin Tracking: Examples.



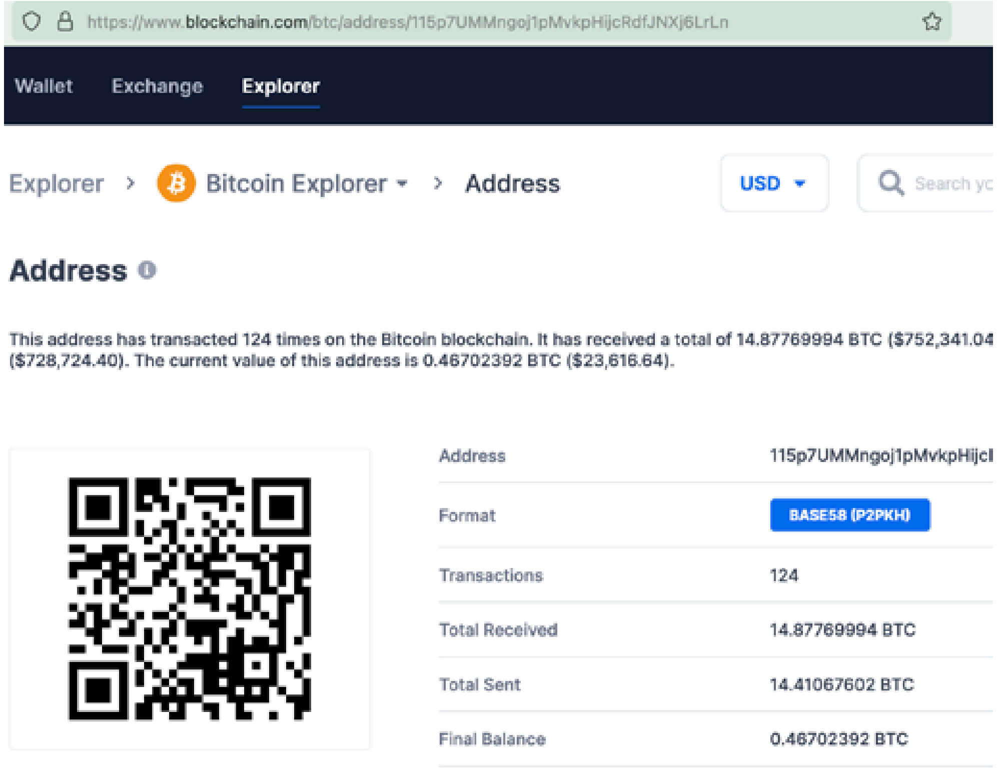
There are 2 blockchains with result(s) to your search 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn :

BTC	Address
BCH	Address

Wallet can be on one more blockchains.

Bitcoin Explorer.

Not very friendly for analysis and investigators.



https://www.blockchain.com/btc/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

