



A deep dive into the I-Soon leak

Ivan Kwiatkowski
Cyber Threat Research
@JusticeRage



I-Soon (Anxun)

- Founded in 2010
 - “APT pentest research department” in 2013
- CEO : Wu Haibo (吴海波)
- HQ in Shanghai
 - Chengdu (Sichuan) subsidiary in 2015 – R&D, pentest
 - Yunnan subsidiary in 2017 – “regional market work”
 - Jiangsu subsidiary in 2020 - “regional market work”
- 72 employees in registration documents
 - ~ 100 at the time of the leaks
- “Become a solid national defense reserve force with a strong sense of political responsibility and a spirit of high responsibility to the Party and the People”



I-Soon (Anxun)

- Certified supplier for the Cyber Security and Defense Bureau of the MPS to “provide technologies, tools or equipment”
- Class II secrecy qualification for weapons and equipment research and production company
- 59 patents, such as “an intelligent platform and its application in assisting criminal investigation”, “special investigative warfare platform”, etc.



1. 中华人民共和国公安部 - Ministry of Public Security of the People's Republic of China
2. 北京市公安局 - Beijing Municipal Public Security Bureau
3. 广东省公安厅 - Guangdong Provincial Public Security Department
4. 江苏省公安厅 - Jiangsu Provincial Public Security Department
5. 河南省公安厅 - Henan Provincial Public Security Department
6. 重庆市公安局 - Chongqing Municipal Public Security Bureau
7. 内蒙古自治区公安厅 - Public Security Department of Inner Mongolia Autonomous Region
8. 宁夏回族自治区公安厅 - Public Security Department of Ningxia Hui Autonomous Region
9. 广西壮族自治区公安厅 - Public Security Department of Guangxi Zhuang Autonomous Region
10. 新疆维吾尔自治区公安厅 - Public Security Department of Xinjiang Uyghur Autonomous Region
11. 西藏自治区公安厅 - Public Security Department of Tibet Autonomous Region
12. 青海省公安厅 - Qinghai Provincial Public Security Department
13. 甘肃省公安厅 - Gansu Provincial Public Security Department
14. 陕西省公安厅 - Shaanxi Provincial Public Security Department
15. 黑龙江省公安厅 - Heilongjiang Provincial Public Security Department
16. 吉林省公安厅 - Jilin Provincial Public Security Department
17. 辽宁省公安厅 - Liaoning Provincial Public Security Department
18. 山东省公安厅 - Shandong Provincial Public Security Department
19. 山西省公安厅 - Shanxi Provincial Public Security Department
20. 河北省公安厅 - Hebei Provincial Public Security Department
21. 天津市公安局 - Tianjin Municipal Public Security Bureau
22. 上海市公安局 - Shanghai Municipal Public Security Bureau
23. 浙江省公安厅 - Zhejiang Provincial Public Security Department
24. 安徽省公安厅 - Anhui Provincial Public Security Department
25. 福建省公安厅 - Fujian Provincial Public Security Department
26. 江西省公安厅 - Jiangxi Provincial Public Security Department
27. 湖南省公安厅 - Hunan Provincial Public Security Department
28. 湖北省公安厅 - Hubei Provincial Public Security Department
29. 四川省公安厅 - Sichuan Provincial Public Security Department
30. 贵州省公安厅 - Guizhou Provincial Public Security Department
31. 云南省公安厅 - Yunnan Provincial Public Security Department
32. 海南省公安厅 - Hainan Provincial Public Security Department

Too many public contracts?

2022-06-13 07:53:29	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	Global proxy
2022-06-13 07:53:40	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	This is what we need to teach them
2022-06-13 07:53:50	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Generally, we sell here and also teach
2022-06-13 07:53:55	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	[Face covering] I want it
2022-06-13 07:54:01	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	I'm really drunk [laughing through tears]
2022-06-13 07:54:08	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	The public security customers are so stupid
2022-06-13 07:54:17	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Calm down
2022-06-13 07:54:19	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Haha
2022-06-13 07:54:21	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	I want to do a business that does not involve police this year
2022-06-13 07:54:23	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	So tired
2022-06-13 07:54:35	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	No fucking money for football
2022-06-13 07:55:08	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Normal
2022-06-13 07:55:13	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	You must deal with after-sales service
2022-06-13 07:55:22	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	[Face covering]

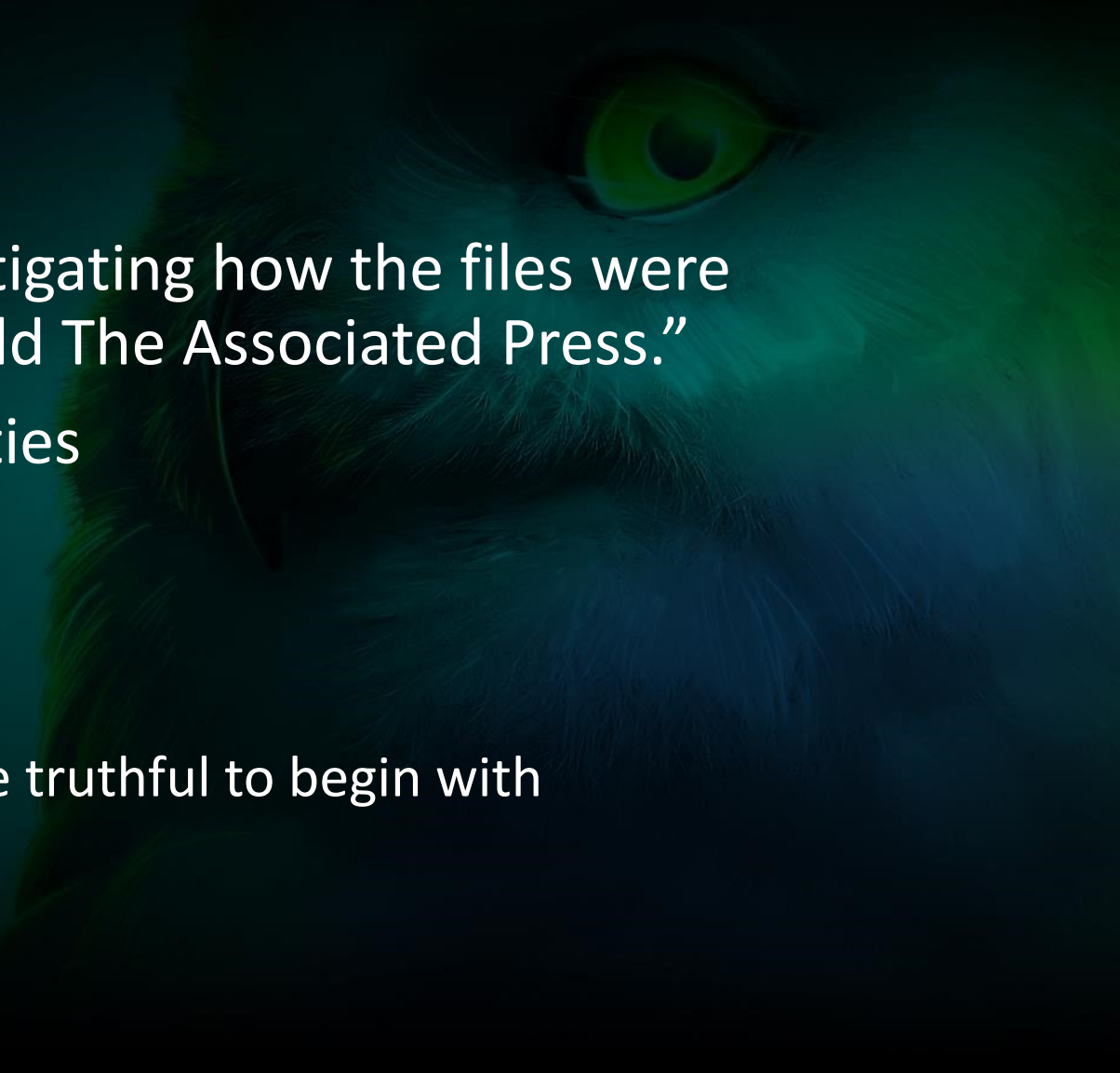
...including Trojan horses?



2021-11-23 08:27:17	lengmo	Shutd0wn	Jiangsu Provincial Department also wants to buy 3 🐼 this time, Windows, Linux and Android, any Android one will be fine. Depends on which house it is from.
2021-11-23 08:28:24	Shutd0wn	lengmo	We will definitely make a full version, supplemented by suppliers
2021-11-23 08:28:53	lengmo	Shutd0wn	Hmm... Then you need to organize a team to do it. It would be best if your own can meet the requirements. Gross profit is still higher.
2021-11-25 02:31:06	lengmo	Shutd0wn	The Wuxi project just won the bid for 7988000
2021-11-25 02:32:06	Shutd0wn	lengmo	niubility
2021-11-25 02:32:25	lengmo	Shutd0wn	Do you know what is the most important thing?
2021-11-25 02:32:26	Shutd0wn	lengmo	There was no mistake or cancellation of the mark. . . .
2021-11-25 02:32:37	lengmo	Shutd0wn	I won the bid at the direct closing price...no quotation was made
2021-11-25 02:32:38	Shutd0wn	lengmo	What?
2021-11-25 02:32:43	lengmo	Shutd0wn	Directly announce that we won the bid
2021-11-25 02:33:03	lengmo	Shutd0wn	After demolition and review, we were announced as the winner
2021-11-25 02:33:20	lengmo	Shutd0wn	It shows that network security is still very strong
2021-11-25 02:33:44	Shutd0wn	lengmo	Well, regional differences, Jiangsu Internet security should be generally strong

Is the leak legitimate?

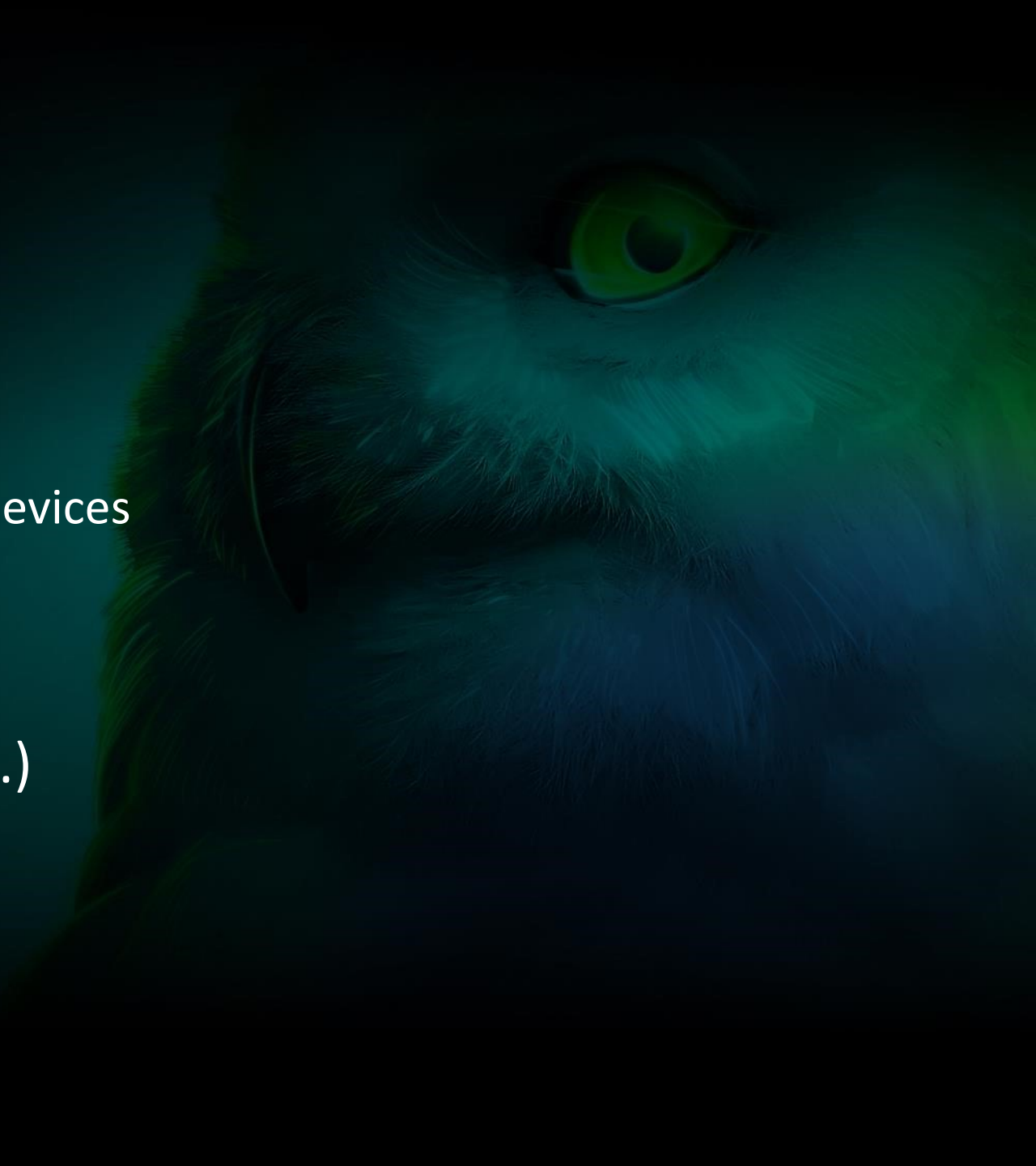
- “I-Soon and Chinese police are investigating how the files were leaked, the two I-Soon employees told The Associated Press.”
- Links to previously known APT activities
- Is the data reliable?
 - Some key information may be missing
 - Possibility of targeted tampering
 - Commercial documentation may not be truthful to begin with



What is in the leak?

- Product documentation
- IM chats between employees
 - Including screenshots from mobile devices
- Raw hacked data
- Bids for public contracts
- Internal documents (pay scale, etc.)

- No source code :(



Leak origin

- Data uploaded on GitHub on February 16, 2024
- Account: `is00n@proton.me`
- Another account created earlier, possibly related

```
pub ed25519 2023-09-25 [SC]
```

```
421EA93EC291A950BD33ECD504AC29C49FAAC430
```

```
uid      isoon@proton.me <isoon@proton.me>
```

```
sub cv25519 2023-09-25 [E]
```

- Competitor? Disgruntled employee? Foreign APT?



