Update of the Cyber Threat Landscape and Its Relationship with Internet Hygiene

HACK A DAY 2

Securing identity

Kok Tin Gan

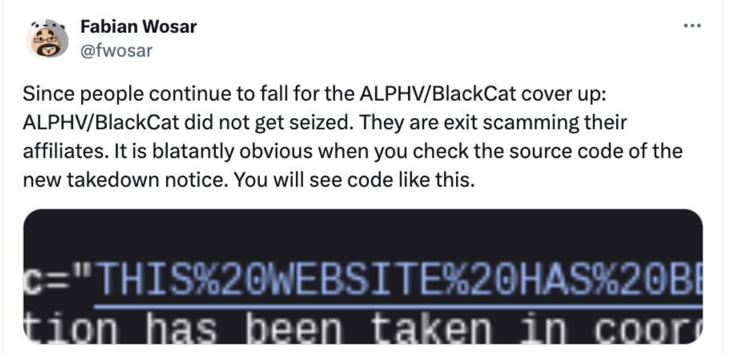
Partner, Cybersecurity and Privacy

Co-Founder of PwC Dark Lab

February 2025

pwc

The ransomware landscape was disrupted in 2024, making them unpredictable following law enforcement disruptions and exit scams

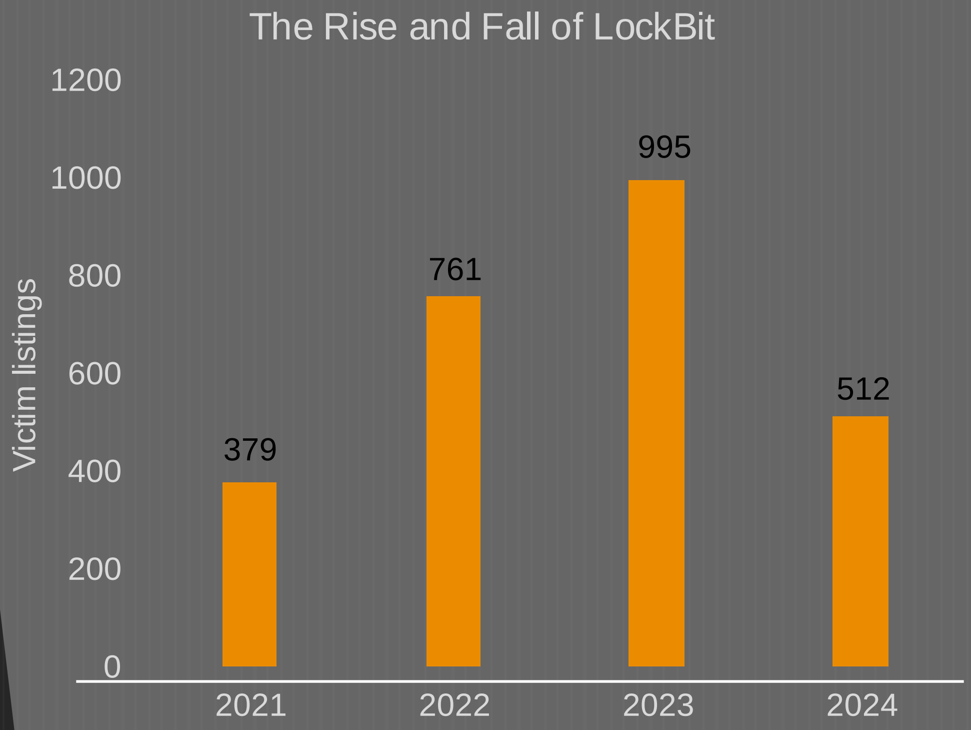


Fabian Wosar
@fwosar

Since people continue to fall for the ALPHV/BlackCat cover up: ALPHV/BlackCat did not get seized. They are exit scamming their affiliates. It is blatantly obvious when you check the source code of the new takedown notice. You will see code like this.

```
c="THIS%20WEBSITE%20HAS%20BE
tion has been taken in coor
```

Source: PwC Dark Lab, August 2021 to October 2024 Threat Intelligence Monitoring Based on Proprietary Insights, Open Source Intelligence, and Dark Web Monitoring



↑ **30%** in active ransomware threat groups

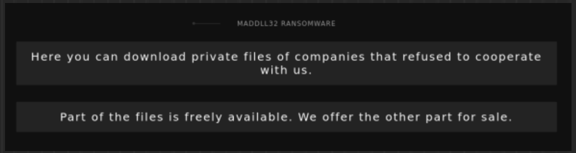
↑ **42** new dedicated leak sites in 2024

💀 **27** ransomware groups defunct in 2024

Dark Lab

February 2025

Threat actors are rapidly adapting by diversifying their tactics and exploring alternative means to increase their chances of success



MADDLL32 RANSOMWARE

Here you can download private files of companies that refused to cooperate with us.

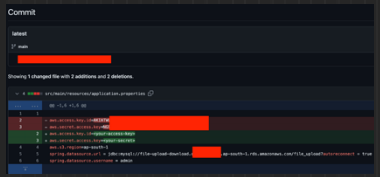
Part of the files is freely available. We offer the other part for sale.

Skip the encryption; it's all about data theft

Single extortion returns with direct sale of victim's data on leak sites

Adoption of Generative AI in social engineering

Accelerate creation of highly convincing deepfake and phishing campaigns



Commit

latest

main

[redacted]

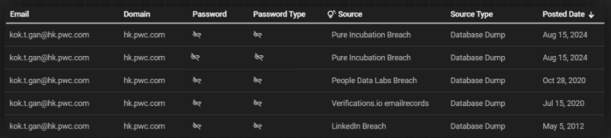
Showing 1 changed file with 2 additions and 2 deletions.

```
4 src/main/resources/application.properties
@@ -1,6 +1,6 @@

- aws.access.key.id=[redacted]
- aws.secret.access.key=
+ aws.access.key.id=<your-access-key>
+ aws.secret.access.key=<your-secret>
  aws.s3.region=ap-south-1
  spring.datasource.url = jdbc:mysql://file-upload-download.[redacted].ap-south-1.rds.amazonaws.com/file_upload?autoreconnect = true
  spring.datasource.username = admin
```

Increased targeting of cloud and SaaS credentials

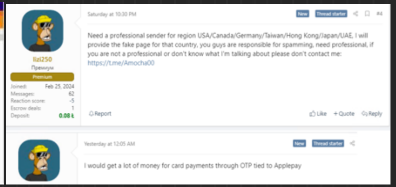
Targeting exposed configuration files with secrets and API keys



Email	Domain	Password	Password Type	Source	Source Type	Posted Date ↓
kok.t.gan@hk.pwc.com	hk.pwc.com			Pure Incubation Breach	Database Dump	Aug 15, 2024
kok.t.gan@hk.pwc.com	hk.pwc.com			Pure Incubation Breach	Database Dump	Aug 15, 2024
kok.t.gan@hk.pwc.com	hk.pwc.com			People Data Labs Breach	Database Dump	Oct 28, 2020
kok.t.gan@hk.pwc.com	hk.pwc.com			Verifications.io emailrecords	Database Dump	Jul 15, 2020
kok.t.gan@hk.pwc.com	hk.pwc.com			LinkedIn Breach	Database Dump	May 5, 2012

Significant increase in data sales

Specifically leaked credentials that extend beyond the victim to their third parties



lizi250

Премиум

Premium

Joined: Feb 25, 2024

Messages: 62

Reaction score: -5

Escrow deals: 1

Deposit: 0.08 Ł

Saturday at 10:30 PM

New Thread starter #4

Need a professional sender for region USA/Canada/Germany/Taiwan/Hong Kong/Japan/UAE, I will provide the fake page for that country, you guys are responsible for spamming, need professional, if you are not a professional or don't know what I'm talking about please don't contact me: https://t.me/Amocha00

Report Like Quote Reply

Yesterday at 12:05 AM

New Thread starter

I would get a lot of money for card payments through OTP tied to Applepay

Increase in fake SMS impersonation

Going beyond PII and credit data, and looking to steal valid credentials, sessions, and victim's metadata

Source: PwC Dark Lab, Threat Intelligence Monitoring Based on Proprietary Insights, Open Source Intelligence, and Dark Web Monitoring

Dark Lab

February 2025

whoami

- Founder
- Dark Lab
- Hack A Day
- Malaysian
- Father of 2
- Wine Lover

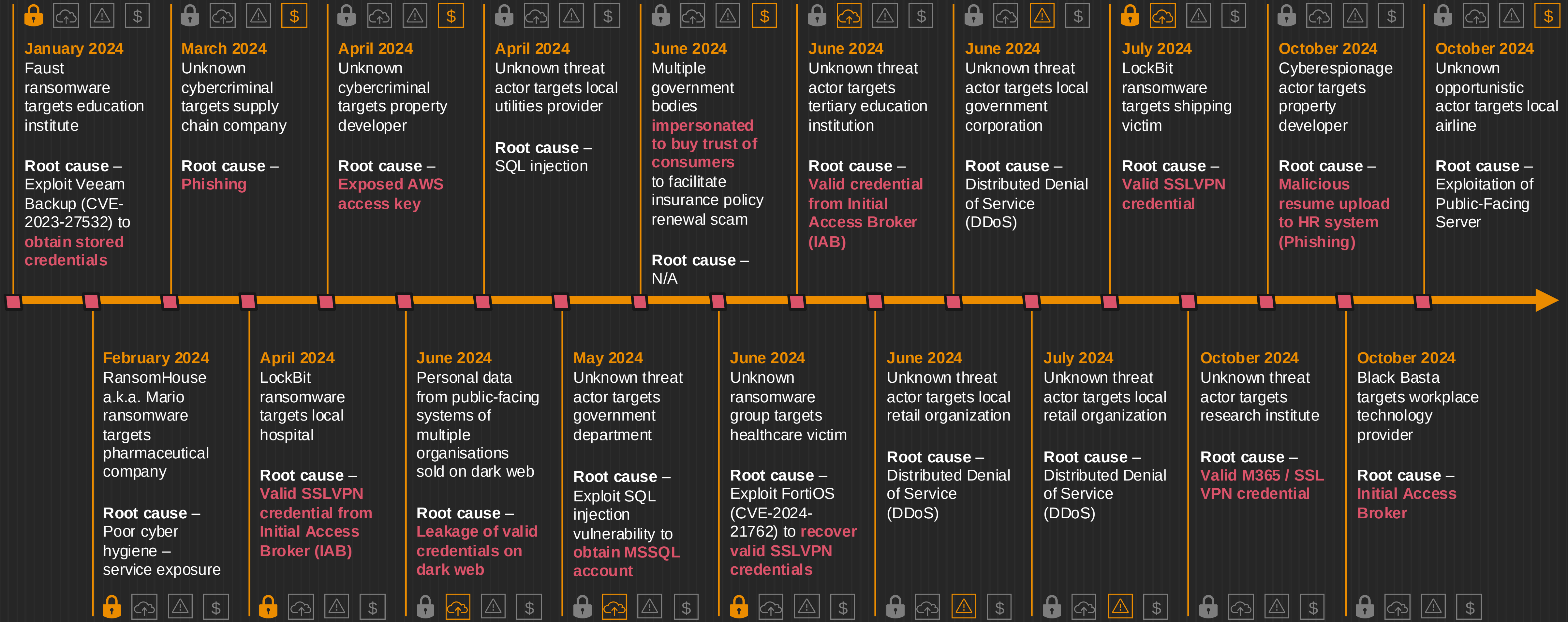
This leads to today's million-dollar question How should we define and protect 'Identity'?