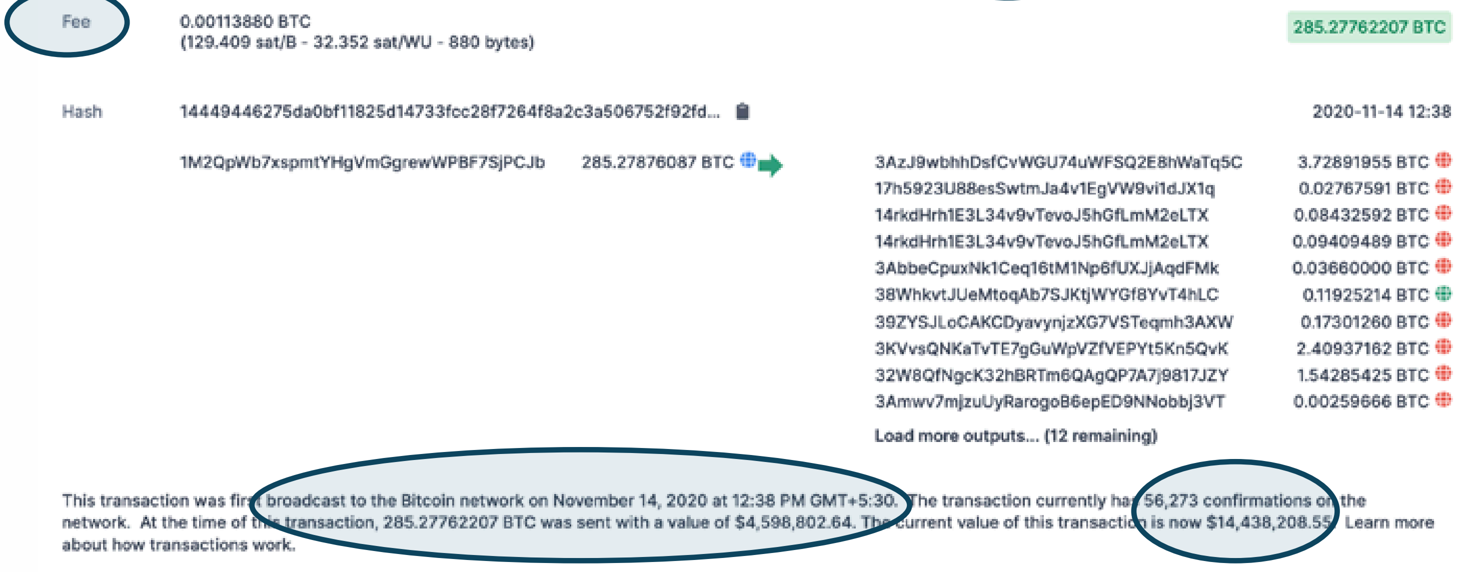
Address

This address has transacted 124 times on the Bitcoin blockchain. It has received a total of 14.87769994 BTC ($752,341.04 ($728,724.40). The current value of this address is 0.46702392 BTC ($23,616.64).

Address	115p7UMMngoj1pMvkpHijcl
Format	BASE58 (P2PKH)
Transactions	124
Total Received	14.87769994 BTC
Total Sent	14.41067602 BTC
Final Balance	0.46702392 BTC

Examine one:

Money Moved out from Wallet to others.



Fee 0.00113880 BTC
(129.409 sat/B - 32.352 sat/WU - 880 bytes)

285.27762207 BTC

Hash 14449446275da0bf11825d14733fcc28f7264f8a2c3a506752f92fd...

2020-11-14 12:38

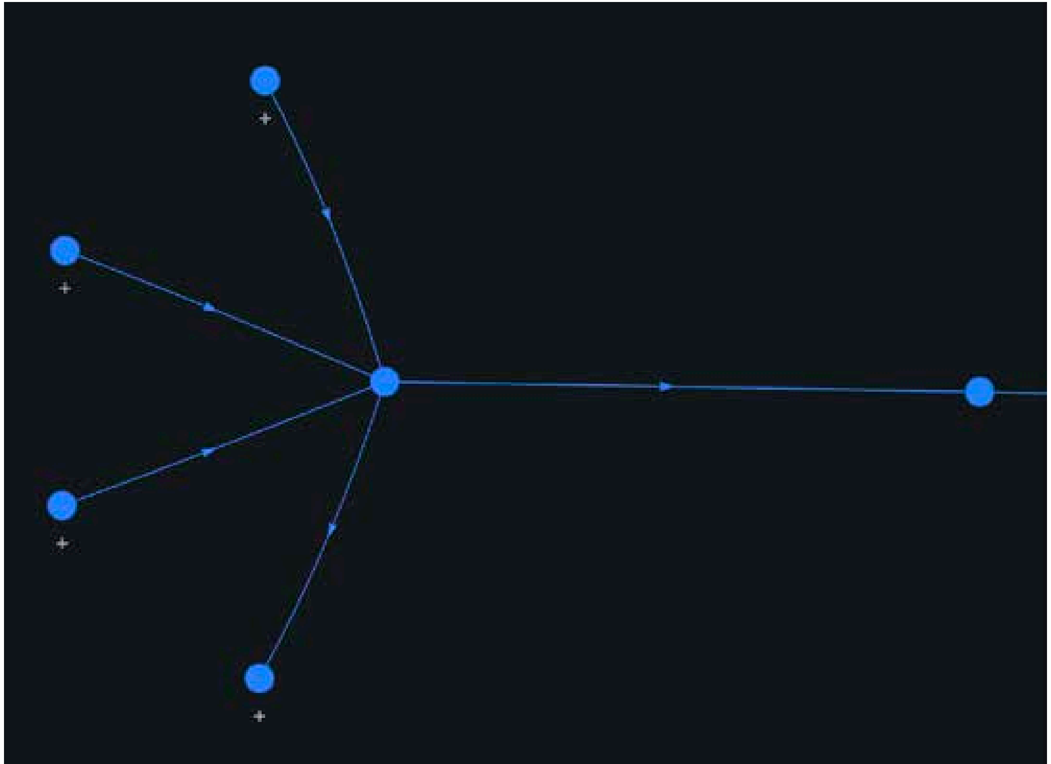
1M2QpWb7xspmtYHgVmGgrewWPBF7SjPCJb 285.27876087 BTC