APT research team



3 penetration teams, 1 security research team, 1
basic support team, a total of 70+ people



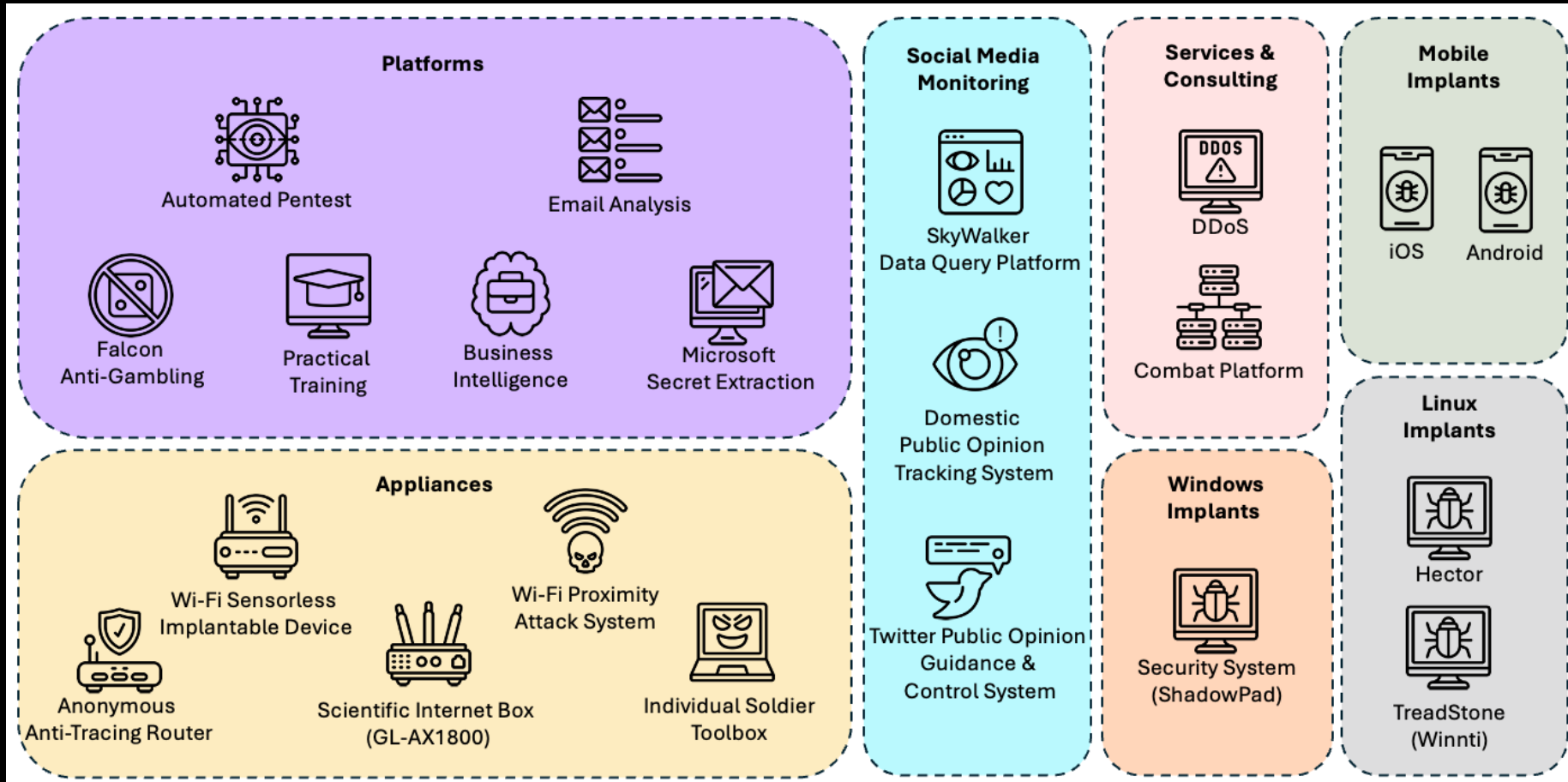
Cooperate with relevant departments
to complete multiple overseas APT projects



Main results area

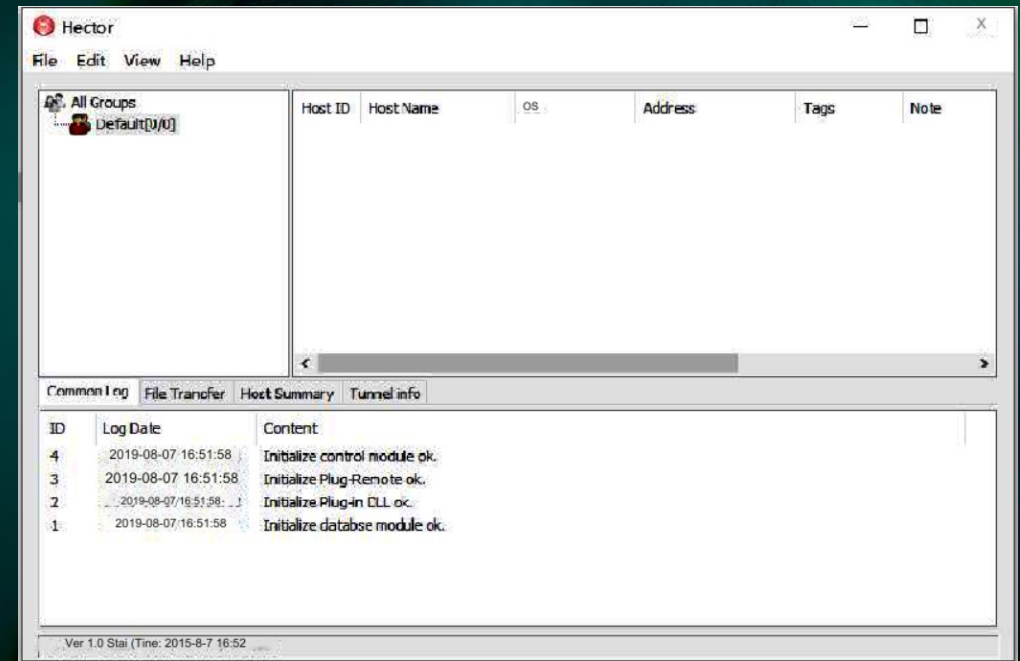
Central Asia/West Asia/Southeast Asia/Hong Kong, Macao and Taiwan direction

Overview



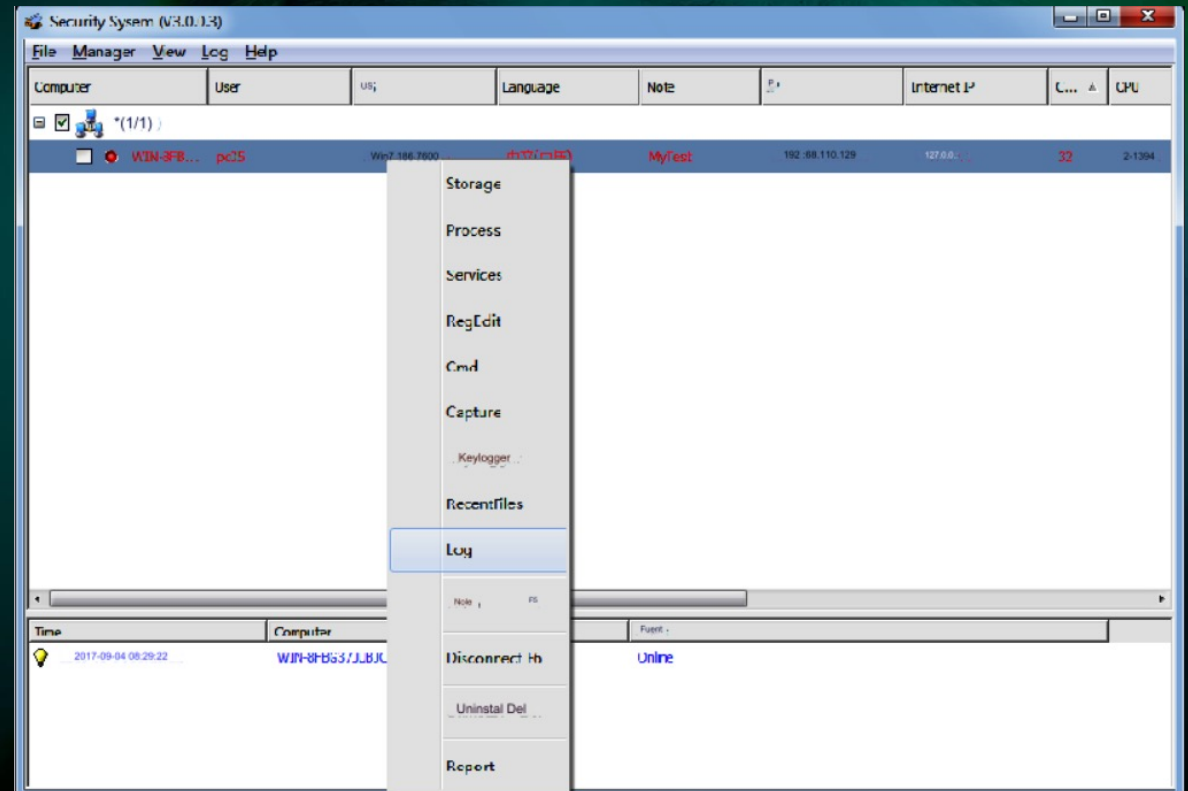
RATs

- Windows
- Linux
- Android & iOS (very limited info)
- Features
 - Download / execute
 - Filesystem management
 - Arbitrary command execution
 - (Keylogging / screen capture)
- Delivered with training + source code



RATs

- Specs for new malware families require more advanced features (proxy bypass, AV evasion, etc.)
- Conversations mention difficulties sourcing trojans for certain systems
- Cooperation / sharing in the ecosystem
- The customer can provide their own RAT for a discount(!?)



Automated Penetration Testing Platform



- Ruby framework with “modules” (exploits, “auxiliary”, “encoders”, “post” ...)
- Attack steps:
 - Verify that the system is up (ping)
 - Scan ports (connect() scan, SYN scan, NULL scan, Idle scan...)
 - Attempt exploitation
- Can be manipulated via API, CLI, web interface, etc.
- Integration with OpenVAS, Nessus, Acunetix, Burp Proxy, Core Impact, Nexpose...

Automated Penetration Testing Platform



- Automated webapp testing
 - Crawling
 - Automatic testing of top 10 OWASP vulnerabilities
- Mobile penetration testing
 - Online generation of Android payloads
 - iOS support advertised without any details
- Social engineering module
 - Generation of phishing emails
 - Website cloning

Automated Penetration Testing Platform



- Passwords
 - Credential verification
 - Bruteforcing
- Platform features
 - Multi-user with permission system
 - Logging of all actions
 - Report generation

Automated Penetration Testing Platform

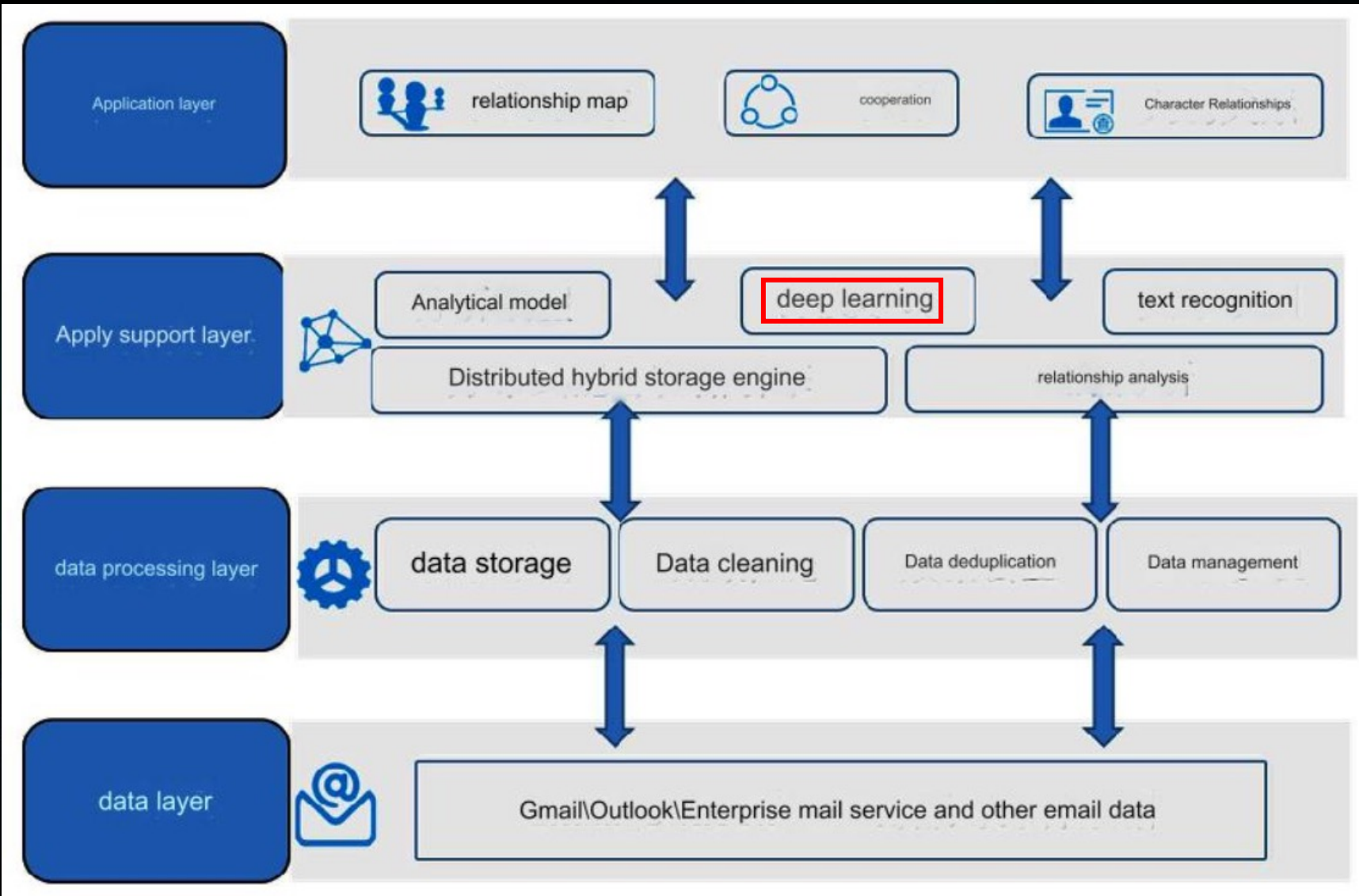


- Assessment: single GUI built on top of existing tools?
 - Nmap: same supported scan modes
 - Metasploit Pro
 - Ruby
 - References to meterpreter, LHOST, LPORT...
 - “Built-in Metasploit professional version”
 - SET (Social Engineering Toolkit): similar features
 - Hydra: similar supported protocols
- Assessment: little added value over OSS tools
 - Marketed at organizations (i.e., military) where the average employee wouldn't be comfortable with Kali Linux

Many data analysis platforms

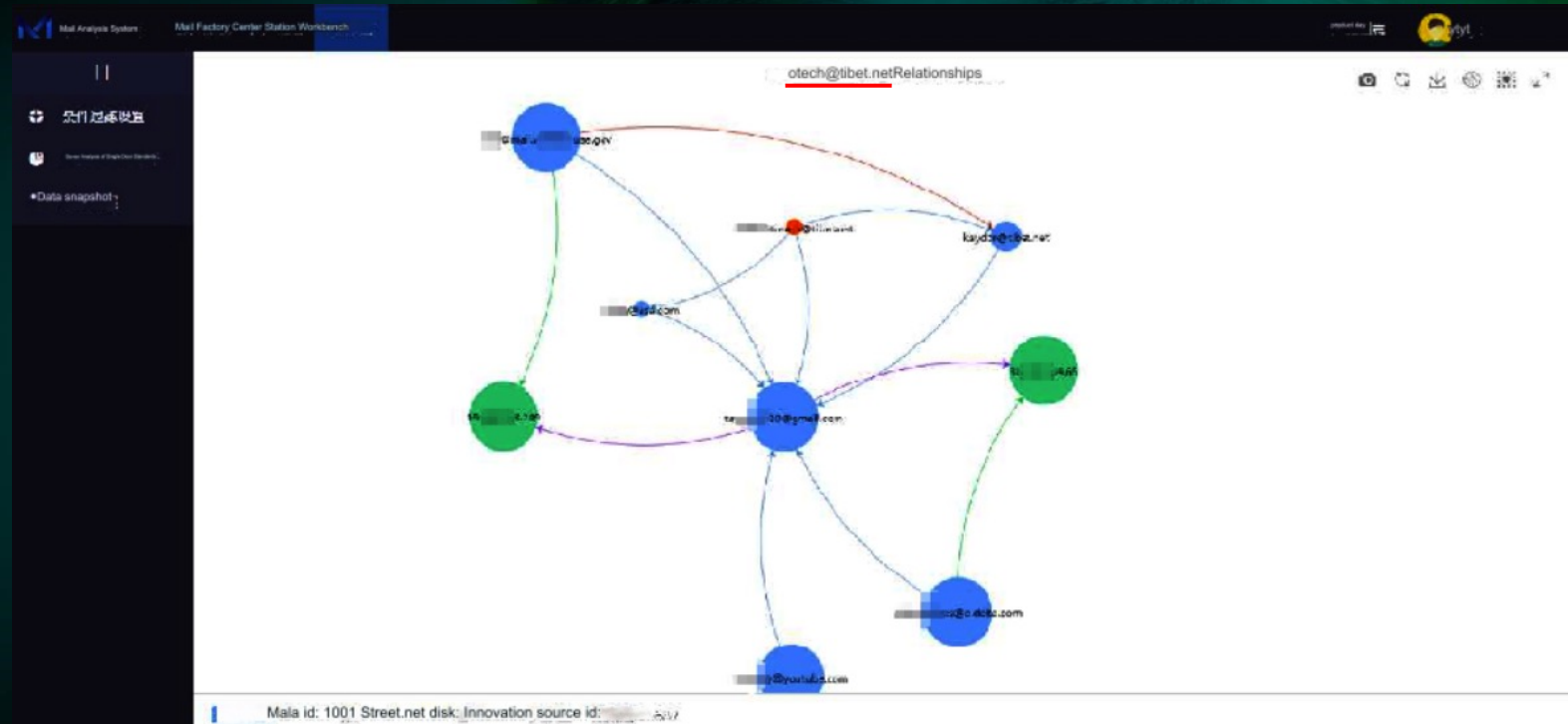
- Likely built from the same engine
 - Knowledge management
 - Data mining
 - Relationship extraction
 - Phishing integration
- Variants for each “market segment”
- SaaS or on-premise
- Data provided by the customer or by I-Soon