" **Identity** refers to an **attribute** or set of attributes that **uniquely describes a user** "

Dark Lab

February 2025

2024 Cyber Threats Overview with Identity as a twist



[✓ 🔒] ☁ ⚠ $
January 2024
Faust ransomware targets education institute

Root cause – Exploit Veeam Backup (CVE-2023-27532) to **obtain stored credentials**

February 2024
RansomHouse a.k.a. Mario ransomware targets pharmaceutical company

Root cause – Poor cyber hygiene – service exposure
[✓ 🔒] ☁ ⚠ $

🔒 ☁ ⚠ [✓ $]
March 2024
Unknown cybercriminal targets supply chain company

Root cause – **Phishing**

April 2024
LockBit ransomware targets local hospital

Root cause – **Valid SSLVPN credential from Initial Access Broker (IAB)**
[✓ 🔒] ☁ ⚠ $

🔒 ☁ ⚠ [✓ $]
April 2024
Unknown cybercriminal targets property developer

Root cause – **Exposed AWS access key**

June 2024
Personal data from public-facing systems of multiple organisations sold on dark web

Root cause – **Leakage of valid credentials on dark web**
🔒 [✓ ☁] ⚠ $

🔒 ☁ ⚠ $
April 2024
Unknown threat actor targets local utilities provider

Root cause – SQL injection

May 2024
Unknown threat actor targets government department

Root cause – Exploit SQL injection vulnerability to **obtain MSSQL account**
🔒 [✓ ☁] ⚠ $

🔒 ☁ ⚠ [✓ $]
June 2024
Multiple government bodies **impersonated to buy trust of consumers** to facilitate insurance policy renewal scam

Root cause – N/A

June 2024
Unknown ransomware group targets healthcare victim

Root cause – Exploit FortiOS (CVE-2024-21762) to **recover valid SSLVPN credentials**
[✓ 🔒] ☁ ⚠ $

🔒 [✓ ☁] ⚠ $
June 2024
Unknown threat actor targets tertiary education institution

Root cause – **Valid credential from Initial Access Broker (IAB)**

June 2024
Unknown threat actor targets local retail organization

Root cause – Distributed Denial of Service (DDoS)
🔒 ☁ [✓ ⚠] $

🔒 ☁ [✓ ⚠] $
June 2024
Unknown threat actor targets local government corporation

Root cause – Distributed Denial of Service (DDoS)

July 2024
Unknown threat actor targets local retail organization

Root cause – Distributed Denial of Service (DDoS)
🔒 ☁ [✓ ⚠] $

[✓ 🔒] [✓ ☁] ⚠ $
July 2024
LockBit ransomware targets shipping victim

Root cause – **Valid SSLVPN credential**

October 2024
Unknown threat actor targets research institute

Root cause – **Valid M365 / SSL VPN credential**
🔒 ☁ ⚠ $

🔒 ☁ ⚠ $
October 2024
Cyberespionage actor targets property developer

Root cause – **Malicious resume upload to HR system (Phishing)**

October 2024
Black Basta targets workplace technology provider

Root cause – **Initial Access Broker**
🔒 ☁ ⚠ $

🔒 ☁ ⚠ [✓ $]
October 2024
Unknown opportunistic actor targets local airline

Root cause – Exploitation of Public-Facing Server

🟥 **Impact** 🔒 Ransomware ☁ Data Exfiltration ⚠ Denial of Service $ Monetary Loss

Dark Lab

February 2025

Summary of Lessons Learnt

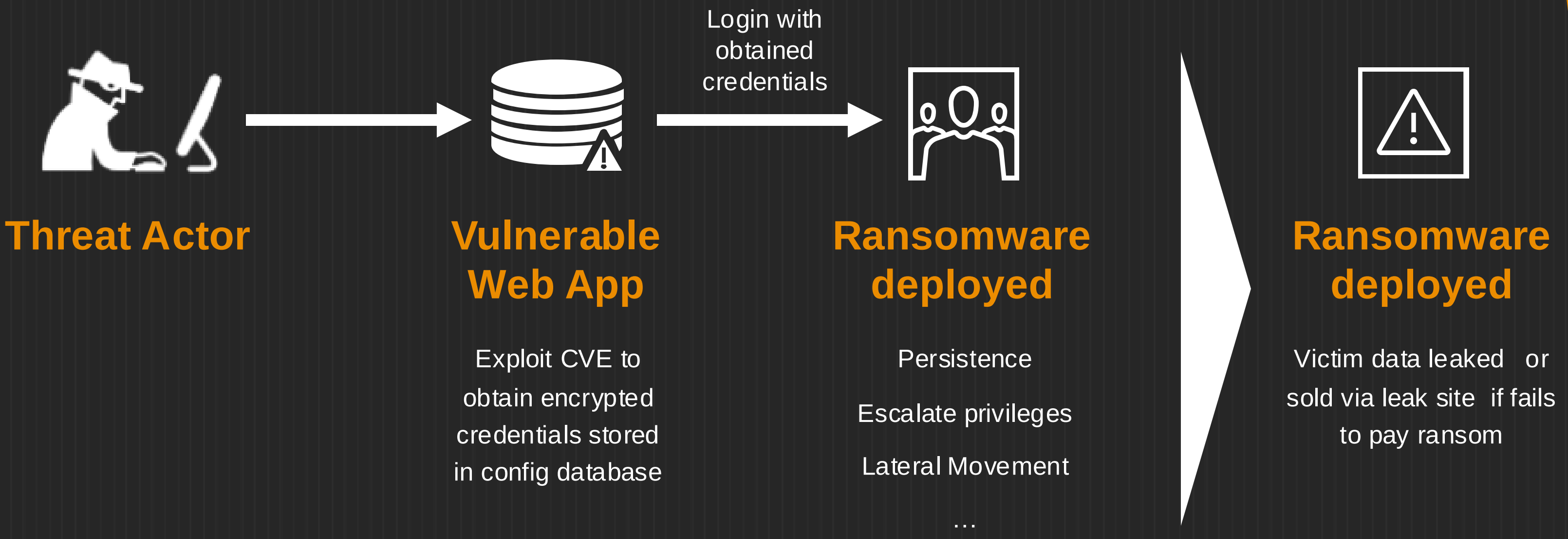
Threat actors are more intentional and resourceful in their attacks, focusing on abusing valid identities to bypass defenses

Weaponisation of CVEs is **increasingly targeted at compromising identity and/or bypassing controls safeguarding identity**

Adaptation of leaked credentials as an attack vector against a broader attack surface such as **unintentionally exposed non-production or administrative services**

Evolution of phishing attacks to **capture valid sessions** and impersonate the victim's identity, while others **impersonate trusted brands**

Exploitation of CVEs are increasingly focused on obtaining valid identities and bypassing identity security



Login with obtained credentials

Threat Actor

Vulnerable Web App

Exploit CVE to obtain encrypted credentials stored in config database

Ransomware deployed

Persistence

Escalate privileges

Lateral Movement

…

Ransomware deployed

Victim data leaked or sold via leak site if fails to pay ransom

Source: PwC Dark Lab, 1 January 2023 to September Threat Intelligence Monitoring Based on Proprietary Insights, Open Source Intelligence

↑ 57% in exploitation of CVEs related to stealing identity

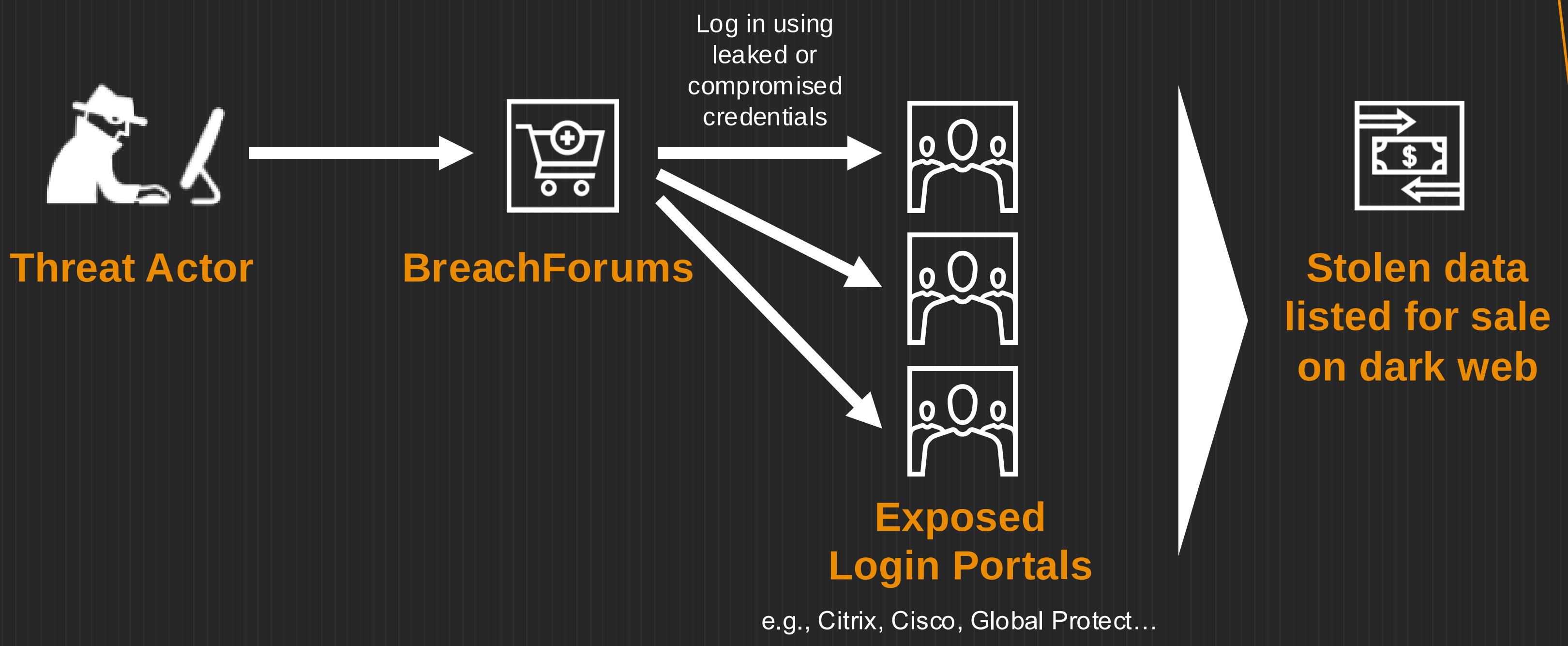
↑ 11% in exploitation of CVEs related to bypassing controls to secure identity

Most targeted technologies:

- SSLVPN
- Firewall
- Mobile Device Management
- Unintentionally exposed public cloud assets/services
- Unhardened 3rd party hosting services

Dark Lab

The cybercriminal ecosystem is increasingly intentional in their weaponization of identities


Threat Actor
BreachForums
Log in using leaked or compromised credentials
Exposed Login Portals
e.g., Citrix, Cisco, Global Protect…
Stolen data listed for sale on dark web