3AzJ9wbhhDsfCvWGU74uWFSQ2E8hWaTq5C	3.72891955 BTC
17h5923U88esSwtmJa4v1EgVW9vi1dJX1q	0.02767591 BTC
14rkdHrh1E3L34v9vTevoJ5hGfLmM2eLTX	0.08432592 BTC
14rkdHrh1E3L34v9vTevoJ5hGfLmM2eLTX	0.09409489 BTC
3AbbeCpuxNk1Ceq16tM1Np6fUXJjAqdFMk	0.03660000 BTC
38WhkvtJUeMtoqAb7SJKtjWYGf8YvT4hLC	0.11925214 BTC
39ZYSJLoCAKCDyavynjzXG7VSTeqmh3AXW	0.17301260 BTC
3KVvsQNKaTvTE7gGuWpVZfVEPYt5Kn5QvK	2.40937162 BTC
32W8QfNgcK32hBRTm6QAgQP7A7j9817JZY	1.54285425 BTC
3Amwv7mjzuUyRarogoB6epED9NNobbj3VT	0.00259666 BTC

Load more outputs... (12 remaining)

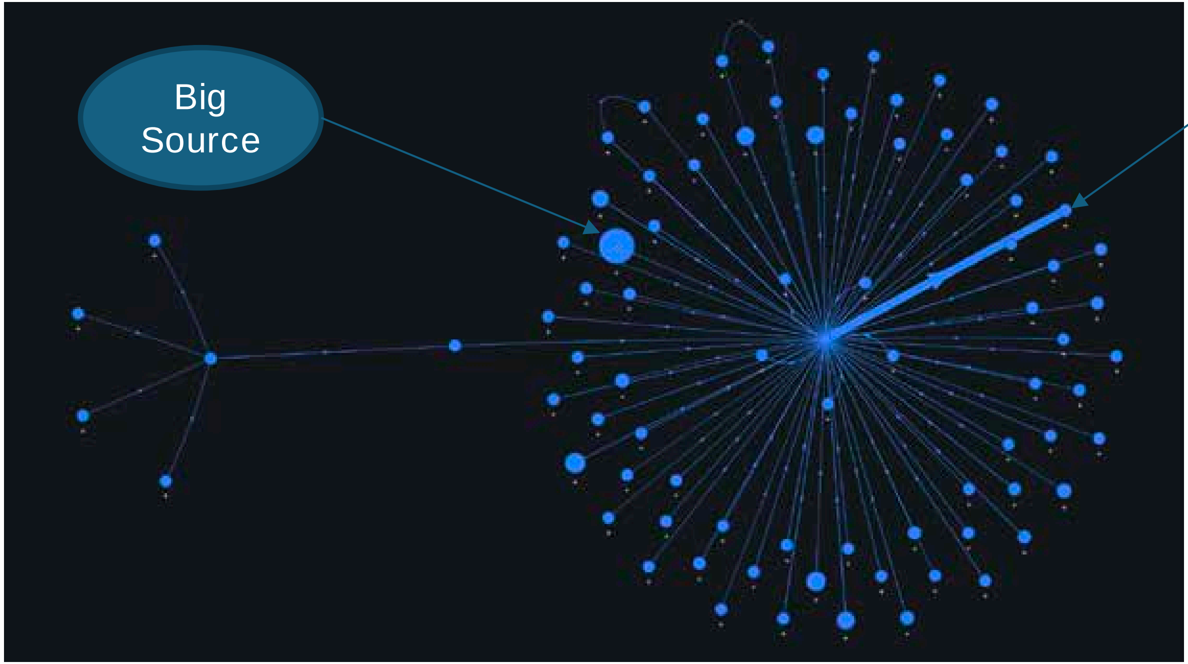
This transaction was first broadcast to the Bitcoin network on November 14, 2020 at 12:38 PM GMT+5:30. The transaction currently has 56,273 confirmations on the network. At the time of this transaction, 285.27762207 BTC was sent with a value of $4,598,802.64. The current value of this transaction is now $14,438,208.55. Learn more about how transactions work.