Product	Input data
Email Analysis Platform	Emails, PSTs, etc.
Microsoft Secret Extraction Platform	Outlook credentials (automated collection + phishing capabilities)
Falcon Anti-Gambling Platform	Data obtained from gambling websites
Anxun Integrated Data Platform	Stolen PII
Anxun Cloud Intelligence Analysis & Decision-Making Platform	Stolen documents
Xunzong Security Intelligence Platform	Data handled by intelligence services
Twitter Public Opinion Guidance and Control System	Twitter credentials (automated collection + phishing capabilities)
SkyWalker Data Query Platform	PII (LEA / domestic use)
Domestic Public Opinion Tracking System	OSINT capabilities for local social networks



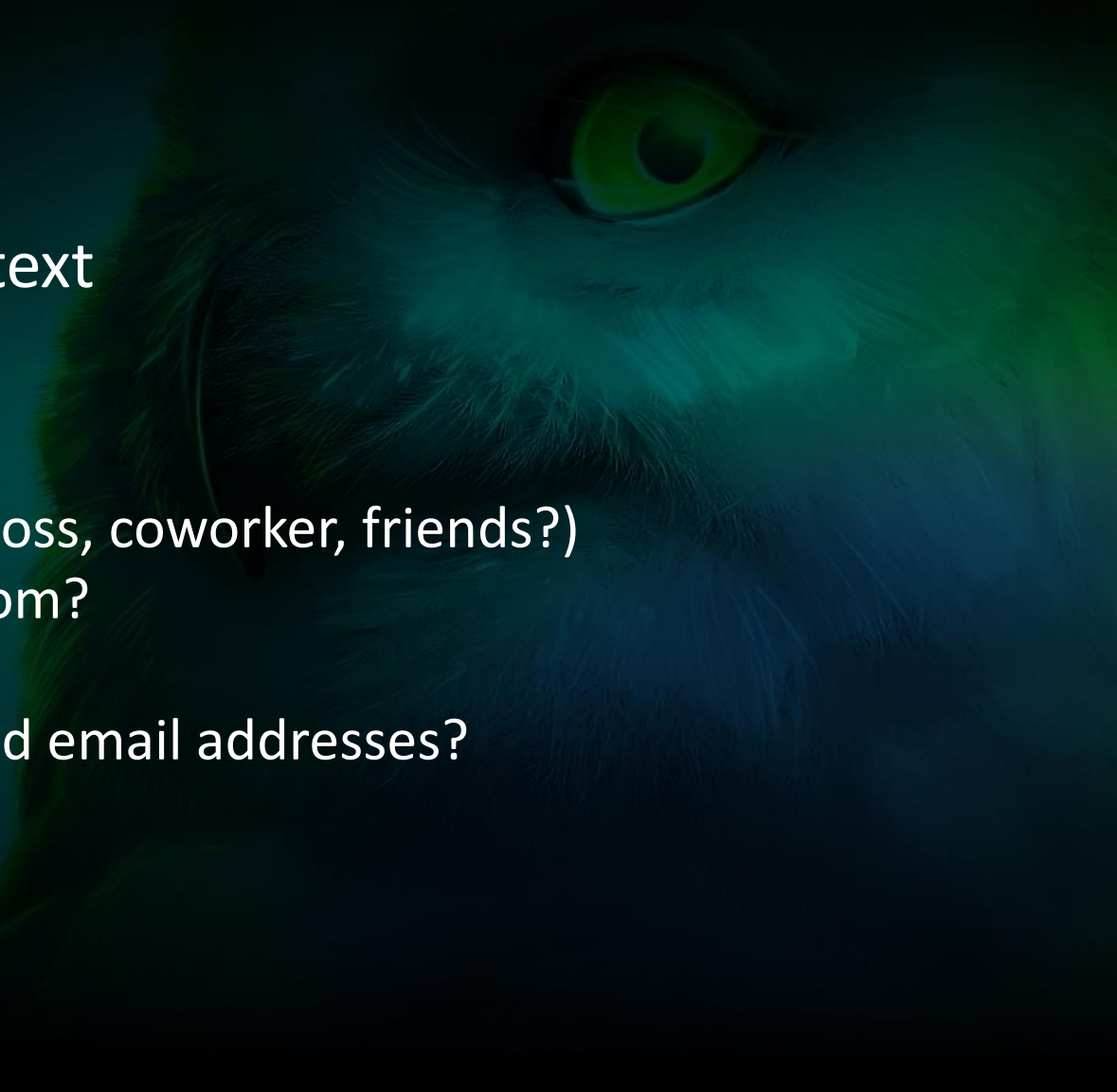
Email analysis platform

- Input: lots of emails
 - Automated collection feature
- Output:
 - Content matching keywords, “sensitive words”
 - Social graph
 - Fulltext search
- Knowledge management system
 - Tagging system
- SaaS or on-premise



Deep learning

- Extraction and classification of email text
- “Relationship network mining”
 - Determines the nature of the relation (boss, coworker, friends?)
 - Based on who talks to whom, about whom?
 - Extracts PII?
 - Automated mapping between names and email addresses?
- Creation of a full listing of individuals
 - Name, age, gender, nationality, etc.



2018 3130

Add analysis data source

11 切换

All(5453)(0) Bu Jia (0) Undeposited(6) 31241

How type theme

- View Your Latest Credit Score
- Uskpa Kichoe Lhaktsang shared mark Angel's v
- Seminar on Improving Purchasing Negotiation S
- Seminar on Improving Purchasing Negotiation S
- EDUCATED HUMANS DEDICATED TO YOU ALL G
- Re: Flight ticket**
- Dispatch Details of Taxman - Volume 254 Part 5
- Draft invoice No-1 Ingenus Strategy.pdf

1 2 3 4 5 + 5/16 >

文件树

Re: Flight ticket

Uploader: admin@gl-soon.net
file name: 20180008-Ke Phil ticket-739/582.eml

Sender: DoHee@tibet.net

收件人:

Text:

Dear Kishure Rau ji,

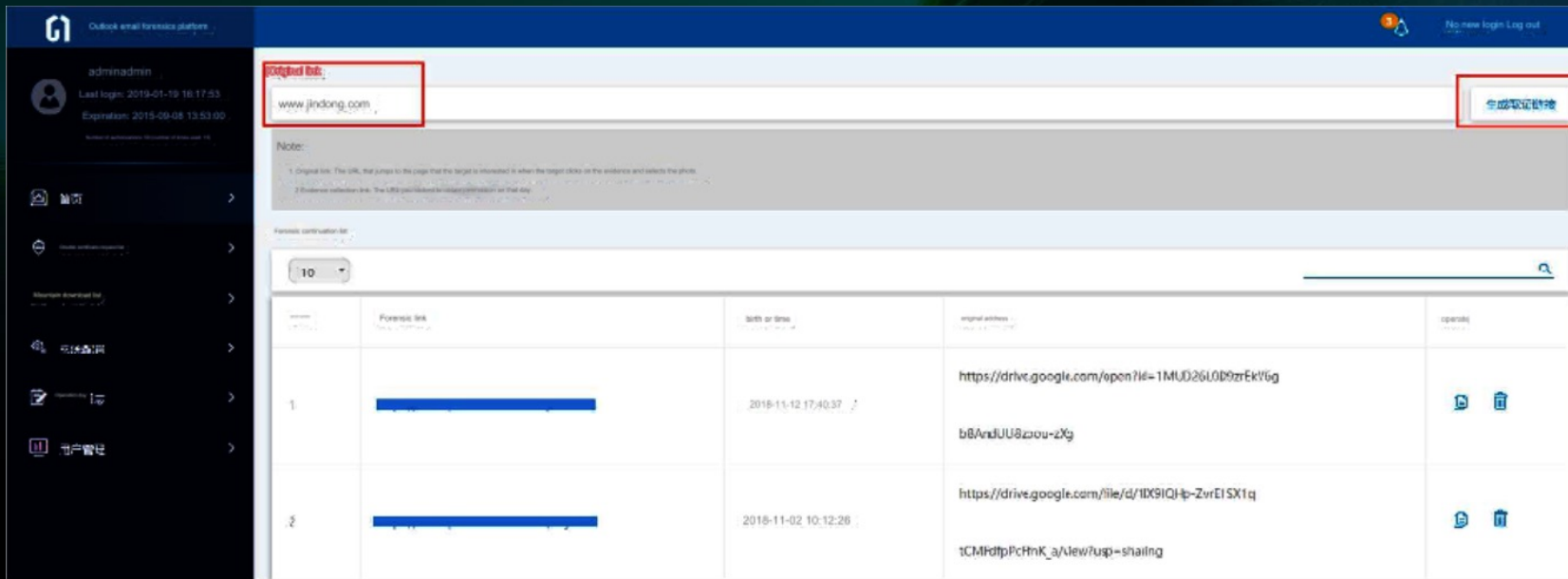
I would like to follow up with our conversation over telephone, I am planning to go to be discuss with & Cooperative President and and other role stakeholders.

1. Selection set up mill factory.
2. Construction of the factory
3. License & registration.
4. Operational management procedure

+Note

Microsoft Secret Extraction Platform

- Platform aimed at breaching Outlook accounts
- Automated generation of phishing emails
- Continuous siphoning of the victim's emails



Outlook email forensic platform

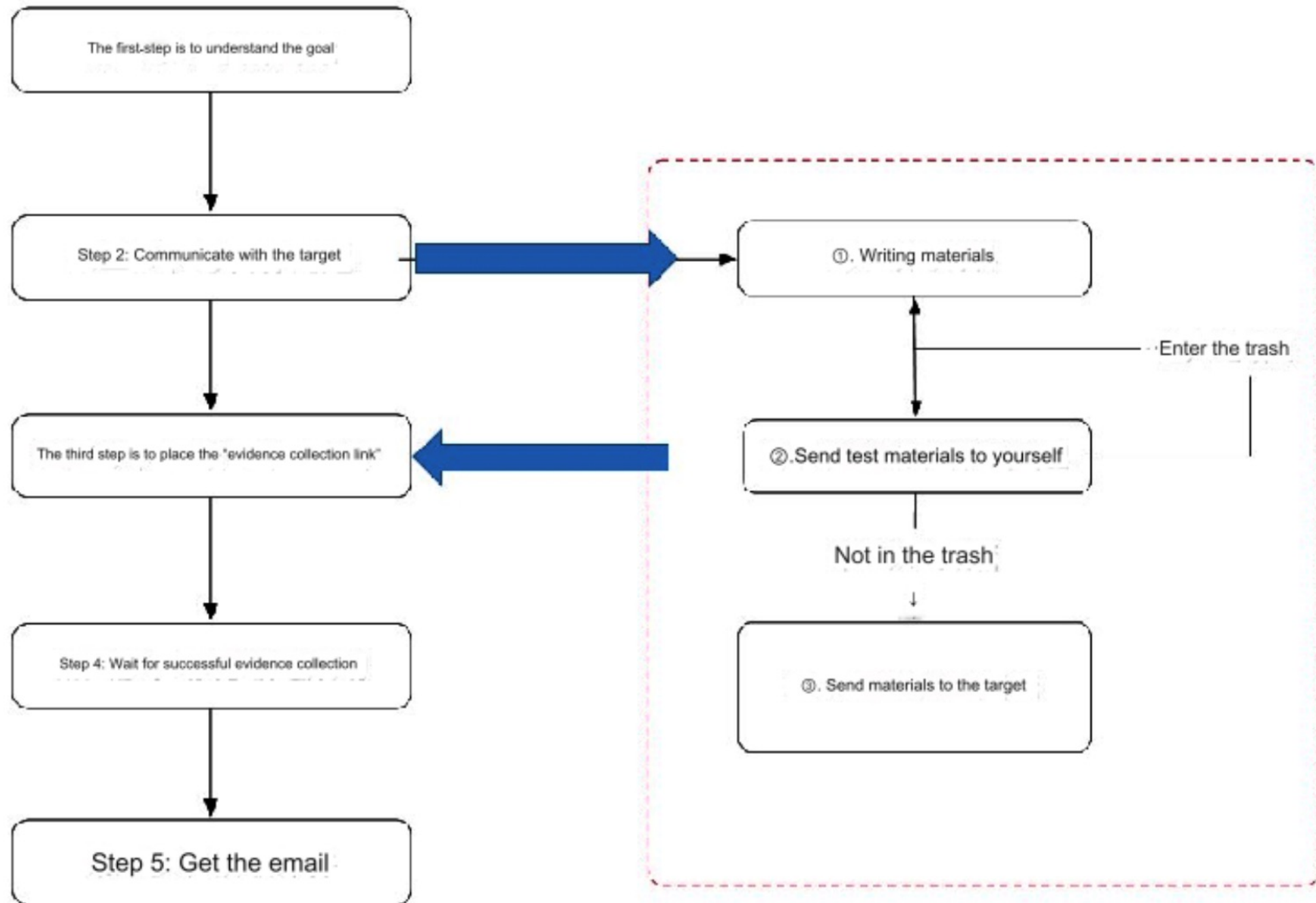
adminadmin
Last login: 2019-01-19 16:17:53
Expiration: 2015-09-08 13:53:00

Original link: www.jindong.com

Note:
1. Original link: The URL that jumps to the page that the target is interested in when the target clicks on the evidence and selects the photo.
2. Forensic extraction link: The URL provided to the target (phishing) on that day.