↑ **37%** in infostealer infections against Hong Kong

↑ **174%** in average price per access sale

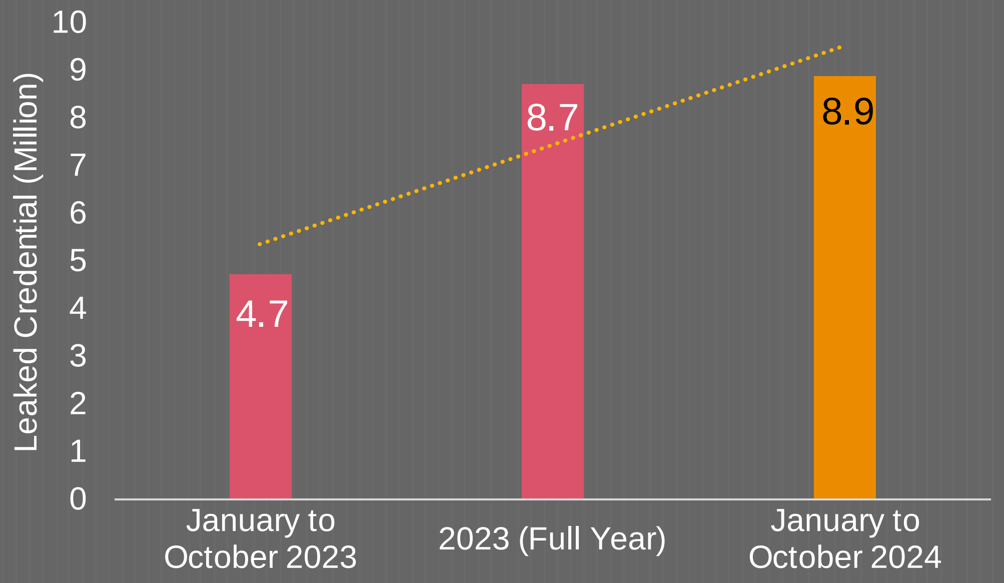
2023 **US$ 1583** 2024 **US$ 4339**

↑ **1238%** highest value listing price

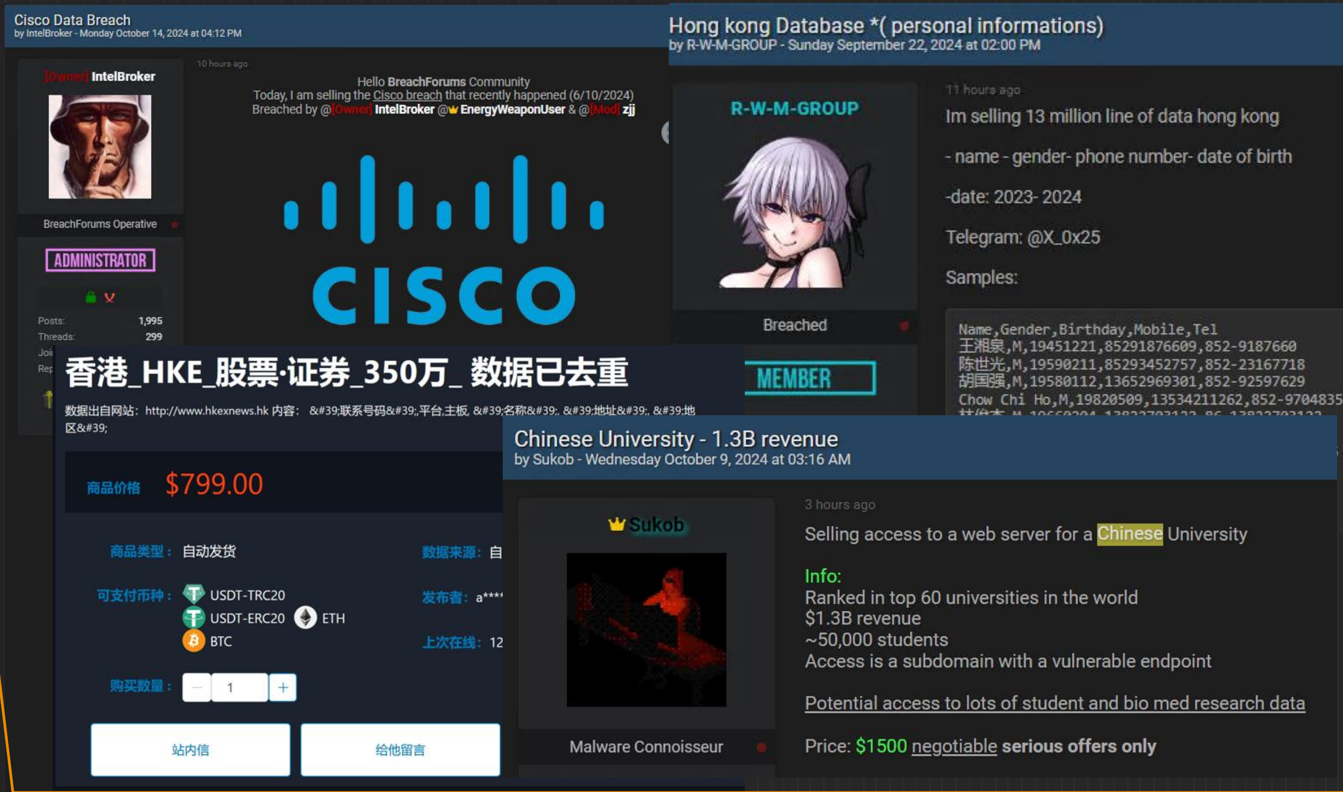
2023 **US$ 74.8K** 2024 **US$ 1 MIL**

Source: PwC Dark Lab, 1 January 2023 to 10 October 2024 Threat Intelligence Monitoring Based on Proprietary Insights, Open Source Intelligence, and Dark Web Monitoring

The macro and micro shifts in the cyber threat landscape have significantly contributed to the increase in leaked credentials on the dark web



Source: PwC Dark Lab, 1 January 2023 to 22 October 2024 Threat Intelligence Monitoring Based on Proprietary Insights, Open Source Intelligence, and Dark Web Monitoring



Cisco Data Breach
by IntelBroker - Monday October 14, 2024 at 04:12 PM

[Owner] IntelBroker

BreachForums Operative

ADMINISTRATOR

Posts: 1,995
Threads: 299

10 hours ago

Hello BreachForums Community
Today, I am selling the Cisco breach that recently happened (6/10/2024)
Breached by @[Owner] IntelBroker @ EnergyWeaponUser & @[Mod] zjj

Hong kong Database *(personal informations)
by R-W-M-GROUP - Sunday September 22, 2024 at 02:00 PM

R-W-M-GROUP

Breached

MEMBER

11 hours ago

Im selling 13 million line of data hong kong

- name - gender- phone number- date of birth

-date: 2023- 2024

Telegram: @X_0x25

Samples:

```
Name,Gender,Birthday,Mobile,Tel
王湘泉,M,19451221,85291876609,852-9187660
陈世光,M,19590211,85293452757,852-23167718
胡国强,M,19580112,13652969301,852-92597629
Chow Chi Ho,M,19820509,13534211262,852-9704835
```

香港_HKE_股票·证券_350万_ 数据已去重

数据出自网站：http://www.hkexnews.hk 内容： &#39;联系号码&#39;,平台,主板, &#39;名称&#39;, &#39;地址&#39;, &#39;地区&#39;;

商品价格 $799.00

商品类型： 自动发货

数据来源： 自

可支付币种： USDT-TRC20 USDT-ERC20 ETH BTC

发布者： a****

上次在线： 12

购买数量： 1

Chinese University - 1.3B revenue
by Sukob - Wednesday October 9, 2024 at 03:16 AM

Sukob

Malware Connoisseur

3 hours ago

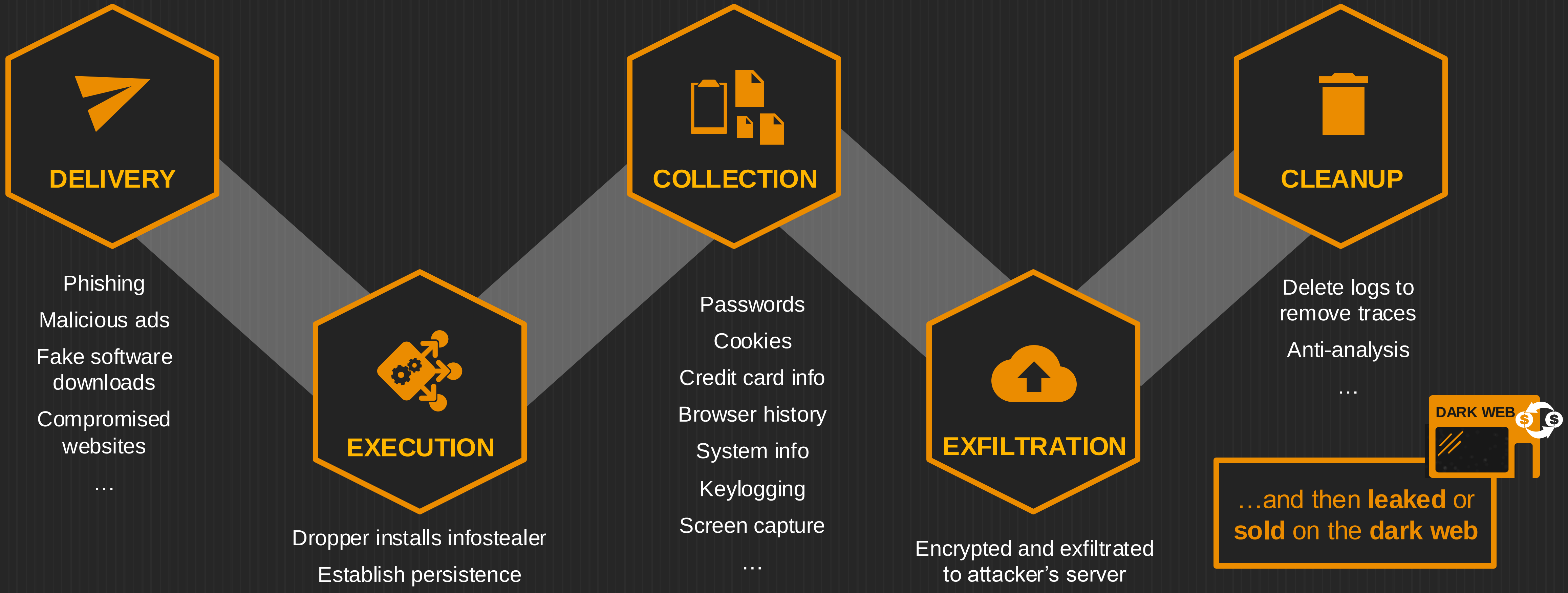
Selling access to a web server for a Chinese University

Info:
Ranked in top 60 universities in the world
$1.3B revenue
~50,000 students
Access is a subdomain with a vulnerable endpoint

Potential access to lots of student and bio med research data

Price: $1500 negotiable **serious offers only**

The use of infostealers has become more prevalent, with these tools specifically designed to harvest credentials from infected systems



DELIVERY

- Phishing
- Malicious ads
- Fake software downloads
- Compromised websites
- …

EXECUTION

- Dropper installs infostealer
- Establish persistence

COLLECTION

- Passwords
- Cookies
- Credit card info
- Browser history
- System info
- Keylogging
- Screen capture
- …

EXFILTRATION

- Encrypted and exfiltrated to attacker's server

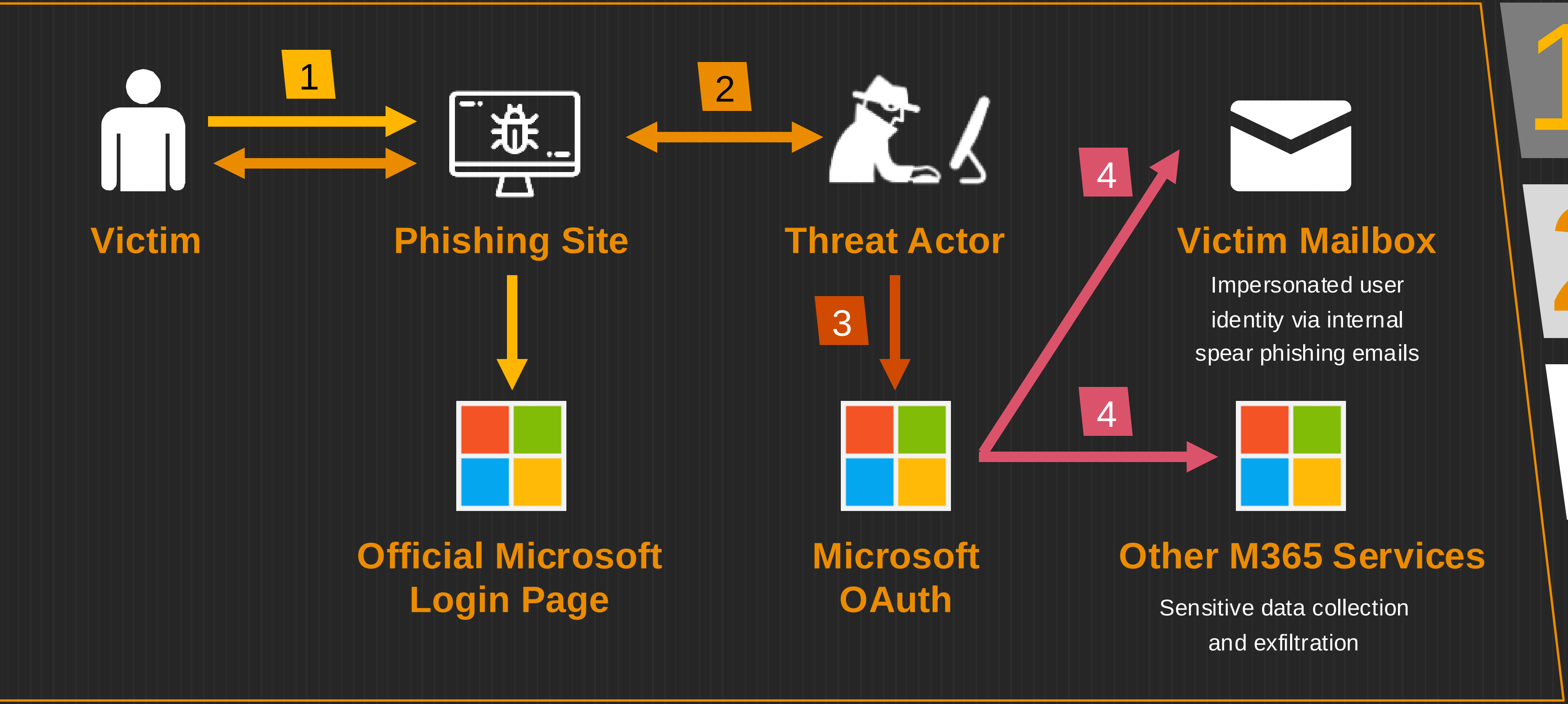
CLEANUP

- Delete logs to remove traces
- Anti-analysis
- …

…and then **leaked** or **sold** on the **dark web**

Source: PwC Dark Lab's Proprietary Insights

Adversary-in-the-Middle (AiTM) phishing campaigns persist, impersonating trusted brands



1

2

Victim

Phishing Site

Threat Actor

3

4

4

Victim Mailbox

Impersonated user identity via internal spear phishing emails

Official Microsoft Login Page

Microsoft OAuth

Other M365 Services

Sensitive data collection and exfiltration

1 Phishing Website Redirect
Victim visits phishing site and is redirected to the official M365 login page.

2 Authentication
Victim performs legitimate login with MFA on the M365 portal. Threat actor captures credentials and token.

3 Persistence
Threat actor requests Primary Refresh Token (PRT) to register own device for Single Sign-On (SSO) to M365.

4 Impact
Access and collect data from M365 services, and victim impersonation via internal spear phishing.

How can we prevent and detect these attacks? We must focus on how to protect the identity!