Bitcoin Tracking: Examples.



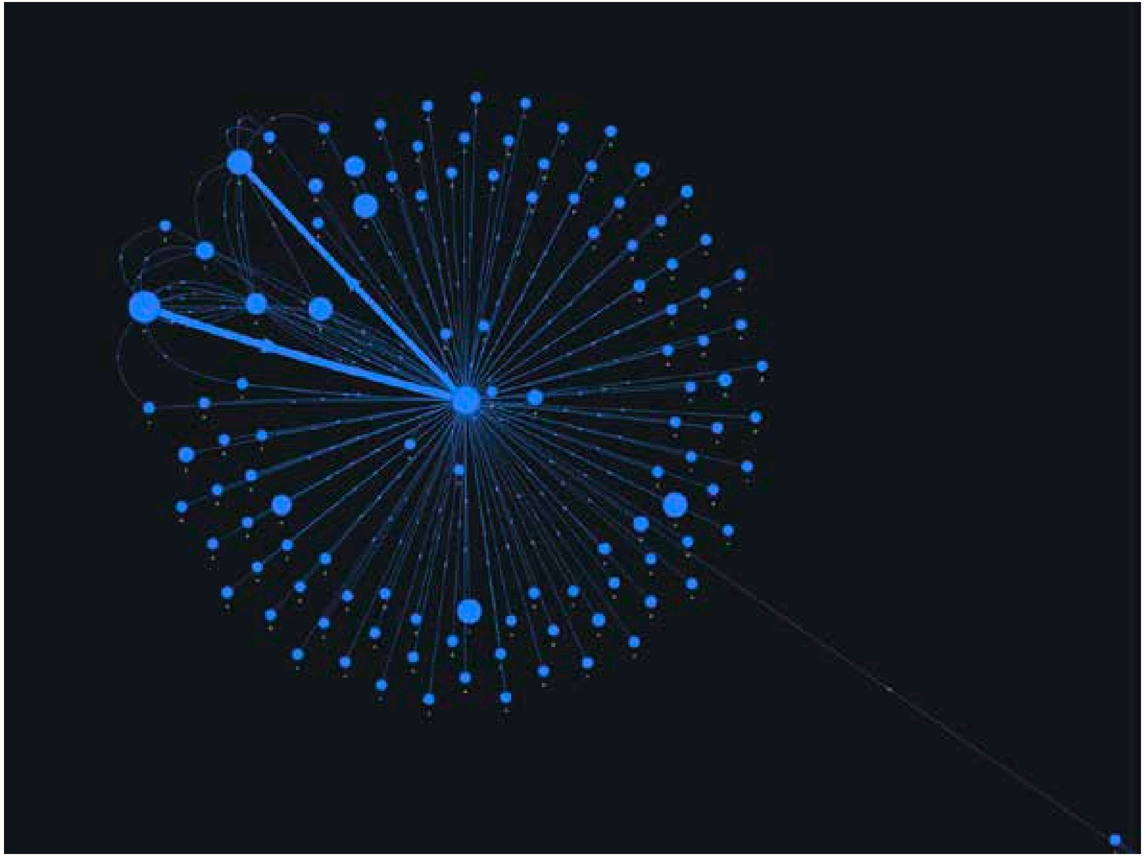
Oxt.me visualization tool.

Bitcoin Tracking: Wannacry.