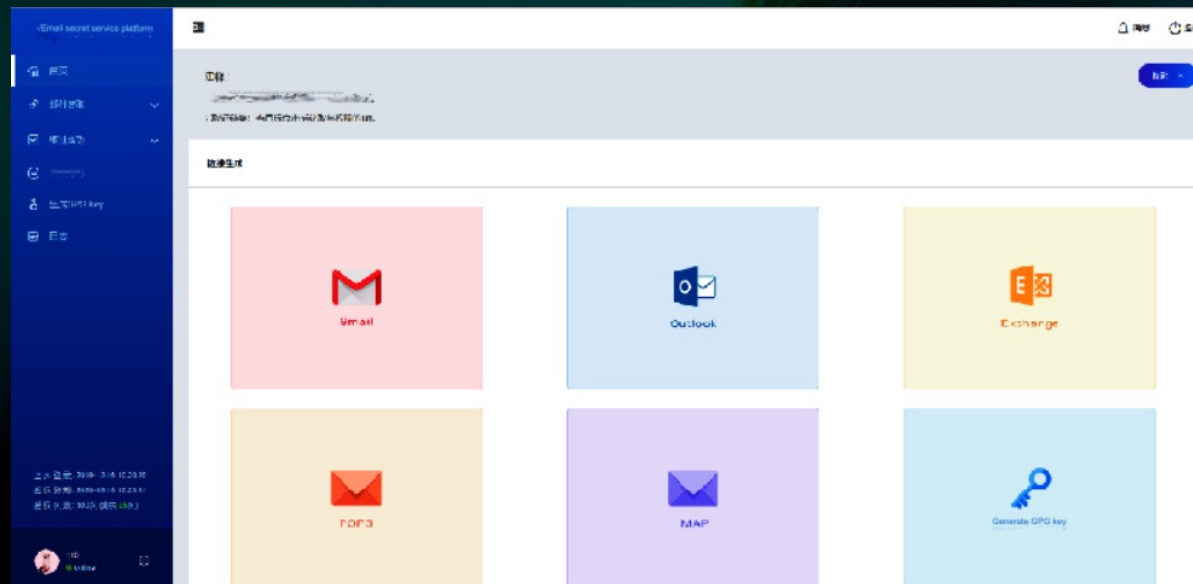
Forensic link table:

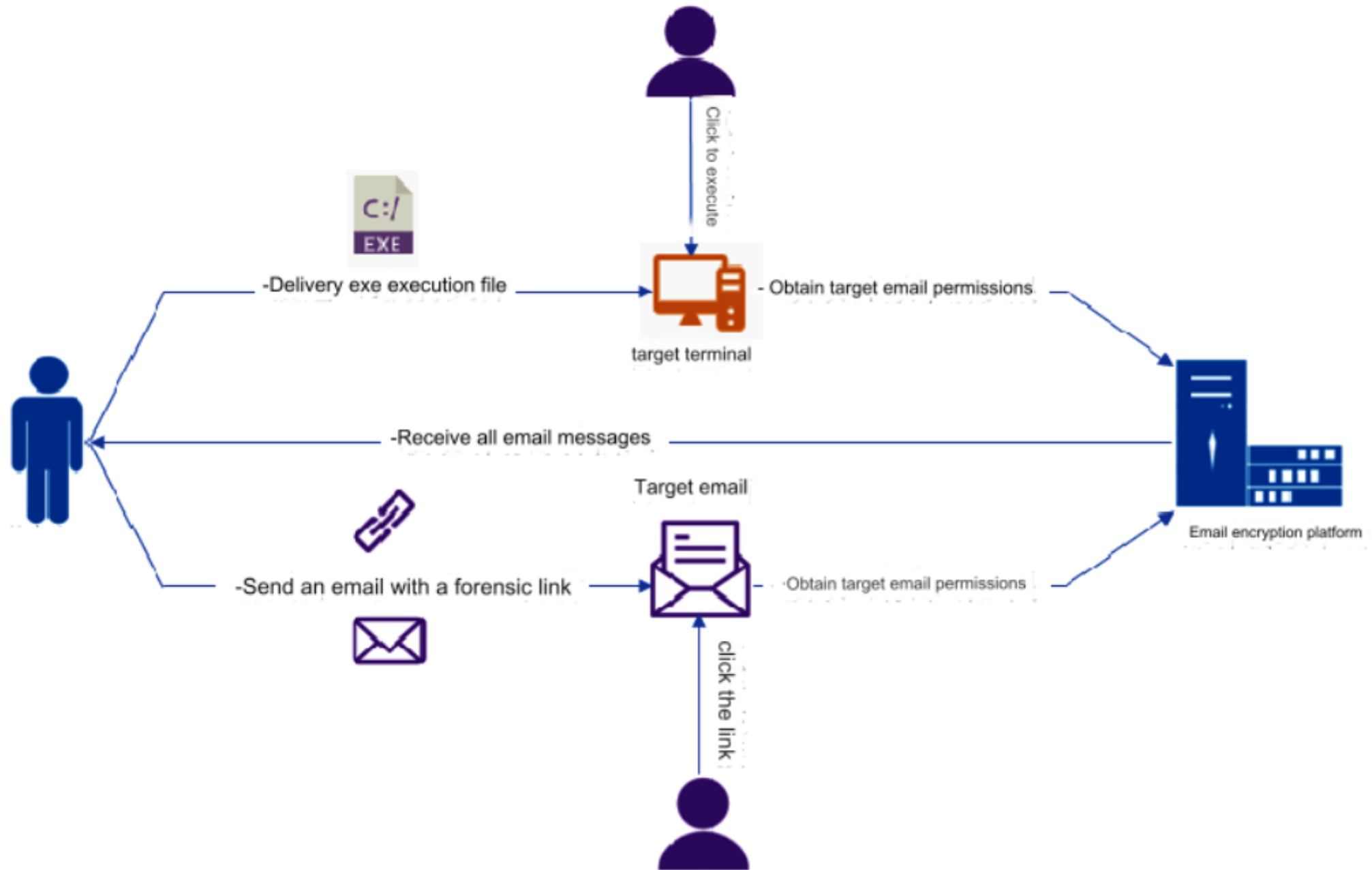
	Forensic link	Date or time	Original address	Operate
1	[Redacted]	2018-11-12 17:40:37	https://drive.google.com/open?id=1MUD26L0D9mEKV6g bBAAndUU8zou-zXg	[Icons]
2	[Redacted]	2018-11-02 10:12:28	https://drive.google.com/file/d/1IX9IQ4p-ZurE1SX1q tCMFdtPpChnK_a/View?usp=sharing	[Icons]



Email collection platform (2020)

- Appears to supersede the Microsoft Secret Extraction Platform (2022)
 - Possibly split in separate products for billing reasons
- Supports Outlook, Gmail, POP3 & IMAP.
- Bypasses 2FA, IP origin verification, etc.
- Identical system for Twitter.





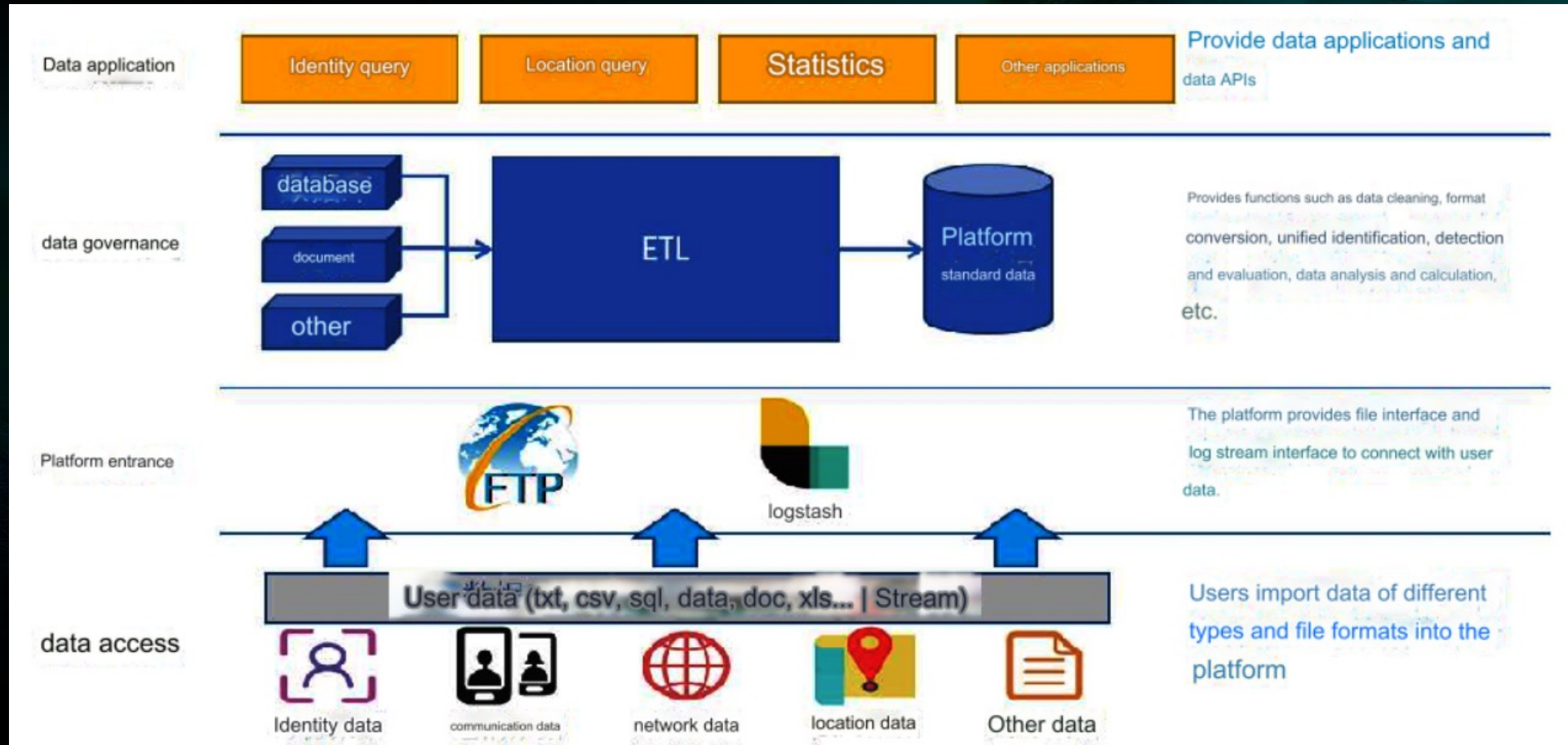
Falcon Anti-Gambling Platform

- Data-analysis/dataviz platform for “gambling data”
 - Account names, email addresses, passwords, mobile number, IP address...
 - Money flow analysis
 - Obtained via hacking? By I-Soon?
- Collaborative platform for investigators / analysts
- After manual review, individual cases are created
 - Forwarded to the “business department” to query bank records

2022-05-11 05:02:10	wxid_7p054rmzkhqf21	gzp1991101	Yeah
2022-05-11 05:58:58	wxid_7p054rmzkhqf21	gzp1991101	Play mahjong
2022-05-11 05:59:24	gzp1991101	wxid_7p054rmzkhqf21	I just lost 1300 yesterday [angry]
2022-05-11 05:59:36	wxid_7p054rmzkhqf21	gzp1991101	Let's lose some more today
2022-05-11 05:59:47	wxid_7p054rmzkhqf21	gzp1991101	The leader will take care of you

(Meanwhile at I-Soon)

Anxun Integrated Data Platform / Anxun Cloud Intelligence Analysis & Decision-Making Platform / Xunzong Security Intelligence Platform



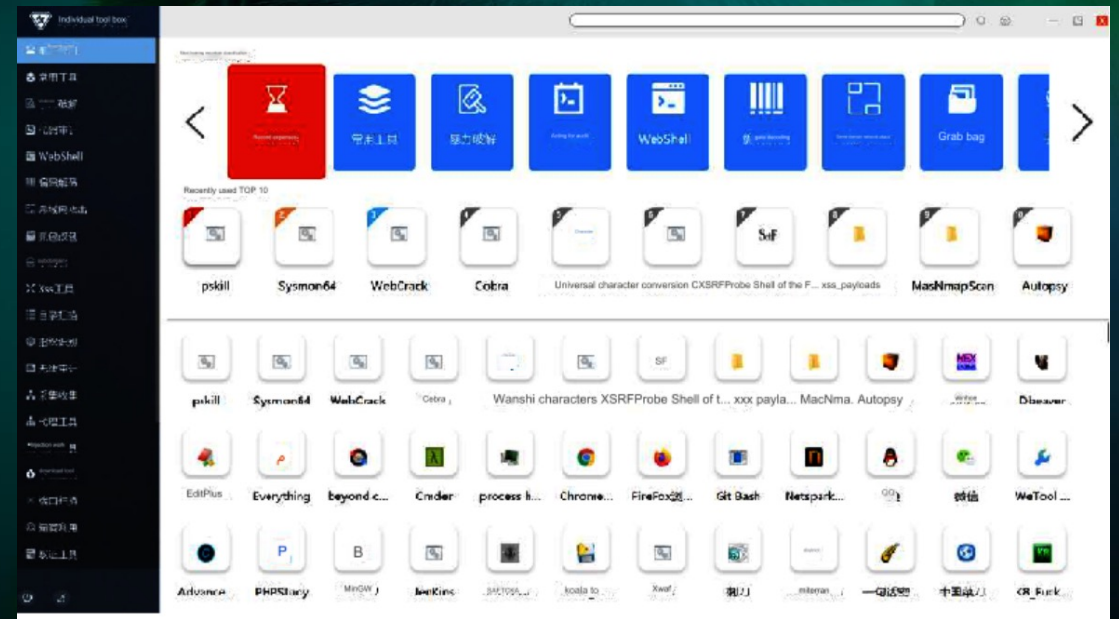
Practical Training Platform

- Cyber range
 - Dynamic environment to simulate “real combat”
- “Based on our company’s years of experience in APT penetration attacks”



Individual Soldier Toolbox

- Notebook pre-configured with security tools
- Windows-based, but all tools gathered in a single GUI



WiFi Proximity Attack System

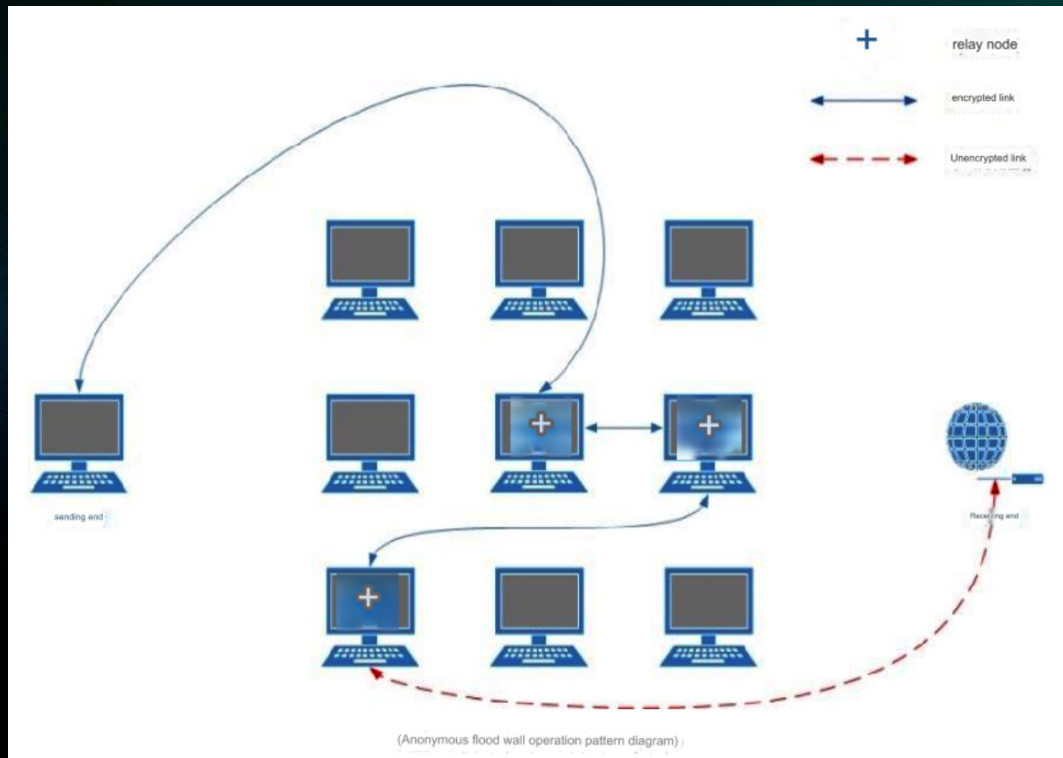
- Device disguised as a power adapter
- Automatic cracking of surrounding WiFi network keys
 - Cloud cracking over 5G for WPA/2
- SOCKS proxy into the victim network
- Credentials sniffing on the network
- Automated hacking of local routers
 - Weak passwords based on the brand?
- Remote wiping

- Other product: “WiFi terminal positioning equipment”