PREVENTION

Employ a **conditional access policy** to restrict unauthorised access

- Restrict the use of tokens only from devices on which they were issued
- Enable token protection
- Allow sign-ins only from devices that hybrid-joined to Entra ID or are managed by MDM or MAM solutions
- Require strong, multi-layered authentication methods
- Limit the session duration of Outlook on the Web (OWA) to 1 hour

DETECTION

Detect and monitor for **anomalous activity**

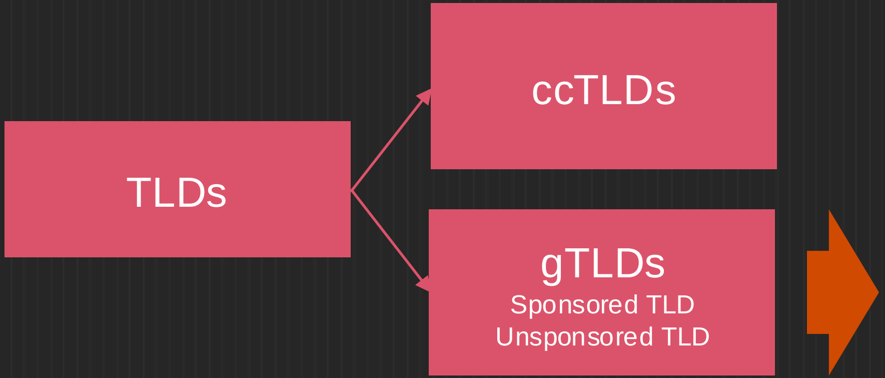
- Accesses from 2+ countries within short period in Entra ID
- Review the 'Risky' Sign-In on Entra ID
- Monitor for assignments of Temporary Access Passes on sensitive accounts
- Monitor for large numbers of users signing in "from" the same device
- Specific user events (e.g., user registered security information, started security info registration,…)

Send **device registration notifications** to users

Dark Lab

Our approach to tracking domains – how do they begin?

Domains take an important role in infrastructure used by cybercriminals and the like. Dark Lab asks the question of: how do threat actors groom their domains?



We start by tracking domains to their birth i.e. as they are registered, and follow through their lifetime. As such, we surveyed publicly-available data on generic TLDs, based on:

Raw DNS Records

Data Feeds
Newly Registered Domains

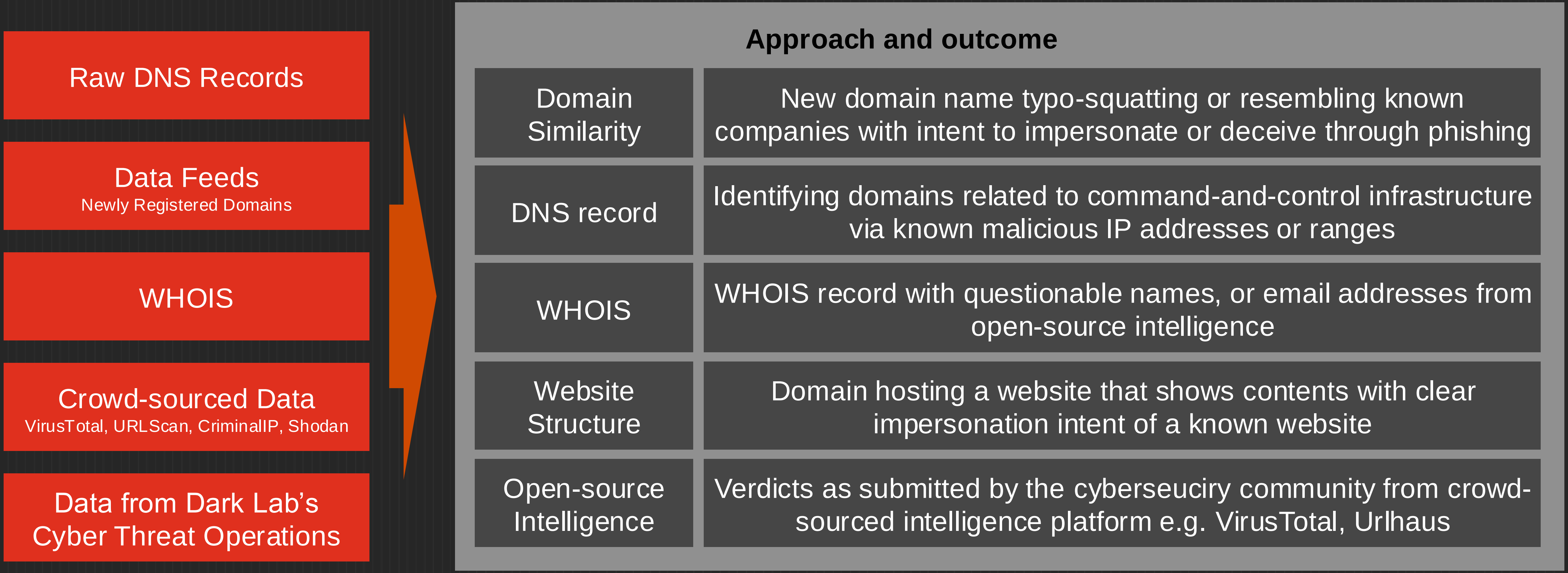
WHOIS

Crowd-sourced Data
VirusTotal, URLScan, CriminalIP, Shodan

Data from Dark Lab's Cyber Threat Operations

Our approach to tracking domains – how do they begin?

We look historically at domains that are deemed suspicious or malicious.



Raw DNS Records

Data Feeds
Newly Registered Domains

WHOIS

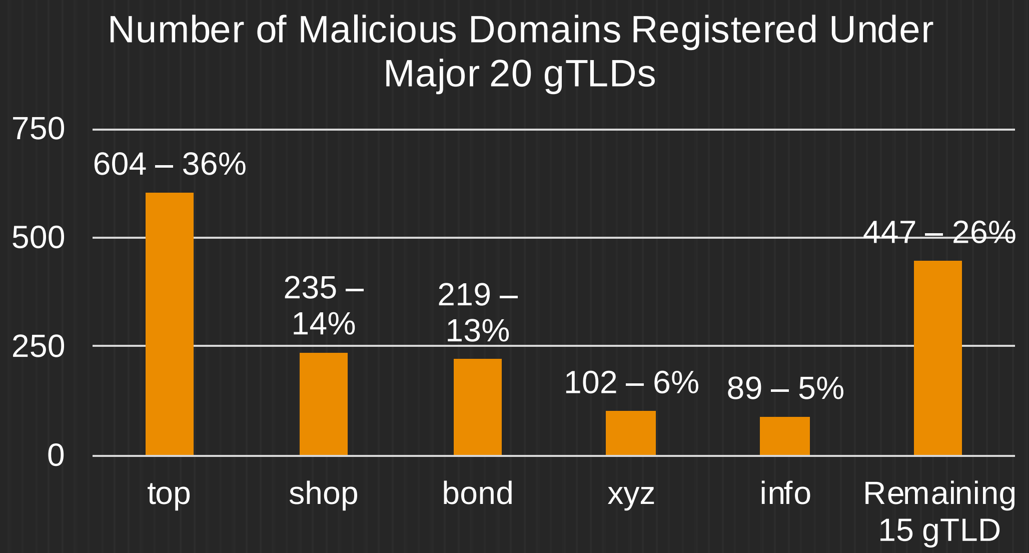
Crowd-sourced Data
VirusTotal, URLScan, CriminalIP, Shodan

Data from Dark Lab's
Cyber Threat Operations

Approach and outcome

Domain Similarity	New domain name typo-squatting or resembling known companies with intent to impersonate or deceive through phishing
DNS record	Identifying domains related to command-and-control infrastructure via known malicious IP addresses or ranges
WHOIS	WHOIS record with questionable names, or email addresses from open-source intelligence
Website Structure	Domain hosting a website that shows contents with clear impersonation intent of a known website
Open-source Intelligence	Verdicts as submitted by the cyberseuciry community from crowd-sourced intelligence platform e.g. VirusTotal, Urlhaus

What insights did we glean from our study into newly registered domains for 20 major gTLDs for a selected day in January 2025?



Source: PwC Dark Lab, January 2025 Threat Intelligence Analysis on 20 major gTLDs for one day, using Open Source Intelligence.
Remaining gTLDs include .online (87), .xin (60), .sbs (58), .click (42), .org (38), .net (38), .vip (29), .icu (24), .site (21), .cyou (18), .pro (11), .store (9), .biz (7), .club (2), and .asia (2)

Phishing

Spam

Malware

C2

APT-related activities

70,000 newly registered domains per day

2,800 of the 70,000 newly registered domains reported as malicious

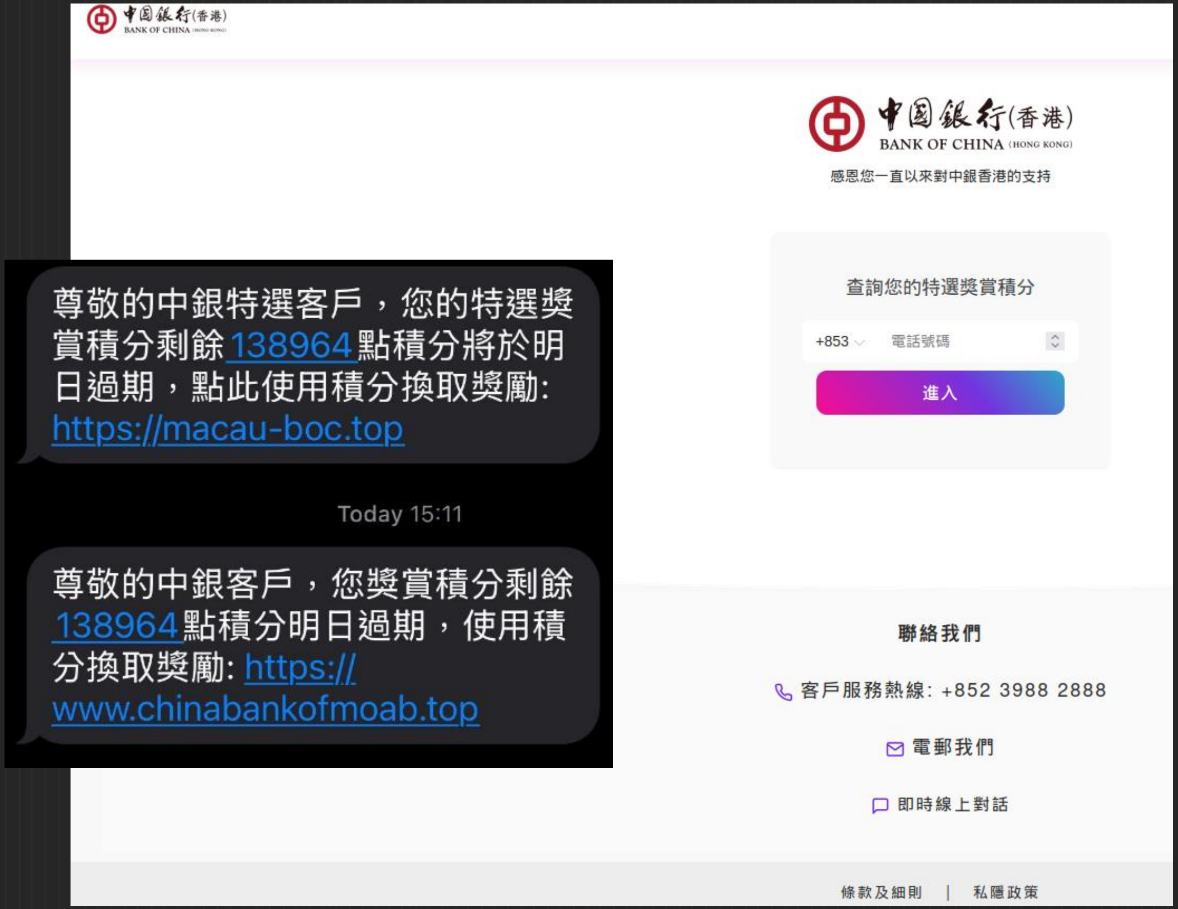
☠ **74%** of newly registered malicious comprise of the top 5 gTLDs

Dark Lab

Example of newly registered malicious domains

Phishing | Spam | Malware | C2

Newly registered domains are typically deployed in SMS to redirect and deceive victims into providing sensitive information (e.g., credentials, PII, etc.) by impersonating well-known organizations



中國銀行(香港) BANK OF CHINA (HONG KONG)