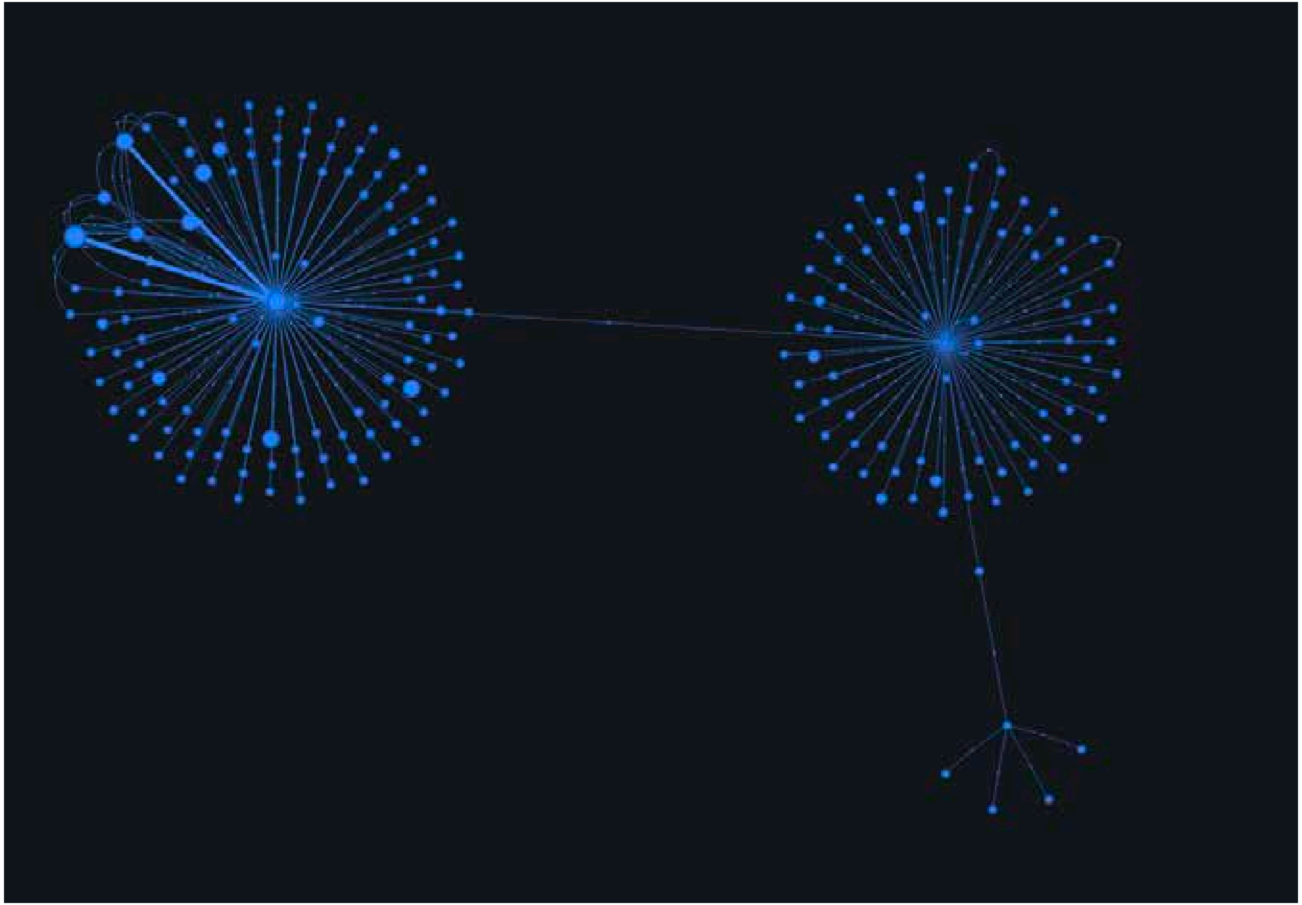
Big Source

Big Transfer



Big Source: Analysis

- Rotation between two more wallets.
- Accumulation and transfer.



We discovered many more transactions connected with the group from this one lead.