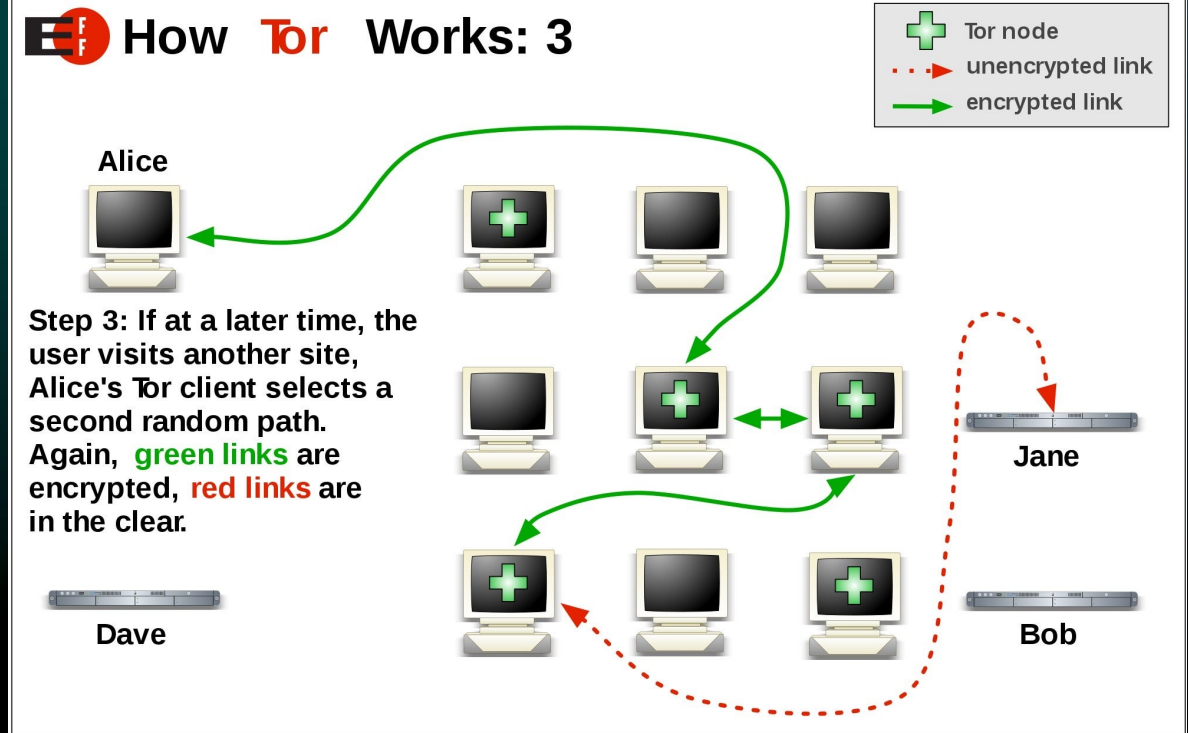


OPSEC: “Anonymous Anti-Tracing Wall”

- Anonymizing 4-port 100Mb router
- Free 1 year maintenance, then renewal is ~15k€



How Tor Works: 3



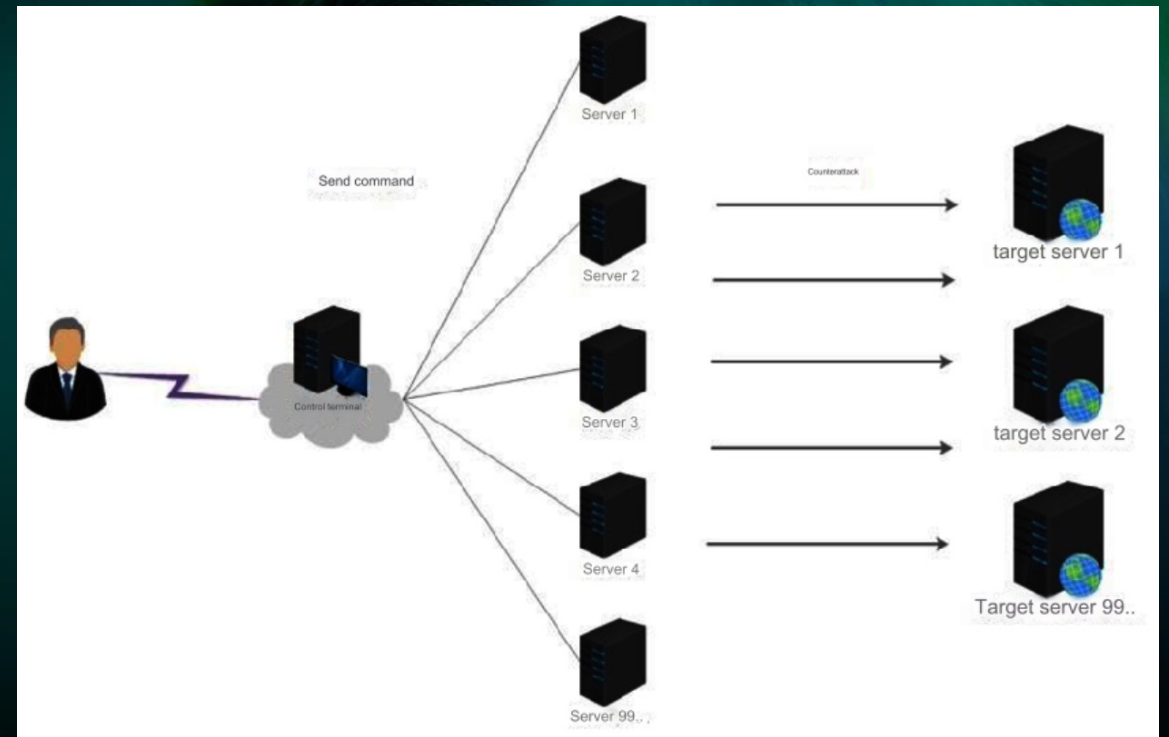
Scientific Internet Box

- WiFi Router for “scientific” research on foreign and domestic opinion
 - Bypasses the Great Firewall of China
- Seems to be derived from the GL-AX1800 router (GL-iNet)
- Routes traffic via “network nodes distributed around the world”
 - Servers located in HK (40), then Japan, USA and Singapore (18 each)



Network Traffic Countermeasures System

- DDoS as a Service
- “Active scanning” to acquire global traffic capabilities.
- Cluster management
- SYN, TCP, UDP, ACK, GET flooding and way more.
- Possibly based on masscan or Zmap

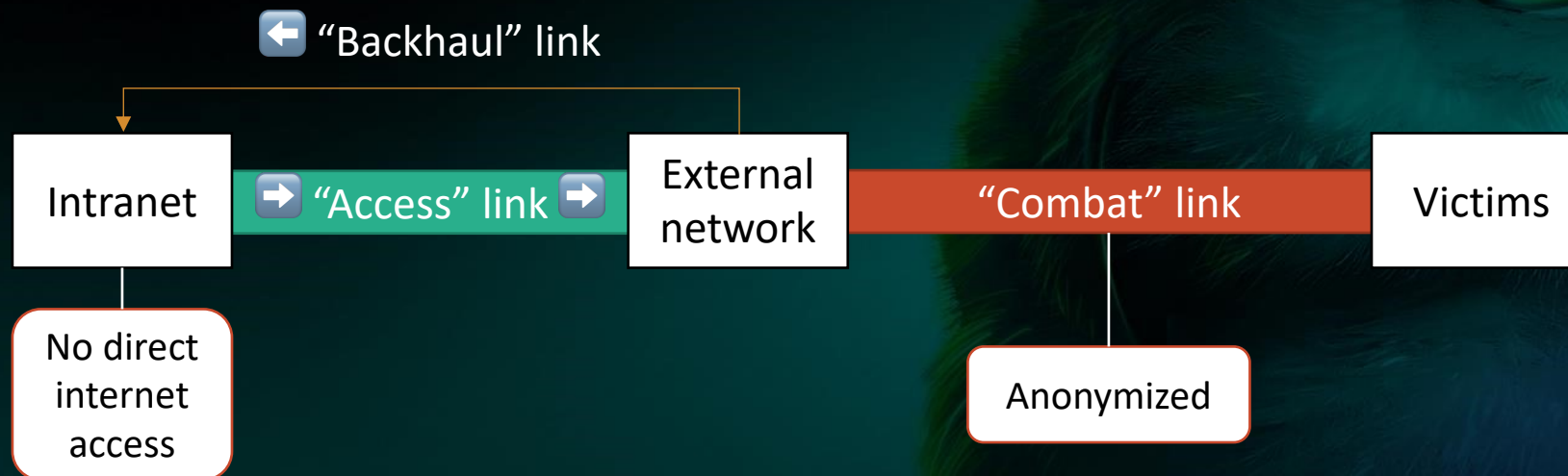


Integrated Combat Platform



- Attack infrastructure installation
- Network design
 - “Covert” link for attacks
 - “Scientific” link for web searches
 - Isolated network with one-way link to send stolen files in the intranet
- Operation management dashboard
 - User management, implant management (encryption + download logging), etc.
 - Review / scoring system for completed tasks, to evaluate performance
 - Internal BBS as a “TTP sharing” system
- VPS & VM management
 - VPS = C2 servers (“all IP addresses are overseas addresses”)
VMs = Operator machines
 - Provisioned from templates (!)
- Sandbox for malware analysis

Integrated Combat Platform / OPSEC

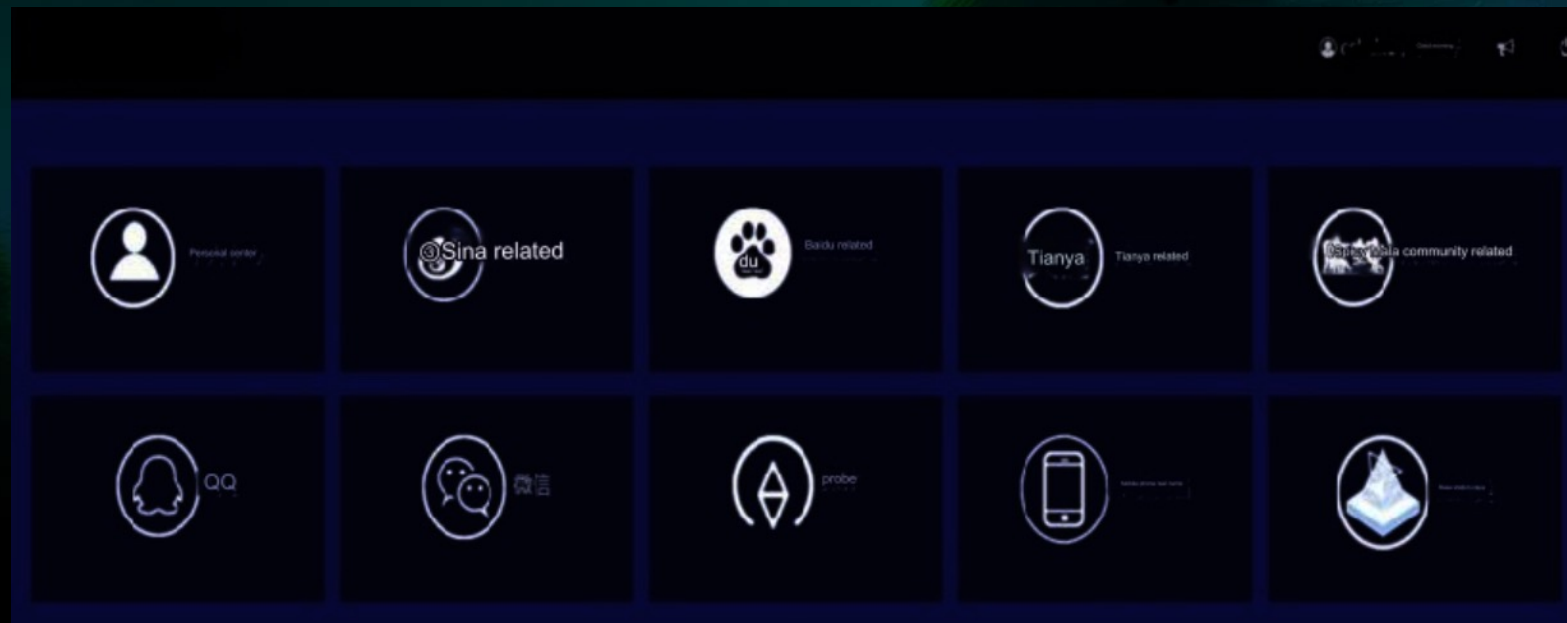


The fifth is security cover: Platform development, line rental, computer room rental and other businesses need to be handled using a cover identity to prevent

Stop being traced and located. The system, language, time zone, font, system environment, input method, etc. used by the external platform must all be in non-Chinese languages. all

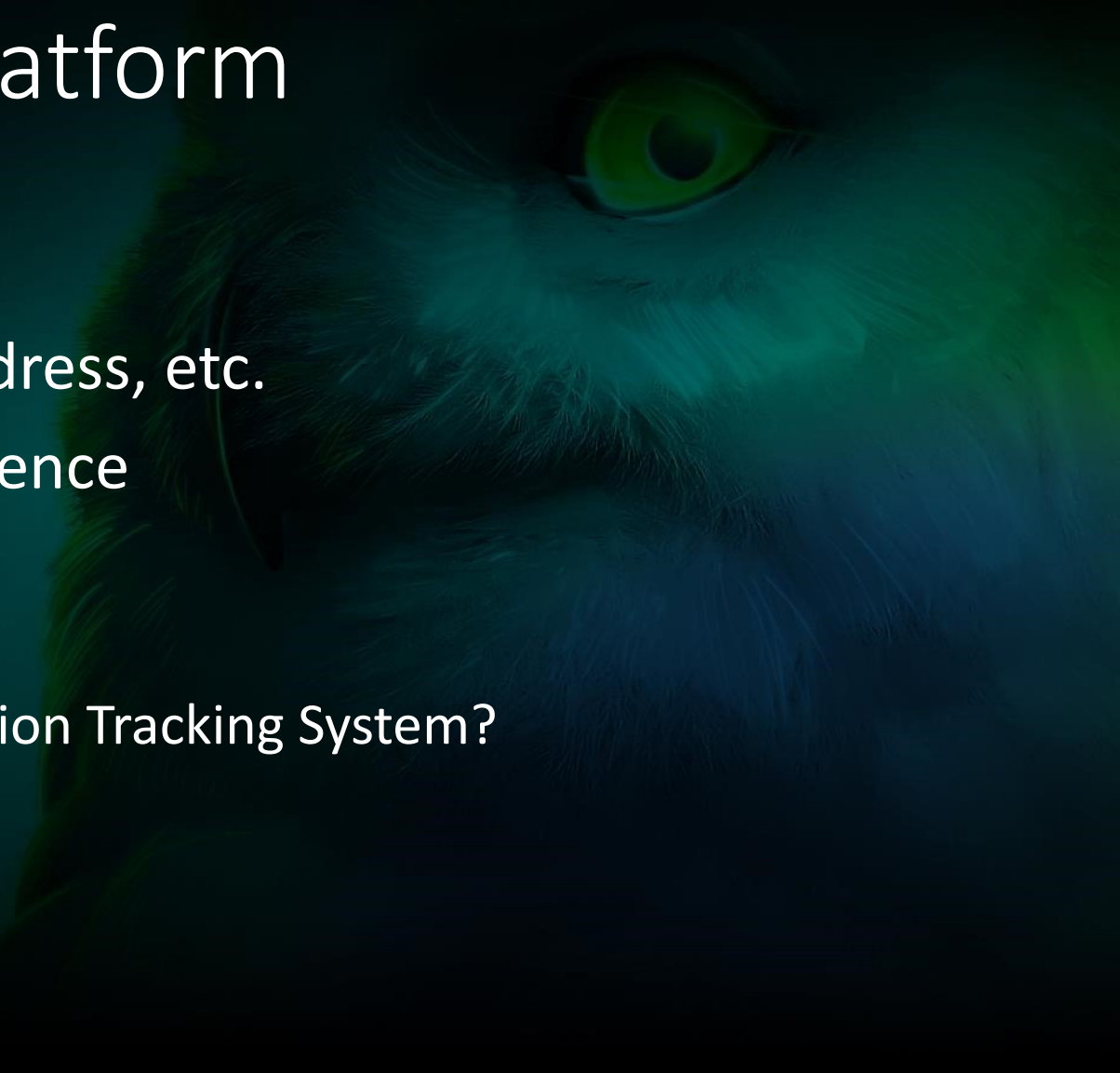
Domestic Public Opinion Tracking System

- Queries registration information on Baidu, Sina, Tianya, etc.
 - Phone number, handle, email address, IP history...
 - Deanonimization of shared links
 - OSINT capabilities?




SkyWalker Data Query Platform

- Another platform, dedicated to PII
- Selectors: name, ID card number, address, etc.
- Reconstructs the target's online presence
- Source of the data unknown.
 - OSINT?
 - Front-end for the Domestic Public Opinion Tracking System?