感恩您一直以來對中銀香港的支持

查詢您的特選獎賞積分

+853 電話號碼

進入

聯絡我們

客戶服務熱線: +852 3988 2888

電郵我們

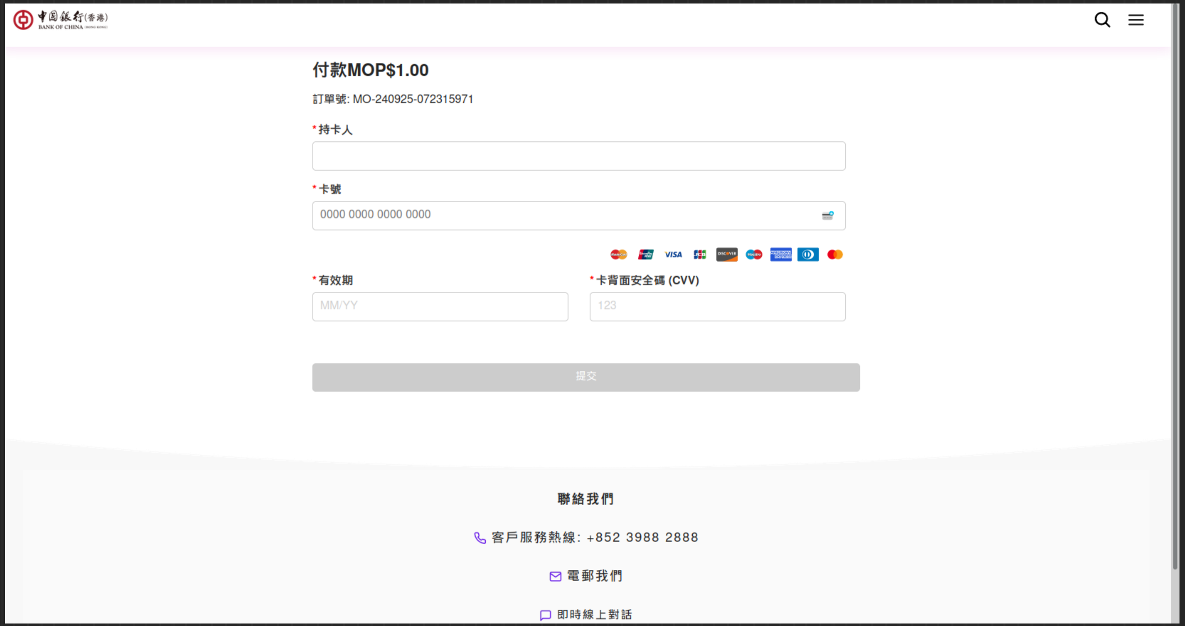
即時線上對話

條款及細則 | 私隱政策

尊敬的中銀特選客戶，您的特選獎賞積分剩餘138964點積分將於明日過期，點此使用積分換取獎勵: https://macau-boc.top

Today 15:11

尊敬的中銀客戶，您獎賞積分剩餘138964點積分明日過期，使用積分換取獎勵: https://www.chinabankofmoab.top



付款MOP$1.00

訂單號: MO-240925-072315971

*持卡人

*卡號

0000 0000 0000 0000

*有效期

MM/YY

*卡背面安全碼 (CVV)

123

提交

聯絡我們

客戶服務熱線: +852 3988 2888

電郵我們

即時線上對話

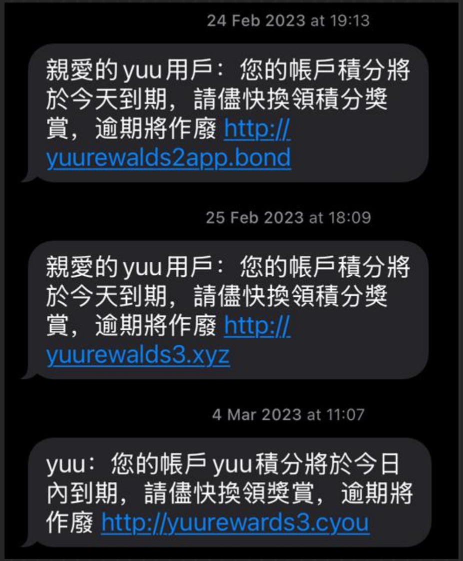
- Impersonate BOC rewards portal to target Macau and HK
- Trick victims to provide credit card info, OTP from credit card and PII, e.g., name, address email, phone number…

Dark Lab

Example of newly registered malicious domains (cont'd.)

Phishing | Spam | Malware | C2

SMS aside, newly registered domains are also used widely in emails to redirect and deceive victims into providing sensitive information (e.g., credentials, PII, etc.) by impersonating well-known organizations



24 Feb 2023 at 19:13

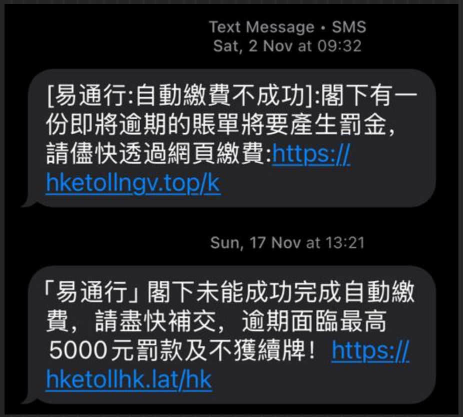
親愛的 yuu 用戶：您的帳戶積分將於今天到期，請儘快換領積分獎賞，逾期將作廢 http://yuurewalds2app.bond

25 Feb 2023 at 18:09

親愛的 yuu 用戶：您的帳戶積分將於今天到期，請儘快換領積分獎賞，逾期將作廢 http://yuurewalds3.xyz

4 Mar 2023 at 11:07

yuu：您的帳戶 yuu 積分將於今日內到期，請儘快換領獎賞，逾期將作廢 http://yuurewards3.cyou

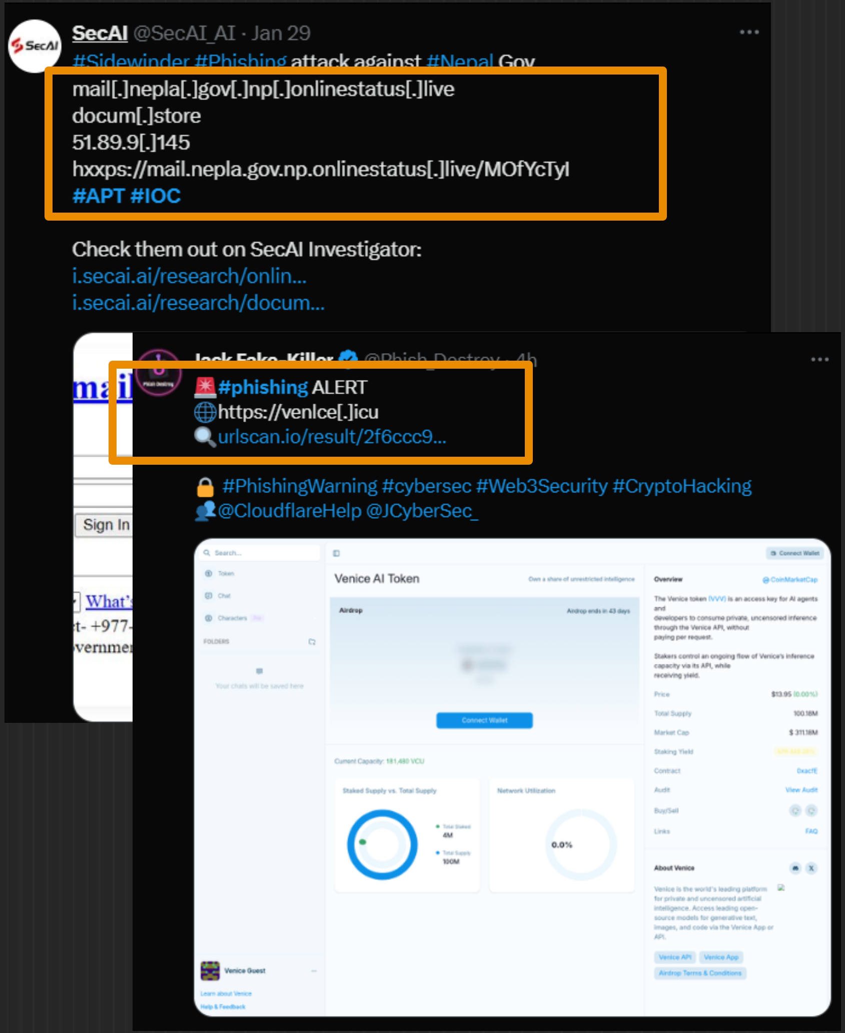


Text Message • SMS
Sat, 2 Nov at 09:32

[易通行:自動繳費不成功]:閣下有一份即將逾期的賬單將要產生罰金，請儘快透過網頁繳費:https://hketollngv.top/k

Sun, 17 Nov at 13:21

「易通行」閣下未能成功完成自動繳費，請盡快補交，逾期面臨最高5000元罰款及不獲續牌！ https://hketollhk.lat/hk



SecAI @SecAI_AI · Jan 29

#Sidewinder #Phishing attack against #Nepal Gov

mail[.]nepla[.]gov[.]np[.]onlinestatus[.]live
docum[.]store
51.89.9[.]145
hxxps://mail.nepla.gov.np.onlinestatus[.]live/MOfYcTyI
#APT #IOC

Check them out on SecAI Investigator:
i.secai.ai/research/onlin...
i.secai.ai/research/docum...

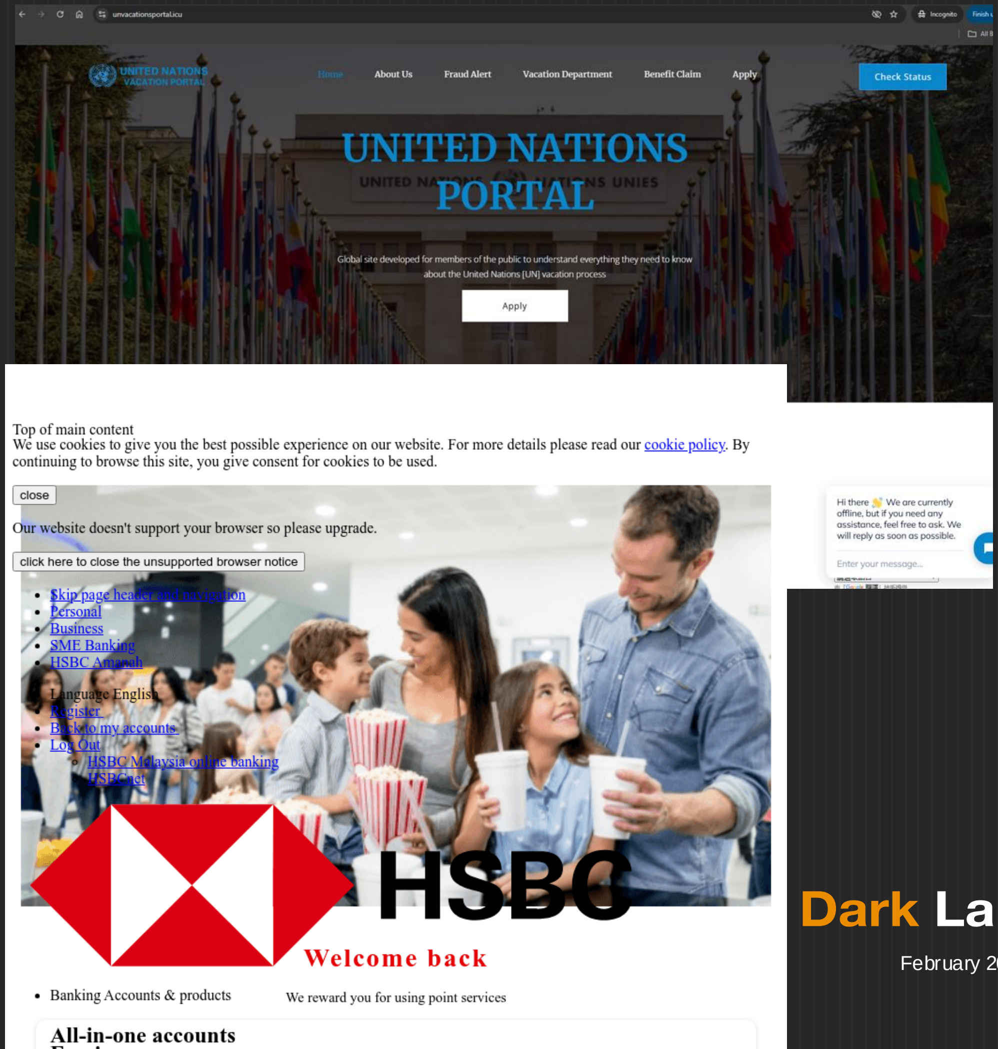
Jack Fake-Killer @Phish_Destroy · 4h

🚨#phishing ALERT
🌐https://venlce[.]icu
🔍urlscan.io/result/2f6ccc9...