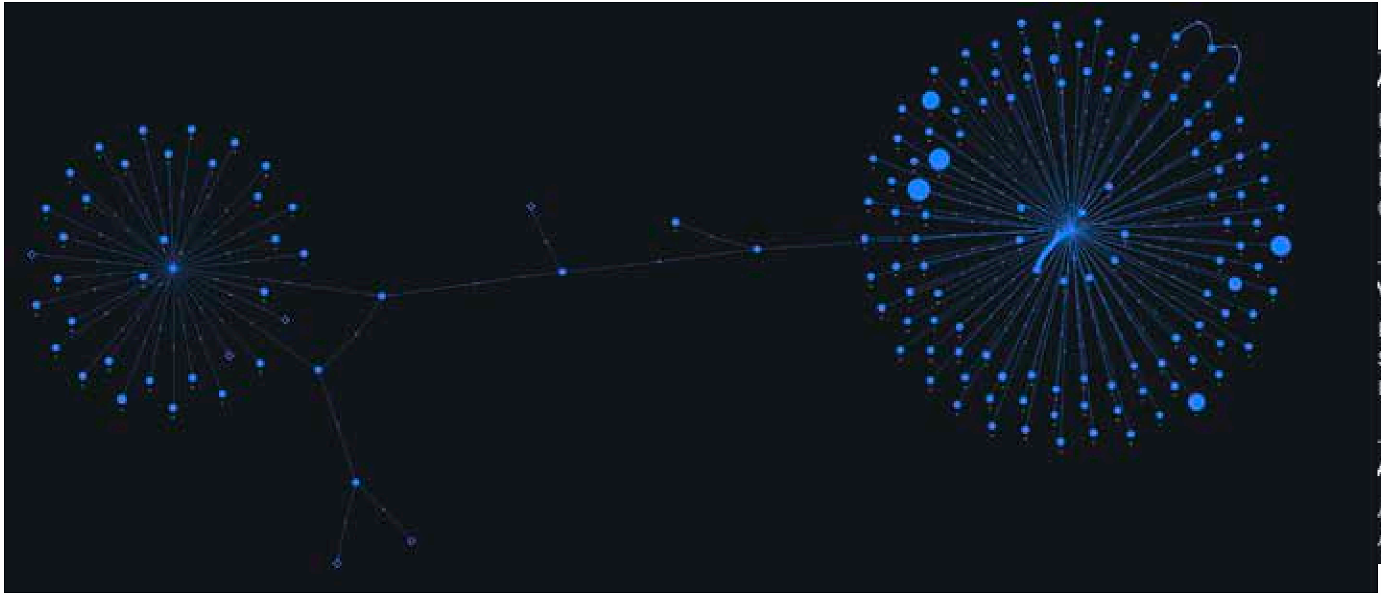
Summary of Wannacry.

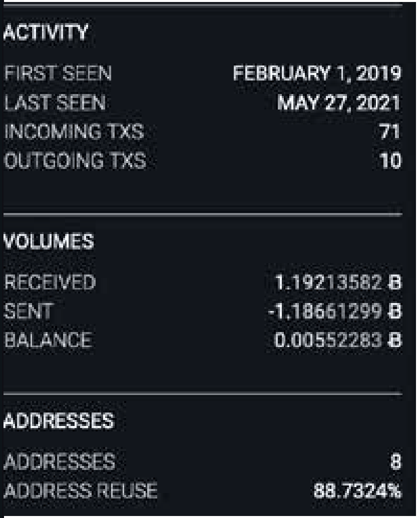
ADDRESS	INCOMING TXS	OUTGOING TXS	VOLUME RECEIVED	VOLUME SENT	BALANCE	ACTIVE TILL
13JfxwBKfL8VcXgjEuVFKRjh44EvL3Lee4	1	1	0.03848800 Ƀ	-	0.00000000 Ƀ	476632
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn	122	2	14.87769994 Ƀ	-14.41067602 Ƀ	0.46702392 Ƀ	656858
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	236	2	19.68879051 Ƀ	-17.77113037 Ƀ	1.91766014 Ƀ	712304
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	141	2	20.07353352 Ƀ	-19.74510304 Ƀ	0.32843048 Ƀ	685156
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1	15	2	1.71956125 Ƀ	-1.54379193 Ƀ	0.17576932 Ƀ	643271
1QAc9S5EmycqjzzWDc1yiWzr9jJLC8sLiY	12	2	3.25249956 Ƀ	-	0.00000000 Ƀ	476632

Wannacry : Business Profits.

Campaign	Bitcoin	Bitcoin-USD	USD-INR
Wannacry Campaign	59.65057278 Ƀ	29,82,529	21,47,42,062
Estimated Software Dev Cost			1,50,00,000
Partner & Affiliate Cost (30%)			6,44,22,619
Profit for the Operators			13,53,19,443
Profit Margin			170%
Taxes			-

ISIS Sympathisers on BTC





ACTIVITY

FIRST SEEN	FEBRUARY 1, 2019
LAST SEEN	MAY 27, 2021
INCOMING TXS	71
OUTGOING TXS	10

VOLUMES

RECEIVED	1.19213582 Ƀ
SENT	-1.18661299 Ƀ
BALANCE	0.00552283 Ƀ

ADDRESSES

ADDRESSES	8
ADDRESS REUSE	88.7324%

Total Amounts to Rs.42,00,000/-

Blockchain Frauds.

- They are only cracked at the place of withdrawls.
- We need a robust legal framework to ensure gaps in KYC and other AML-CTF norms are plugged.

Thanks !