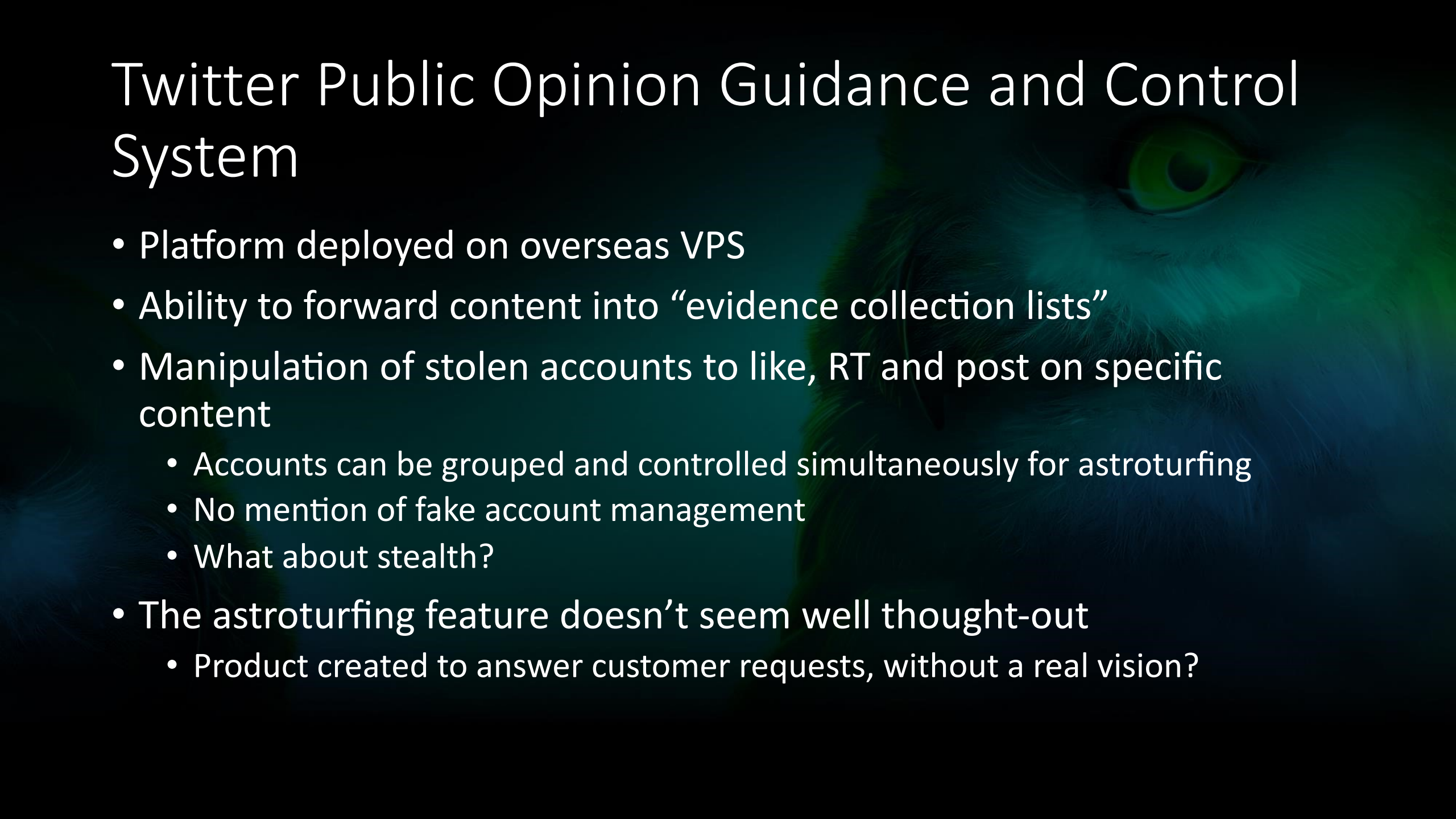


Twitter Public Opinion Guidance and Control System



- Problem statement: “All around supervision of Twitter requires huge resources”
- Objectives:
 - Discovery of bad/illegal opinions
 - Keyword-based search, at account-level only
 - No global monitoring of Twitter
 - Document and counteract opinions overseas
- Similar to the Outlook e-mail extraction product
 - Phishing
 - 2FA & IP check bypass(?)
 - Automated extraction of account information (tweets, DMs, etc.)

Twitter Public Opinion Guidance and Control System



- Platform deployed on overseas VPS
- Ability to forward content into “evidence collection lists”
- Manipulation of stolen accounts to like, RT and post on specific content
 - Accounts can be grouped and controlled simultaneously for astroturfing
 - No mention of fake account management
 - What about stealth?
- The astroturfing feature doesn't seem well thought-out
 - Product created to answer customer requests, without a real vision?

Hints of 0day acquisition

mikrotik's 0day, Gmail acquisition, is it related to ios?

2021-11-30 09:16:37 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 What is the affected firmware version of the Juniper race you gave me before?

2021-11-30 09:18:30 wxid_zb45i0rc71yk21 wxid_12n748um1thl21 Which one?

2021-11-30 09:20:24 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 [20211103-1.txt](#)

2021-11-30 09:20:28 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 3. juniper SRX firewall Name: juniper SRX firewall front desk unconditional RCE Affected versions: SRX300, SRX320, SRX340, SRX345, SRX100, SRX110, SRX110H2, SRX210, SRX220, SRX240, SRX550, SRX650, etc.

2021-11-30 09:20:36 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 Is this it

2021-11-30 09:21:51 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 Implement it

2021-11-30 09:24:23 wxid_zb45i0rc71yk21 wxid_12n748um1thl21 Isn't this a version?

2021-11-30 09:25:02 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 Have you got it yet?

2021-11-30 09:25:10 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 This 0day

2021-11-30 09:25:46 wxid_zb45i0rc71yk21 wxid_12n748um1thl21 Should be there

2021-11-30 09:26:33 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 Should

2021-11-30 09:26:36 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 !!!

2021-11-30 09:26:51 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 Should TMD not be said in your mouth

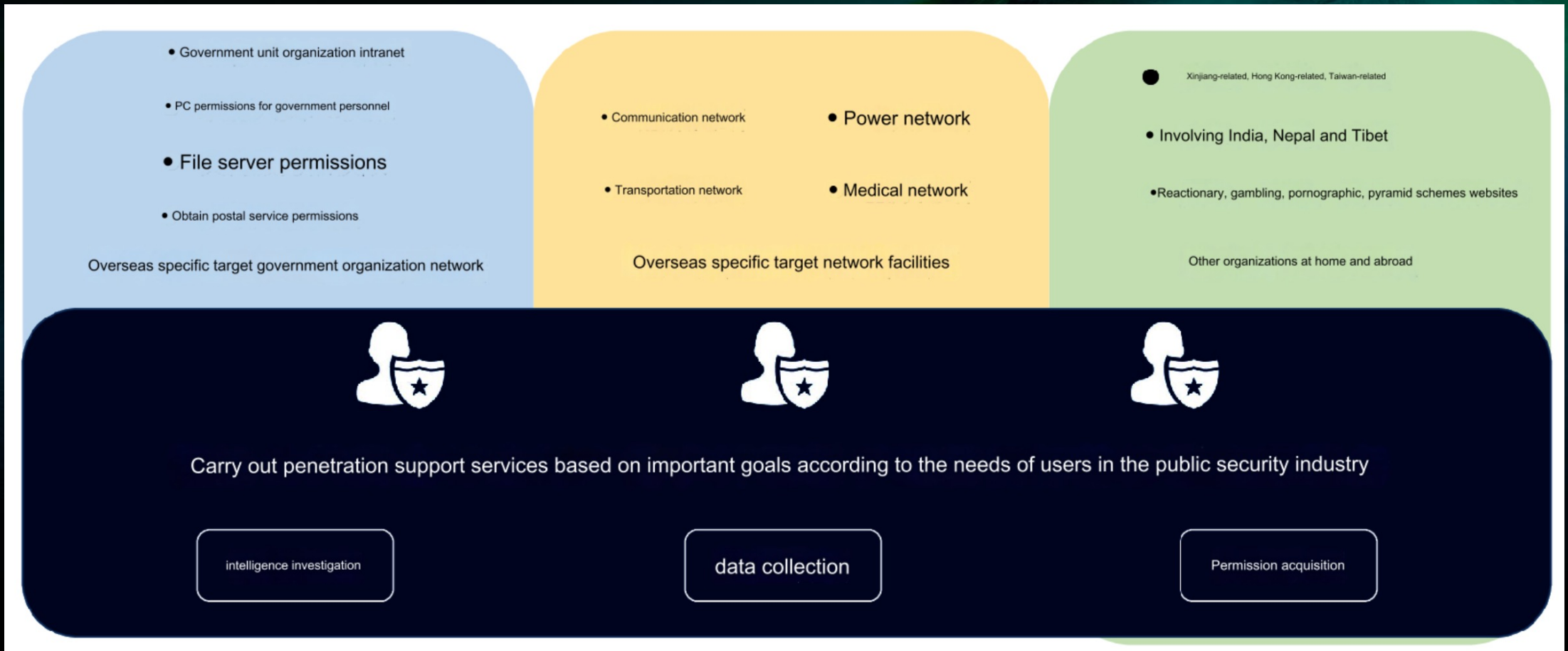
2021-11-30 09:26:57 wxid_12n748um1thl21 wxid_zb45i0rc71yk21 You are so professional

Tianfu Cup 0days

2021-10-26 01:53:17	Shutd0wn	lengmo	The 0DAY loopholes in the Tianfu Cup competition are said to have been given to the POC to the police. Can I get this?
2021-10-26 01:53:49	lengmo	Shutd0wn	If not, I asked that day. The Ministry gave it to Jiangsu
2021-10-26 01:53:59	lengmo	Shutd0wn	Given every year
2021-10-26 01:54:17	lengmo	Shutd0wn	It is said that some loopholes are relatively useless
2021-10-26 01:54:37	lengmo	Shutd0wn	I can only see if there is any prefecture or city in the hall
2021-10-26 01:55:36	Shutd0wn	lengmo	It is said that the Ministry of Public Security obtained the POC, and it takes some effort to write it into EXP
2021-10-26 01:56:09	Shutd0wn	lengmo	For vulnerabilities like IOS, it is not easy to make EXP even if you know the POC
2021-10-26 01:56:13	lengmo	Shutd0wn	I talked about it during dinner that day
2021-10-26 01:56:18	lengmo	Shutd0wn	Let me ask
2021-10-26 01:56:54	lengmo	Shutd0wn	The provincial department seems to have given it to Wuxi
2021-10-26 01:57:07	lengmo	Shutd0wn	This was mentioned in our training that day
2021-10-26 01:57:24	Shutd0wn	lengmo	Well, please pay attention, we will ask for a copy when they spread.
2021-10-26 01:57:31	Shutd0wn	lengmo	It will be nothing if it spreads
2021-10-26 01:57:57	lengmo	Shutd0wn	Well, okay 🙄

Victims

- 71 entities (government, energy, universities, airlines, telcos, ...)

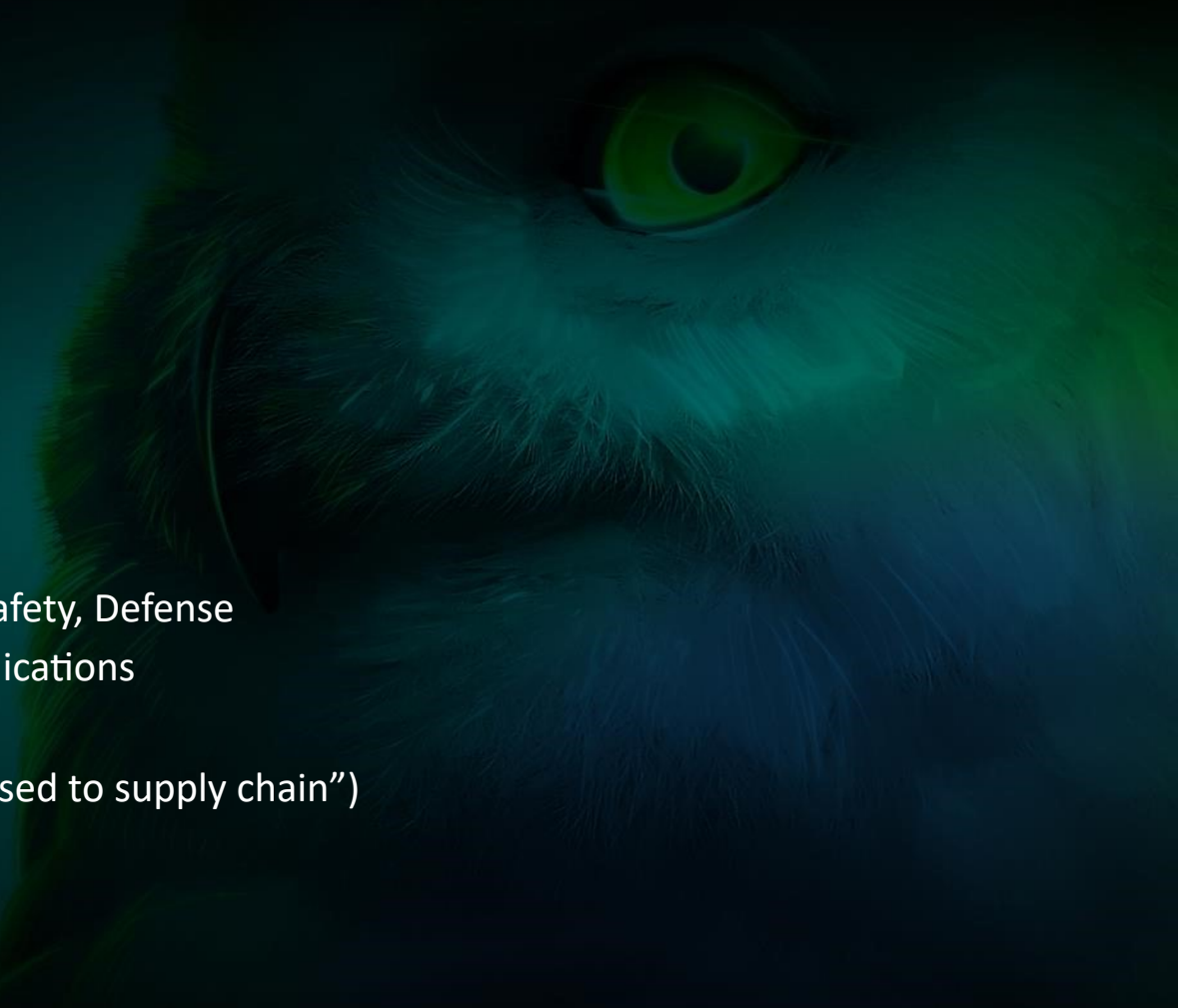


Victims (not exhaustive)

- Document: cooperation proposal with Bazhou (Xinjiang) Province Security Bureau
 - “Based on our company's APT work for more than ten years, we have controlled various types of server permissions and intranet permissions in multiple countries.”
 - Pakistan
 - Punjab Anti-Terrorism Center
 - Pakistani government postal service
 - Punjab Police Postal Service
 - Perouz Police Station Post Service
 - Zong (mobile operator)
 - Afghanistan
 - National Security Council intranet
 - Postal service
 - Southeast Asia Anti-Terrorism Center postal service
 - Kyrgyzstan
 - Diplomatic Oil Service, National Security Council Oil Service
 - Megacom

Victims

- Malaysia
 - Ministry of Foreign Affairs and Interior
 - Military Network
- Thailand
 - Prime Minister's Office
 - National Intelligence Agency
 - Ministries of Finance and Commerce, Digital Economy and Safety, Defense
 - Armed Forces Preparatory School & Thai Army HQ, Communications
 - Navy & Railway
 - Thailand Royal Government Development Agency (“can be used to supply chain”)
- Mongolia
 - Ministry of Foreign Affairs and Police
 - Mongolia Telecom & Skytel
- Taiwan
 - National Taxation Bureau of Taipei
 - Ministry of Foreign Affairs



Victims

- Kazakhstan
 - Kcell and Beeline (mobile operators)
 - RDP access to “Defense Mail Service”
- India
 - Ministries of Foreign & Home Affairs, Defense, Finance
 - Apollo Hospital
- Nepal
 - Presidential Palace
 - National Defense
 - Foreign Affairs
- Domestic
 - Gambling websites
 - Uyghur minority



Victims

- Vietnam
 - Unspecified telecom operator
 - Chiang Mai University
 - Academy of Social Sciences
- Myanmar
 - Myanmar Post and Telecommunications
- South Korea
 - Sejong Research Institute Cultural Services
- Philippines
 - Navy Postal Service



Victims (or targets?)