🔒 #PhishingWarning #cybersec #Web3Security #CryptoHacking
👥@CloudflareHelp @JCyberSec_

The Venice token (VVV) is an access key for AI agents and developers to consume private, uncensored inference through the Venice API, without paying per request.

Stakers control an ongoing flow of Venice's inference capacity via its API, while receiving yield.



unvacationsportal.icu

Global site developed for members of the public to understand everything they need to know about the United Nations [UN] vacation process

Top of main content
We use cookies to give you the best possible experience on our website. For more details please read our cookie policy. By continuing to browse this site, you give consent for cookies to be used.

close

Our website doesn't support your browser so please upgrade.

click here to close the unsupported browser notice

- Skip page header and navigation
- Personal
- Business
- SME Banking
- HSBC Amanah
- Language English
- Register
- Back to my accounts
- Log Out
  - HSBC Malaysia online banking
  - HSBCnet

- Banking Accounts & products

We reward you for using point services

All-in-one accounts

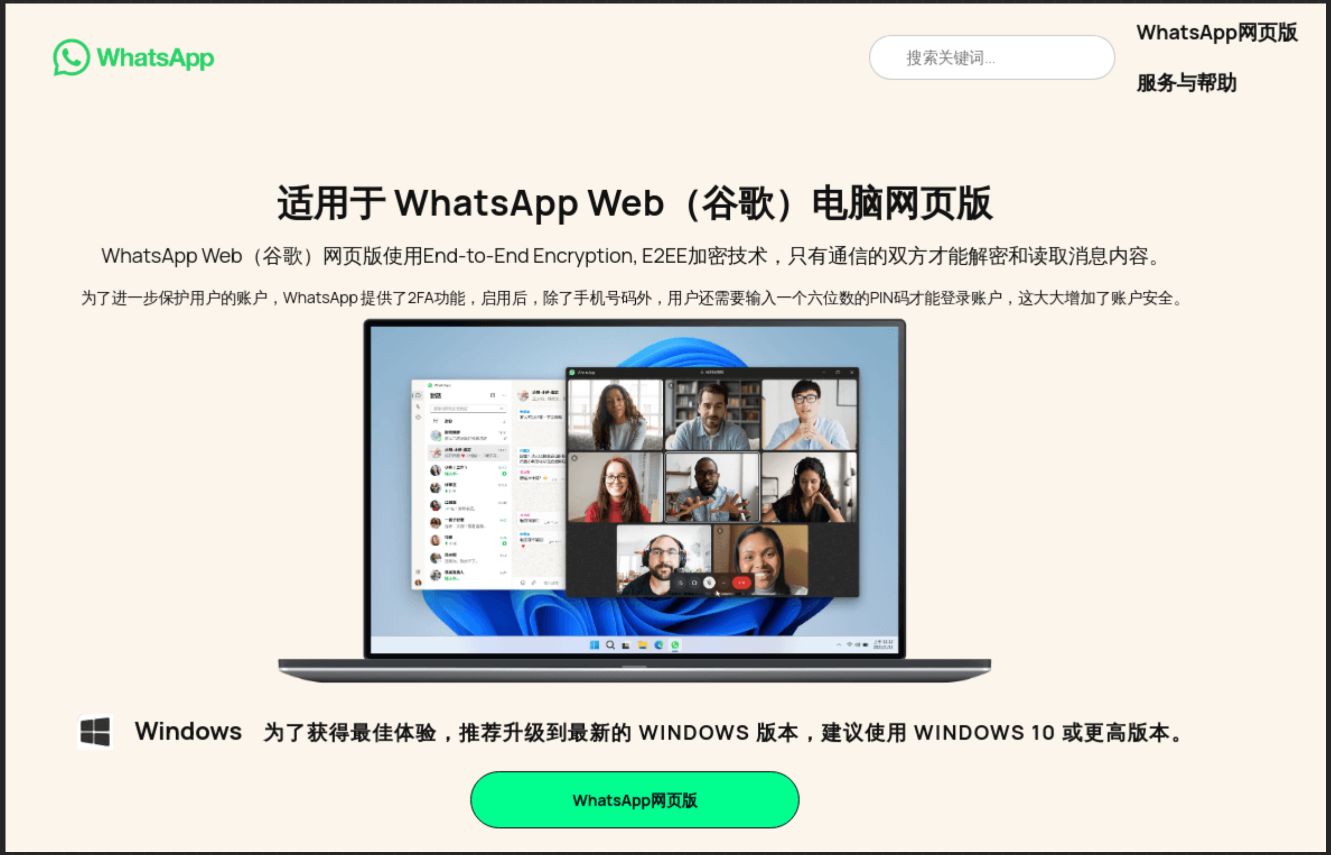
Hi there 👋 We are currently offline, but if you need any assistance, feel free to ask. We will reply as soon as possible.

Enter your message...

Example of newly registered malicious domains (cont'd.)

Phishing Spam Malware C2

Social media and instant messaging platforms have become a popular target for financial gain in recent years, facilitated by low cost to register look-alike domains



WhatsApp

搜索关键词...

WhatsApp网页版

服务与帮助

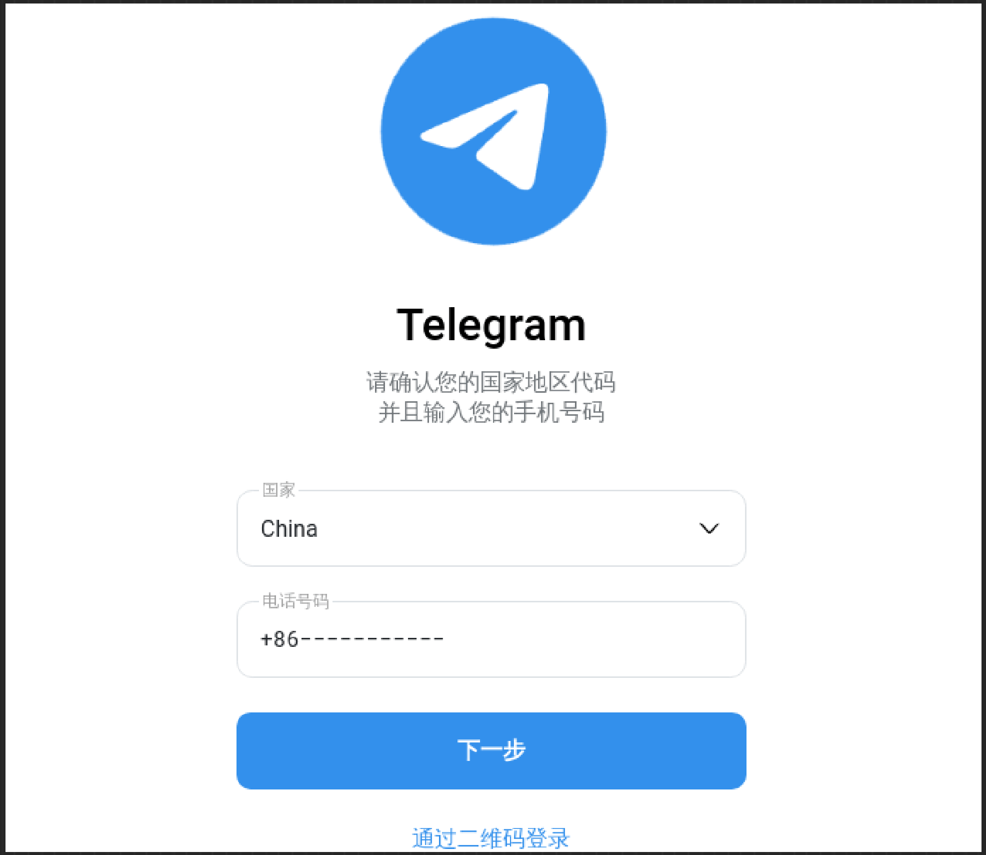
适用于 WhatsApp Web（谷歌）电脑网页版

WhatsApp Web（谷歌）网页版使用End-to-End Encryption, E2EE加密技术，只有通信的双方才能解密和读取消息内容。

为了进一步保护用户的账户，WhatsApp 提供了2FA功能，启用后，除了手机号码外，用户还需要输入一个六位数的PIN码才能登录账户，这大大增加了账户安全。

Windows 为了获得最佳体验，推荐升级到最新的 WINDOWS 版本，建议使用 WINDOWS 10 或更高版本。

WhatsApp网页版



Telegram

请确认您的国家地区代码
并且输入您的手机号码

国家

China

电话号码

+86-----------

下一步

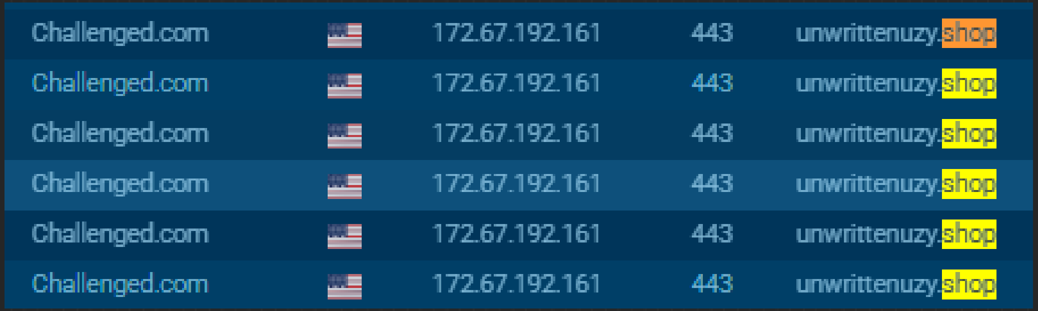
通过二维码登录

Dark Lab

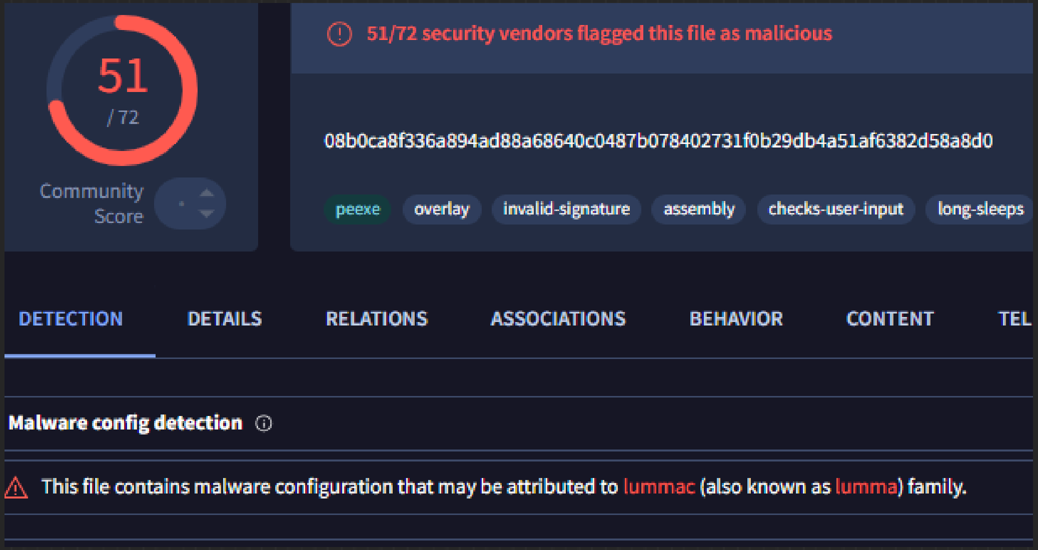
February 2025

Example of newly registered malicious domains (cont'd.)

Threat actors leveraging infostealers (e.g., Lumma) or hosting C2 often register new domains to either distribute the malware to unsuspecting users or to maintain persistence and communicate with their victim.



Challenged.com	🇺🇸	172.67.192.161	443	unwrittenuzy.shop
Challenged.com	🇺🇸	172.67.192.161	443	unwrittenuzy.shop
Challenged.com	🇺🇸	172.67.192.161	443	unwrittenuzy.shop
Challenged.com	🇺🇸	172.67.192.161	443	unwrittenuzy.shop
Challenged.com	🇺🇸	172.67.192.161	443	unwrittenuzy.shop
Challenged.com	🇺🇸	172.67.192.161	443	unwrittenuzy.shop



51 / 72

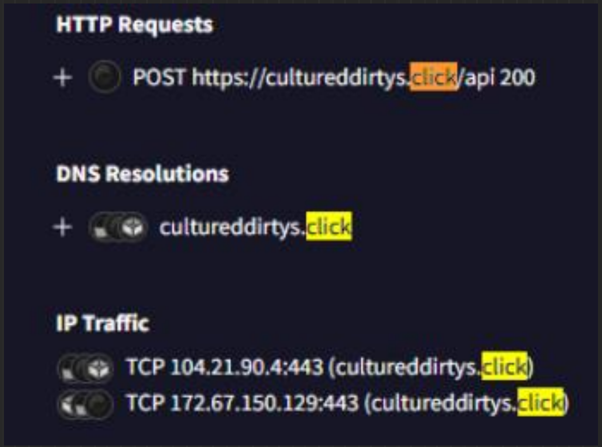
Community Score

51/72 security vendors flagged this file as malicious

08b0ca8f336a894ad88a68640c0487b078402731f0b29db4a51af6382d58a8d0

Malware config detection

⚠ This file contains malware configuration that may be attributed to lummac (also known as lumma) family.