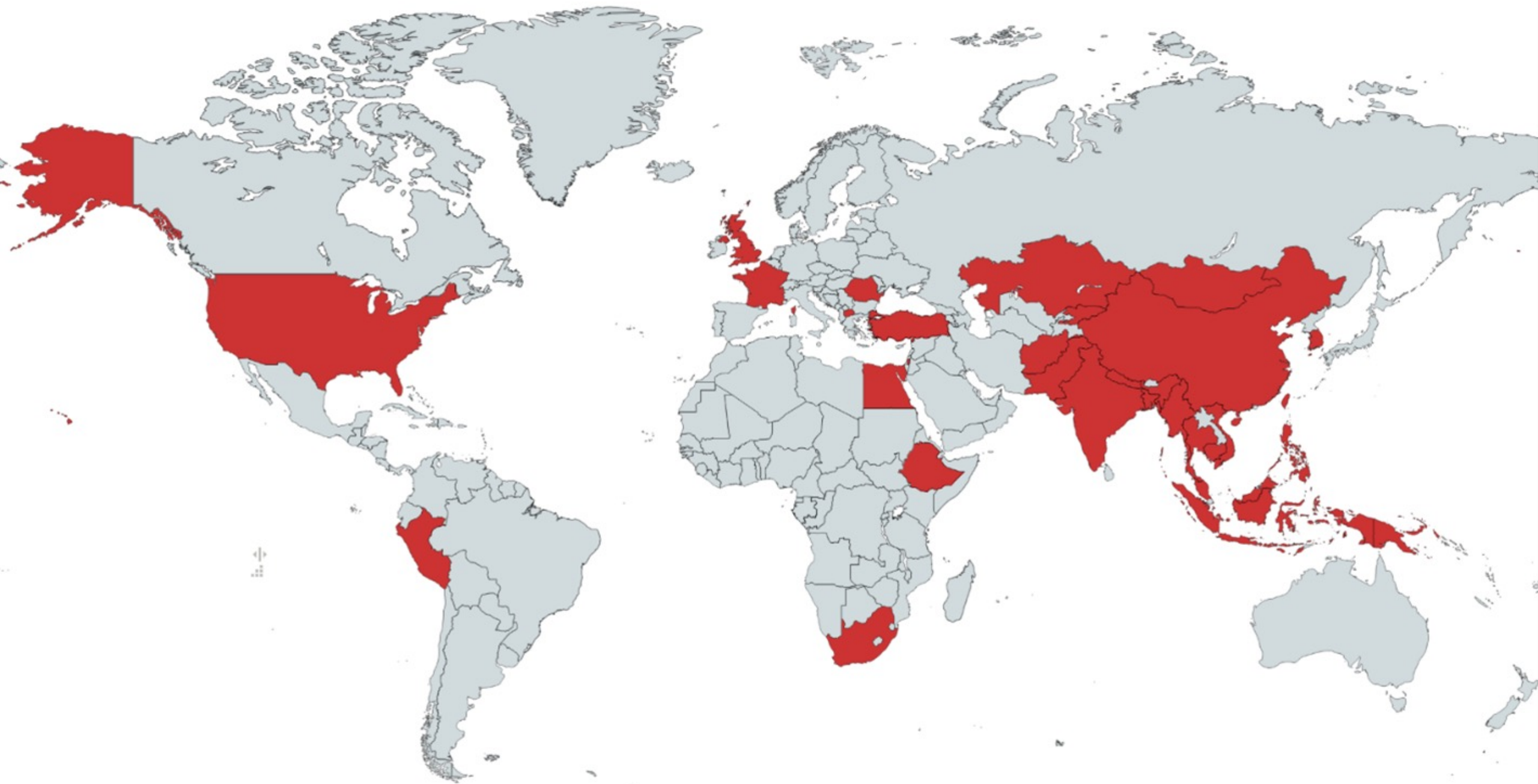
- United Kingdom
 - Home office
 - ~~Ministry of Foreign Affairs~~ (already taken by another contractor)
 - British treasury
 - Department for Business, Energy and Industrial Strategy; Environment, Food and Rural Affairs; Health and Social Care
 - UK National Crime Agency
 - Center for Foreign Policy Studies
 - Chatham House
- USA
 - Center for Foreign Policy Studies
- France
 - Sciences Po
- NGOs
 - Human Rights Watch
 - Amnesty International
 - RAND Institute Europe



Victims

- Macedonia
 - Secretariat of European Affairs
- Airlines (PNR)
 - AirAstana Airlines Company
 - Air Macau
 - Vietnam Airlines
- New regions in 2022:
 - Afghanistan
 - Syria
 - Uzbekistan
 - Iran





CDR extraction from telcos

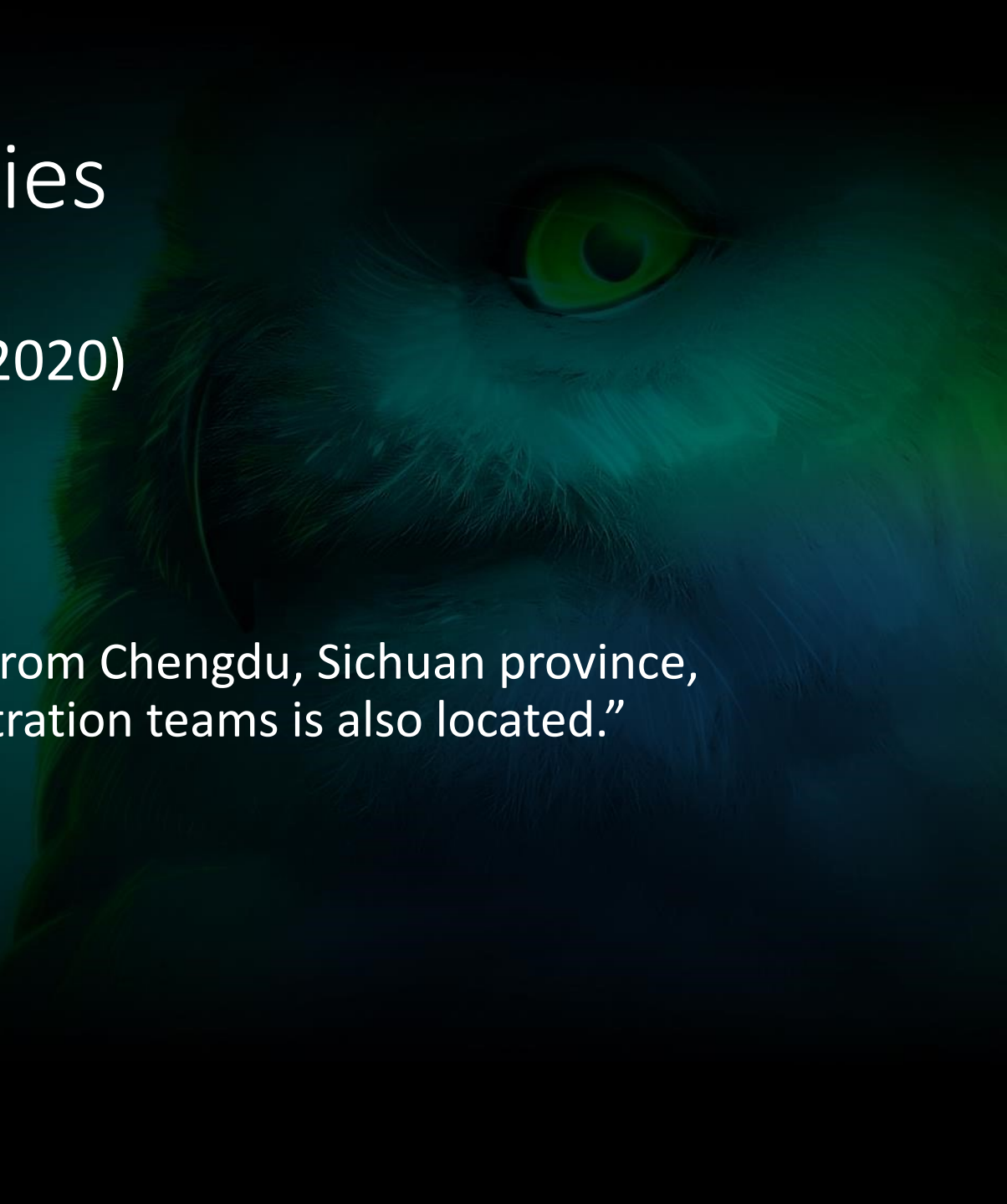
CALL_TYPE_ID	A_NUMBER	B_NUMBER	CALL_DATE	DURATION	RATE_DATE	IMEI	SERVED_LOCATION	CELL_ID	TARIFF_ID	UPLINK	DOWNLINK	BRAND_ID	SERVED_ZONE_ID	DESTINATION_ID
77	77010155050	87782835050	2020-04-01 20:06:42	55	2020-04-01 20:07:36	35484409231712	LAC_77010004212	6345	817	0	0	2	476	50079
416	77010155050	internet	2020-04-01 10:13:03	0	2020-04-02 03:24:56	35484409231712	LAC_40102-13252-138595962	183779	817	0	131703516	2	1	34946
416	77010155050	internet	2020-04-01 09:07:05	0	2020-04-01 09:59:21	35484409231712	LAC_40102-13252-138572156	158997	817	0	41892	2	1	34946
416	77010155050	internet	2020-04-01 08:57:08	0	2020-04-01 09:59:21	35484409231712	LAC_40102-13252-138572156	158997	817	0	385043	2	1	34946
416	77010155050	internet	2020-04-01 03:07:04	0	2020-04-01 09:07:04	35484409231712	LAC_40102-13252-138595962	183779	817	0	295618	2	1	34946
416	77010155050	internet	2020-04-01 08:57:08	0	2020-04-01 09:59:21	35484409231712	LAC_40102-13252-138572156	158997	817	0	1471315	2	1	34946
416	77010155050	internet	2020-04-01 10:04:21	0	2020-04-02 03:24:56	35484409231712	LAC_40102-13252-138595962	183779	817	0	135070013	2	1	34946
77	77010155050	87787949194	2020-04-01 20:41:47	27	2020-04-01 20:42:14	35484409231712	LAC_77010004212	6345	817	0	0	2	476	50079
416	77010155050	internet	2020-04-01 04:57:08	0	2020-04-01 08:57:08	35484409231712	LAC_40102-13252-138595962	183779	817	0	2566838	2	1	34946
416	77010155050	internet	2020-04-01 10:13:05	0	2020-04-02 03:24:56	35484409231712	LAC_40102-13252-138595962	183779	817	0	264006124	2	1	34946
77	77010155050	87782835050	2020-04-01 20:12:59	31	2020-04-01 20:13:29	35484409231712	LAC_77010004212	6345	817	0	0	2	476	50079
182	77010155050	internet	2020-04-01 01:06:34	0	2020-04-01 09:11:44	35484409231712	LAC_40102-13252-65535	-99	817	0	247013646	2	1	34946
416	77010155050	internet	2020-04-01 09:59:26	0	2020-04-02 03:24:56	35484409231712	LAC_40102-13252-138595962	183779	817	0	46431690	2	1	34946
416	77010155050	internet	2020-04-01 04:57:08	0	2020-04-01 08:57:08	35484409231712	LAC_40102-13252-138595962	183779	817	0	2573013	2	1	34946
192	77010155050	77023905414	2020-04-01 14:05:28	40	2020-04-01 14:08:25	35484409231712	LAC_77010004203	100658	817	0	0	2	396	3681
103	77010155050		2020-04-01 00:00:00	0	2020-04-01 00:07:44			-101	817	0	0	2	-101	-101
416	77010155050	internet	2020-04-01 17:34:57	0	2020-04-02 03:24:56	35484409231712	LAC_40102-13252-138595962	183779	817	0	35351188	2	1	34946
416	77010155050	internet	2020-04-02 09:59:33	0	2020-04-03 04:02:04	35484409231712	LAC_40102-13252-138595962	183779	817	0	2777178	2	1	34946
416	77010155050	internet	2020-04-02 08:50:18	0	2020-04-02 09:59:26	35484409231712	LAC_40102-13251-138656622	143511	817	0	15286	2	1	34946
192	77010155050	77010495050	2020-04-02 15:55:25	53	2020-04-02 15:59:22	35484409231712	LAC_77010004203	186067	817	0	0	2	396	3404
192	77010155050	77023905414	2020-04-02 20:04:07	36	2020-04-02 20:08:21	35484409231712	LAC_77010004203	186067	817	0	0	2	396	3681
192	77010155050	77023905414	2020-04-02 17:15:28	68	2020-04-02 17:19:10	35484409231712	LAC_77010004203	6345	817	0	0	2	396	3681
416	77010155050	internet	2020-04-02 08:50:18	0	2020-04-02 09:59:26	35484409231712	LAC_40102-13251-138656622	143511	817	0	60973	2	1	34946
416	77010155050	internet	2020-04-02 08:50:18	0	2020-04-02 09:59:26	35484409231712	LAC_40102-13251-138656622	143511	817	0	661446	2	1	34946
77	77010155050	77022710784	2020-04-02 12:58:36	724	2020-04-02 13:10:39	35484409231712	LAC_77010004212	124175	817	0	0	2	476	3681
127	77010155050	internet	2020-04-02 03:24:56	0	2020-04-02 08:50:17	35484409231712	LAC_40102-13252-6322	186067	817	0	30851	2	1	34946
416	77010155050	internet	2020-04-02 08:50:18	0	2020-04-02 09:59:26	35484409231712	LAC_40102-13251-138656622	143511	817	0	65915	2	1	34946
127	77010155050	internet	2020-04-02 03:24:56	0	2020-04-02 08:50:17	35484409231712	LAC_40102-13252-6322	186067	817	0	12629	2	1	34946
416	77010155050	internet	2020-04-02 10:14:24	0	2020-04-03 04:02:04	35484409231712	LAC_40102-13252-138595962	183779	817	0	9657272	2	1	34946
192	77010155050	77023905414	2020-04-02 20:53:43	24	2020-04-02 21:00:16	35484409231712	LAC_77010004203	124526	817	0	0	2	396	3681
103	77010155050		2020-04-02 00:00:00	0	2020-04-02 00:07:38			-101	817	0	0	2	-101	-101
416	77010155050	internet	2020-04-03 20:18:26	0	2020-04-04 03:27:23	35484409231712	LAC_40102-13253-138580848	142997	817	0	2850006	2	1	34946
416	77010155050	internet	2020-04-03 19:20:27	0	2020-04-04 03:27:23	35484409231712	LAC_40102-13253-138580848	142997	817	0	109355	2	1	34946
182	77010155050	internet	2020-04-03 10:00:55	0	2020-04-03 10:52:51	35484409231712	LAC_40102-13252-4074	124211	817	0	1437	2	1	34946
416	77010155050	internet	2020-04-03 11:55:29	0	2020-04-04 03:27:23	35484409231712	LAC_40102-13253-138580848	142997	817	0	1111728	2	1	34946
192	77010155050	77017007999	2020-04-03 10:52:41	108	2020-04-03 10:57:17	35484409231712	LAC_77010004203	124211	817	0	0	2	396	3404
192	77010155050	77010495050	2020-04-03 10:38:54	64	2020-04-03 10:44:22	35484409231712	LAC_77010004203	186067	817	0	0	2	396	3404
416	77010155050	internet	2020-04-03 10:54:14	0	2020-04-04 03:27:23	35484409231712	LAC_40102-13253-138580848	142997	817	0	69663580	2	1	34946
416	77010155050	internet	2020-04-03 10:58:35	0	2020-04-04 03:27:23	35484409231712	LAC_40102-13253-138580848	142997	817	0	33830926	2	1	34946
77	77010155050	77710100009	2020-04-03 22:03:44	29	2020-04-03 22:04:13	35484409231712	LAC_77010004212	124436	817	0	0	2	476	34631
182	77010155050	internet	2020-04-03 10:01:11	0	2020-04-03 10:52:51	35484409231712	LAC_40102-13252-4074	124211	817	0	24938	2	1	34946