HTTP Requests

+ POST https://cultureddirtys.click/api 200

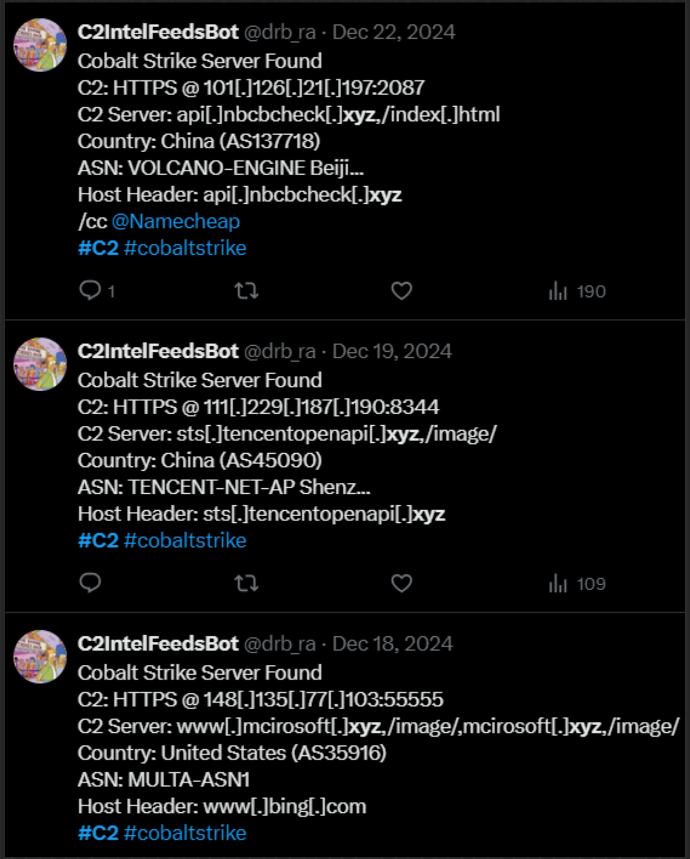
DNS Resolutions

+ cultureddirtys.click

IP Traffic

TCP 104.21.90.4:443 (cultureddirtys.click)

TCP 172.67.150.129:443 (cultureddirtys.click)



C2IntelFeedsBot @drb_ra · Dec 22, 2024

Cobalt Strike Server Found
C2: HTTPS @ 101[.]126[.]21[.]197:2087
C2 Server: api[.]nbcbcheck[.]xyz,/index[.]html
Country: China (AS137718)
ASN: VOLCANO-ENGINE Beiji...
Host Header: api[.]nbcbcheck[.]xyz
/cc @Namecheap
#C2 #cobaltstrike

C2IntelFeedsBot @drb_ra · Dec 19, 2024

Cobalt Strike Server Found
C2: HTTPS @ 111[.]229[.]187[.]190:8344
C2 Server: sts[.]tencentopenapi[.]xyz,/image/
Country: China (AS45090)
ASN: TENCENT-NET-AP Shenz...
Host Header: sts[.]tencentopenapi[.]xyz
#C2 #cobaltstrike

C2IntelFeedsBot @drb_ra · Dec 18, 2024

Cobalt Strike Server Found
C2: HTTPS @ 148[.]135[.]77[.]103:55555
C2 Server: www[.]mcirosoft[.]xyz,/image/,mcirosoft[.]xyz,/image/
Country: United States (AS35916)
ASN: MULTA-ASN1
Host Header: www[.]bing[.]com
#C2 #cobaltstrike

Why might this be happening?

Lack of Proactive Governance of gTLD

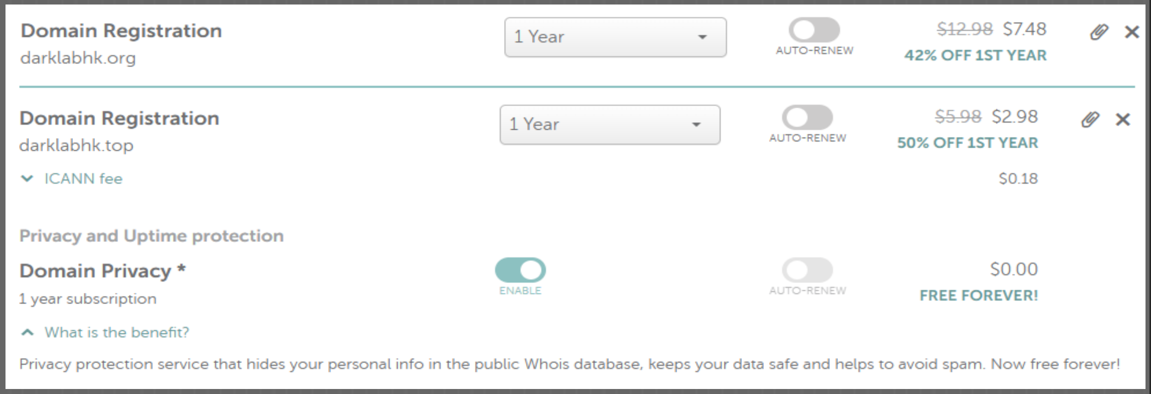
Per ICANN, registrars rely on the community’s **abuse report** to identify and takedown malicious domains

There is a lack of a **proactive, regular and measurable monitoring mechanism** to flag suspicious domains in a timely manner

This similar pain point **extends to ccTLDs (!)**

Too Simple Registration Process, Compounded by Low Cost

Very **affordable** to register domains at scale



Domain Registration
darklabhk.org
1 Year
AUTO-RENEW
~~$12.98~~ $7.48
42% OFF 1ST YEAR

Domain Registration
darklabhk.top
1 Year
AUTO-RENEW
~~$5.98~~ $2.98
50% OFF 1ST YEAR

ICANN fee $0.18

Privacy and Uptime protection

Domain Privacy *
1 year subscription
ENABLE
AUTO-RENEW
$0.00
FREE FOREVER!

What is the benefit?

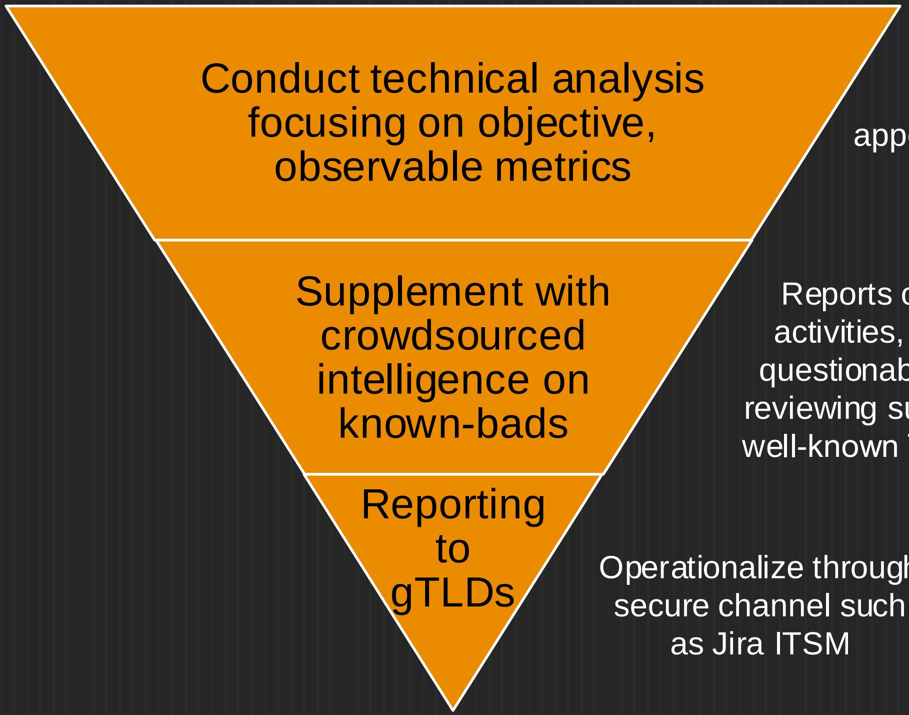
Privacy protection service that hides your personal info in the public Whois database, keeps your data safe and helps to avoid spam. Now free forever!

Limited WHOIS contact information required, with **insufficient validation** of registrant data due to domain privacy

Dark Lab

We devised a proactive mechanism and are working with .top to proof of concept it, before looking to scale out

Receive zone file from gTLD on regular basis



Conduct technical analysis focusing on objective, observable metrics

DNS metrics, appearance look-alike, WHOIS, …

Supplement with crowdsourced intelligence on known-bads

Reports of malicious activities, crawling for questionable keywords, reviewing submissions on well-known TI platforms…

Reporting to gTLDs

Operationalize through secure channel such as Jira ITSM

Takedown by gTLD or share with law enforcement and potential victims

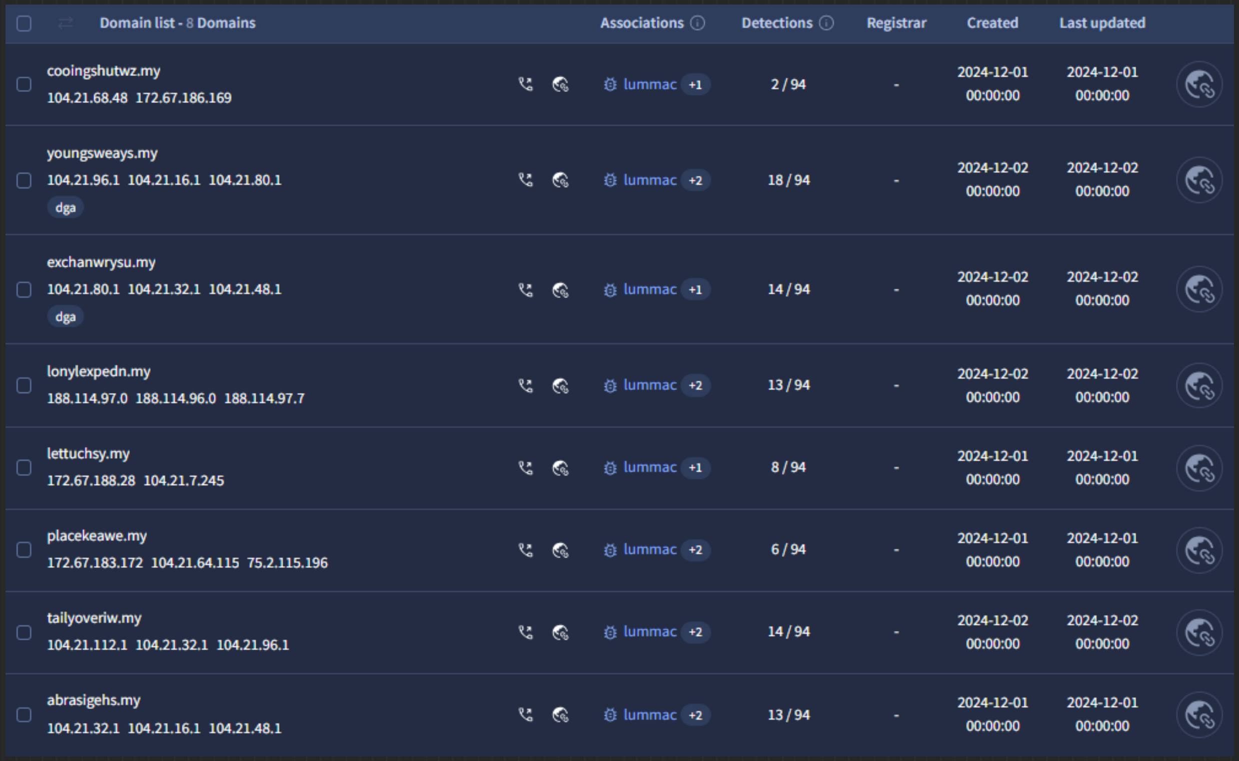
Official collaboration since 2024 Hack A Day to strengthen Hong Kong's cyberspace resilience

Source: https://www.pwchk.com/en/press-room/press-releases/pr-111124.html

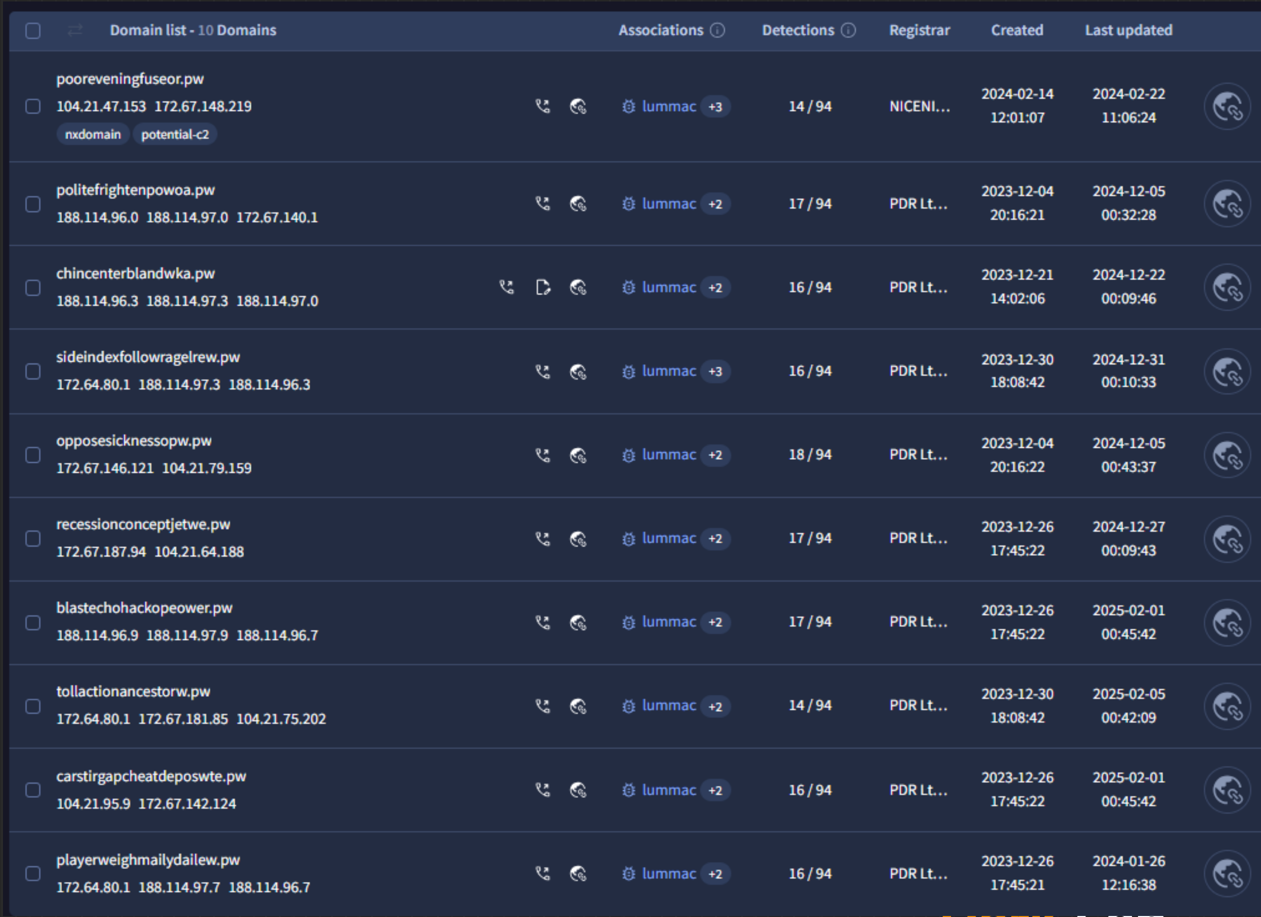
Dark Lab

Q&A

.my and .pw domain related to Lumma stealer

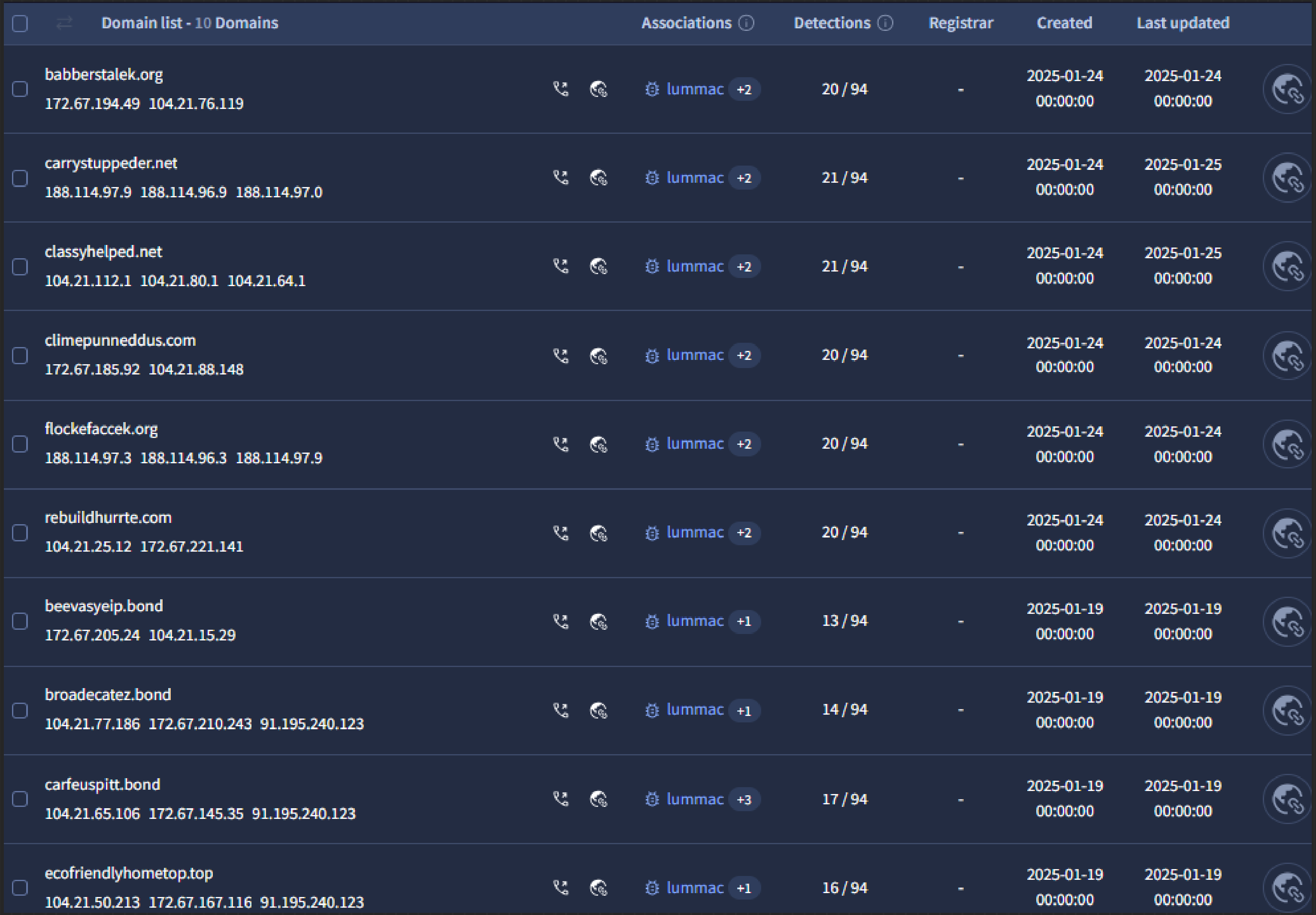


□	Domain list - 8 Domains	Associations	Detections	Registrar	Created	Last updated
□	cooingshutwz.my 104.21.68.48 172.67.186.169	lummac +1	2 / 94	-	2024-12-01 00:00:00	2024-12-01 00:00:00
□	youngsweays.my 104.21.96.1 104.21.16.1 104.21.80.1 dga	lummac +2	18 / 94	-	2024-12-02 00:00:00	2024-12-02 00:00:00
□	exchanwrysu.my 104.21.80.1 104.21.32.1 104.21.48.1 dga	lummac +1	14 / 94	-	2024-12-02 00:00:00	2024-12-02 00:00:00
□	lonylexpedn.my 188.114.97.0 188.114.96.0 188.114.97.7	lummac +2	13 / 94	-	2024-12-02 00:00:00	2024-12-02 00:00:00
□	lettuchsy.my 172.67.188.28 104.21.7.245	lummac +1	8 / 94	-	2024-12-01 00:00:00	2024-12-01 00:00:00
□	placekeawe.my 172.67.183.172 104.21.64.115 75.2.115.196	lummac +2	6 / 94	-	2024-12-01 00:00:00	2024-12-01 00:00:00
□	tailyoveriw.my 104.21.112.1 104.21.32.1 104.21.96.1	lummac +2	14 / 94	-	2024-12-02 00:00:00	2024-12-02 00:00:00
□	abrasigehs.my 104.21.32.1 104.21.16.1 104.21.48.1	lummac +2	13 / 94	-	2024-12-01 00:00:00	2024-12-01 00:00:00



□	Domain list - 10 Domains	Associations	Detections	Registrar	Created	Last updated
□	pooreveningfuseor.pw 104.21.47.153 172.67.148.219 nxdomain potential-c2	lummac +3	14 / 94	NICENI...	2024-02-14 12:01:07	2024-02-22 11:06:24
□	politefrightenpowoa.pw 188.114.96.0 188.114.97.0 172.67.140.1	lummac +2	17 / 94	PDR Lt...	2023-12-04 20:16:21	2024-12-05 00:32:28
□	chincenterblandwka.pw 188.114.96.3 188.114.97.3 188.114.97.0	lummac +2	16 / 94	PDR Lt...	2023-12-21 14:02:06	2024-12-22 00:09:46
□	sideindexfollowragelrew.pw 172.64.80.1 188.114.97.3 188.114.96.3	lummac +3	16 / 94	PDR Lt...	2023-12-30 18:08:42	2024-12-31 00:10:33
□	opposesicknessopw.pw 172.67.146.121 104.21.79.159	lummac +2	18 / 94	PDR Lt...	2023-12-04 20:16:22	2024-12-05 00:43:37
□	recessionconceptjetwe.pw 172.67.187.94 104.21.64.188	lummac +2	17 / 94	PDR Lt...	2023-12-26 17:45:22	2024-12-27 00:09:43
□	blastechohackopeower.pw 188.114.96.9 188.114.97.9 188.114.96.7	lummac +2	17 / 94	PDR Lt...	2023-12-26 17:45:22	2025-02-01 00:45:42
□	tollactionancestorw.pw 172.64.80.1 172.67.181.85 104.21.75.202	lummac +2	14 / 94	PDR Lt...	2023-12-30 18:08:42	2025-02-05 00:42:09
□	carstirgapcheatdeposwte.pw 104.21.95.9 172.67.142.124	lummac +2	16 / 94	PDR Lt...	2023-12-26 17:45:22	2025-02-01 00:45:42
□	playerweighmailydailew.pw 172.64.80.1 188.114.97.7 188.114.96.7	lummac +2	16 / 94	PDR Lt...	2023-12-26 17:45:21	2024-01-26 12:16:38

Lumma gTLD



□	Domain list - 10 Domains	Associations	Detections	Registrar	Created	Last updated
□	babberstalek.org 172.67.194.49 104.21.76.119	lummac +2	20 / 94	-	2025-01-24 00:00:00	2025-01-24 00:00:00
□	carrystuppeder.net 188.114.97.9 188.114.96.9 188.114.97.0	lummac +2	21 / 94	-	2025-01-24 00:00:00	2025-01-25 00:00:00
□	classyhelped.net 104.21.112.1 104.21.80.1 104.21.64.1	lummac +2	21 / 94	-	2025-01-24 00:00:00	2025-01-25 00:00:00
□	climepunneddus.com 172.67.185.92 104.21.88.148	lummac +2	20 / 94	-	2025-01-24 00:00:00	2025-01-24 00:00:00
□	flockefaccek.org 188.114.97.3 188.114.96.3 188.114.97.9	lummac +2	20 / 94	-	2025-01-24 00:00:00	2025-01-24 00:00:00
□	rebuildhurrte.com 104.21.25.12 172.67.221.141	lummac +2	20 / 94	-	2025-01-24 00:00:00	2025-01-24 00:00:00
□	beevasyeip.bond 172.67.205.24 104.21.15.29	lummac +1	13 / 94	-	2025-01-19 00:00:00	2025-01-19 00:00:00
□	broadecatez.bond 104.21.77.186 172.67.210.243 91.195.240.123	lummac +1	14 / 94	-	2025-01-19 00:00:00	2025-01-19 00:00:00
□	carfeuspitt.bond 104.21.65.106 172.67.145.35 91.195.240.123	lummac +3	17 / 94	-	2025-01-19 00:00:00	2025-01-19 00:00:00
□	ecofriendlyhometop.top 104.21.50.213 172.67.167.116 91.195.240.123	lummac +1	16 / 94	-	2025-01-19 00:00:00	2025-01-19 00:00:00

Thank you

pwc.com