BTS listing

158997	ERICSSON	ERBS_41297_USHILYAEV2_KB	541297-124	Г.Шымкент	13252	138572156	Южно-Ка: Шымкент Шымкент	511010000			2	South
124436	ERICSSON	41286MEGAIND	2MEGA7	Г.Шымкент	13251	12867	Южно-Ка: Шымкент Шымкент	511010000	69.5961	42.31909972	2	South
124211	ERICSSON	41297USHILYAEV2	EB2974	Г.Шымкент	13252	4074	Южно-Ка: Шымкент Шымкент	511010000	69.610105	42.318360	2	South
53048	ERICSSON	42502MADANIKCTW	5MADAN1	С.Мадани	17255	5021	-99 Южно-Ка: Толебийс Шымкент	515845100	70.07127778	42.33530556	2	South
6141	ERICSSON	41126SHKOKTEM	2KOKTE2	Г.Шымкент	13252	1192	31 Южно-Ка: Шымкент Шымкент	511010000	69.63764889	42.33018778	2	South
101639	ERICSSON	41162BCASTANA	2UKUNA2	Г.Шымкент	13252	1292	Южно-Ка: Шымкент Шымкент	511010000	69.602358	42.334356	2	South
10698	ERICSSON	41010AUEZOVUNIV	2SAUEZ2	Г.Шымкент	13252	222	31 Южно-Ка: Шымкент Шымкент	511010000	69.59966389	42.33180167	2	South
142816	ERICSSON	ERBS_41627_SHM_Sapar_BK	541627-102	Г.Шымкент	13251	138656614	Южно-Ка: Шымкент Шымкент	511010000	69.599161	42.322222	2	South
142211	ERICSSON	ERBS_45070_KZTOKTYBA_KB	L8_KZL_45070KZTOKTYBA-30	Г.Кызылорда	11001	139537950	Кызылорд Кызылорд Кызылорд	431010000	65.486176	44.841192	2	South
142480	ERICSSON	ERBS_00913_ALM_Business_BK	L18_ALM_business-12	Г.Алматы	30012	128233740	Алматы Г. Алматы Г. Алматы	750000000	76.8911	43.239162	1	Almaty
142160	ERICSSON	ERBS_81170_URL_Avanguard_BK	581170-100	Г.Уральск	2003	148779620	Западно-Уральск Г. Уральск	271010000	51.352222	51.211942	4	West
142373	ERICSSON	ERBS_45032_KYZORDAHOT_KB	545032-102	Г.Кызылорда	3246	139528294	Кызылорд Кызылорд Кызылорд	431010000	65.494759	44.843177	2	South
143475	ERICSSON	ERBS_71116_TEMIRBETON_KB	L8_AKT_71116TEMIRBETON-10	Г.Актобе	24001	146205706	Актюбинс Актобе Г. Актобе	151010000	57.178109	50.299058	4	West
142093	ERICSSON	ERBS_71157_GAZTEPLO_KB	571157-110	Г.Актобе	3017	146216302	Актюбинс Актобе Г. Актобе	151010000	57.124293	50.317962	4	West
98379	ERICSSON	42249BADAM	EC2491	С.Бадам	47251	29791	Южно-Ка: Ордабась Шымкент	514633100	69.260237	42.382990	2	South
97096	ERICSSON	42600IKANUMID	EC6006	С.Сузак	17266	26006	Южно-Ка: Сузакский Туркестан	515647100	68.515720	43.191741	2	South
97402	ERICSSON	41133USHALADDIN	EB1336	С.Аксу	17253	4206	Южно-Ка: Сайрамск Шымкент	515230100	69.827492	42.419801	2	South
97296	ERICSSON	42179UXARYSKALJ	EC1798	Г.Арысь	47253	21178	Южно-Ка: Арысь Г.А Шымкент	511610000	68.792996	42.407109	2	South
99937	ERICSSON	43043TRGLUHOY	ED0437	Г.Тараз	7274	1707	Жамбылс Тараз Г.А. Тараз	311010000	71.398516	42.892578	2	South
97003	ERICSSON	42605TLBTOGYS	EC6056	С.Маятас	17255	33306	Южно-Ка: Толебийс Шымкент	515849600	69.805133	42.221832	2	South
69617	ERICSSON	11790SAURSEVEN	USAURS3	Г.Астана	43172	17903	Астана Г. Астана Г. Астана	711000000	71.417270	51.119063	8	Astana
69562	ZTE	32110AKSUSTR0Y	UAKST6	Г.Аксу	1304	32216	Павлодар Аксу Г.А. Павлодар	551610000			7	East
69799	ERICSSON	44243SARYBEGEI	BEGEI1	С.Сарыкемер	7262	44431	Жамбылс Байзакски Тараз	313630100	71.51365278	43.01414167	2	South
69742	ERICSSON	42654BAYALDYR	BAYAL3	С.Баялдыр	17257	26543	Южно-Ка: Кентау Г. Туркестан	512035100	68.27608306	42.82811111	2	South
69594	ERICSSON	24078SHATALYUKA	DZHSH3	Г.Жезказган	3102	40783	Караганди Жезказган Караганди	351810000	67.51411111	47.91097778	3	North
69648	ERICSSON	43176TRBOLASHAK	BOLAS8	Г.Тараз	7262	31768	Жамбылс Тараз Г.А. Тараз	311010000			2	South
3141	ERICSSON	11415AGALAU	UASAGA2	Г.Астана	43172	14152	12 Астана Г. Астана Г. Астана	711000000	71.413407	51.118602	8	Astana
3142	ERICSSON	11416XKORME	UKORM6	Г.Астана	43172	14166	12 Астана Г. Астана Г. Астана	711000000	71.420703	51.127903	8	Astana
3143	ERICSSON	11416XKORME	UKORM7	Г.Астана	43172	14167	12 Астана Г. Астана Г. Астана	711000000	71.420703	51.127903	8	Astana
3144	ERICSSON	11416XKORME	UKORM8	Г.Астана	43172	14168	12 Астана Г. Астана Г. Астана	711000000	71.420703	51.127903	8	Astana
3145	ERICSSON	11419STREET66	5STRET1	Г.Астана	53172	14191	13 Астана Г. Астана Г. Астана	711000000	71.46613889	51.13069444	8	Astana
3146	ERICSSON	11419STREET66	5STRET2	Г.Астана	53172	14192	13 Астана Г. Астана Г. Астана	711000000	71.46613889	51.13069444	8	Astana
3147	ERICSSON	11419STREET66	5STRET3	Г.Астана	53172	14193	13 Астана Г. Астана Г. Астана	711000000	71.46613889	51.13069444	8	Astana
3148	ERICSSON	11421PROMZONA	5PRMZ1	Г.Астана	53172	14211	13 Астана Г. Астана Г. Астана	711000000	71.52894444	51.12641667	8	Astana
3149	ERICSSON	11421PROMZONA	5PRMZ2	Г.Астана	53172	14212	13 Астана Г. Астана Г. Астана	711000000	71.52894444	51.12641667	8	Astana
104950	ERICSSON	11696NAZUNTEPLO	B86968	Г.Астана	43173	6038	Астана Г. Астана Г. Астана	711000000	71.398559	51.094140	8	Astana
104687	ERICSSON	11866PARADISE	1UPARD1C	Г.Астана	13173	38661	Астана Г. Астана Г. Астана	711000000	71.453598	51.177599	8	Astana
104755	ERICSSON	11930EIFELTOWER	3UILEF7	Г.Астана	33172	19307	Астана Г. Астана Г. Астана	711000000	71.252968	51.124964	8	Astana
104473	ERICSSON	11509ASKORGAN	UASKOR2	Г.Астана	47173	8042	Астана Г. Астана Г. Астана	711000000	71.338456	51.177374	8	Astana
107870	ERICSSON	11951ZANGAR	SUZANG8	Г.Астана	53174	19518	Астана Г. Астана Г. Астана	711000000	71.553762	51.146239	8	Astana
106871	ERICSSON	11774ASKFC	1USKFC2	Г.Астана	13173	4312	Астана Г. Астана Г. Астана	711000000	71.428535	51.159672	8	Astana
104801	ERICSSON	11911SPETSTSON	USPSON1	Г.Астана	47173	19111	Астана Г. Астана Г. Астана	711000000	71.318049	51.207587	8	Astana
105543	ERICSSON	11628XLOMONOS	B86283D	Г.Астана	13173	36288	Астана Г. Астана Г. Астана	711000000	71.452053	51.167825	8	Astana

Links to know APT activities

- ESET: Fishmonger (HK universities, ~2020)
- Trend Micro: Earth Lusca
 - Same targeting
 - Use of ShadowPad and Winnti
 - “Earth Lusca’s source IP addresses are from Chengdu, Sichuan province, where the main office of I-Soon’s penetration teams is also located.”
- Recorded Future: RedHotel
- Citizen Lab: POISON CARP



Time	From	To
2023-01-09 02:28:07	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 02:28:14	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 02:28:18	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 02:36:19	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 02:36:25	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 02:43:51	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 02:44:06	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 02:44:09	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 02:44:20	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 02:44:33	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 02:44:51	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 02:44:58	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 02:48:54	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 02:52:01	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 02:52:03	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 02:55:53	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 02:55:56	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 02:56:36	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 03:01:26	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 03:02:07	wxid_hlmnhsq64tt722	wxid_12n748um1thl21
2023-01-09 03:02:26	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 07:25:16	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 07:25:29	wxid_12n748um1thl21	wxid_hlmnhsq64tt722
2023-01-09 07:57:13	wxid_hlmnhsq64tt722	wxid_12n748um1thl21

Wait a minute, there is something wrong with the platform
 Okay
<https://74.120.172.10:10092/home>
 access OrFRXV LZtestUser lzqzmp@123
 Send a demo video
 No need to give this information
 [呲呲呲]
 This is Microsoft's trial version
 Well, I saw it
 Is there a demonstration video from Microsoft?
 Let me ask
[Microsoft Email Encryption Platform.7z](#)
 Is your video wrong?
 I can't open
 Huh?
 Just decompress it
 I guess I didn't watch the video
 There is also Android remote control
 Android wait a moment, there is a problem
 Good
[202301090144.pdf](#)
 Look, can we do it?
 It can be done. Only the agent needs to be tested

Resolutions (5)

Resolve	First seen	Last seen
www.mailteso.online	2021-05-30	2023-12-30
mailteso.online	2020-09-22	2023-12-29
74.120.172.10.16clouds.com	2021-01-01	2023-10-11
hds45k4lch1xdzvc1h4xik6zf53a9999.brqdc4uev	2022-10-28	2022-10-28
mailnotes.online	2021-08-09	2022-07-08



<https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/>

2022-06-13 04:50:20	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Yeah
2022-06-13 04:50:28	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Call anytime
2022-06-13 04:50:32	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	What do you need me to do
2022-06-13 07:39:19	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Asking about personal PC access in Yangzhou
2022-06-13 07:39:21	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	[Face covering]
2022-06-13 07:39:23	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Can I give it now
2022-06-13 07:40:26	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	【Caibaobao】 【acting】 8.218.67.52:27011 【TCP Tunnel】 8.218.67.52:17011 【account】 admin 【password】 88888888
2022-06-13 07:40:34	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Yeah
2022-06-13 07:40:37	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	My day
2022-06-13 07:40:44	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	
2022-06-13 07:40:54	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	This server is in Hong Kong
2022-06-13 07:41:06	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	You don't care
2022-06-13 07:41:07	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	domain access result(1).csv
2022-06-13 07:41:11	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Hmm
2022-06-13 07:41:14	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	This server is ours
2022-06-13 07:41:20	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	No
2022-06-13 07:41:24	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	I mean the spinach in the morning
2022-06-13 07:41:45	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	Our springboard server
2022-06-13 07:41:47	wxid_zb45i0rc71yk21	wxid_c9yv0nsla3yn22	Oh oh
2022-06-13 07:41:58	wxid_c9yv0nsla3yn22	wxid_zb45i0rc71yk21	Needed

3. Gets machine information, such as the following:

- IP address
- Device name
- Username
- Running process name
- Windows product name
- Events with event ID 6005 (the event log service was started), events with Event ID 6006 (the event log service was stopped)
- Any TCP endpoints listening on ports 8090, 8091, 8092, 8093, 8094, 8095, 8096
- Any TCP endpoint established to 8.218.67.52:18024
- Antivirus product name
- If Skype or Telegram is installed
- Number of connected monitors
- Product ID value from Windows registry

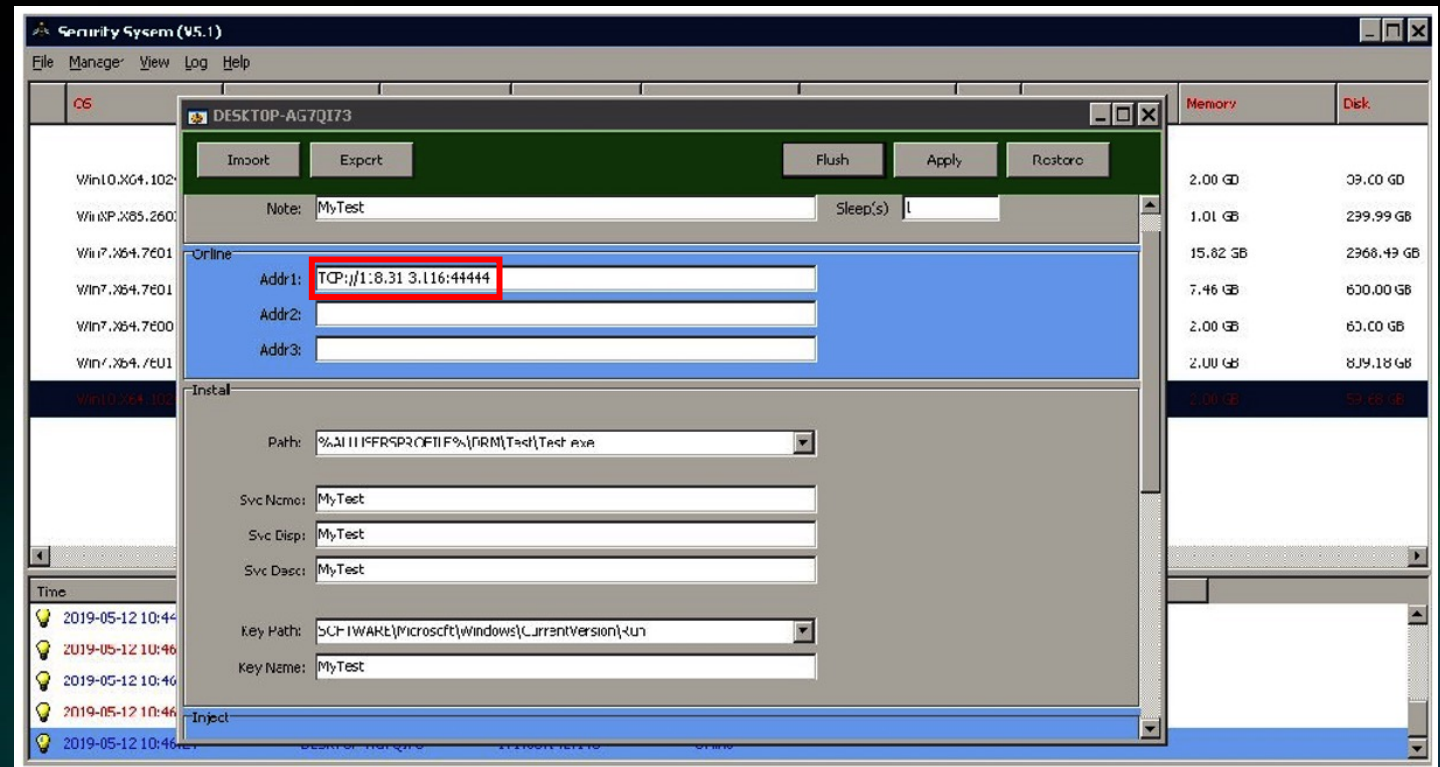
Source (Sep. 2022):
https://www.trendmicro.com/en_sg/research/22/l/p/robing-weaponized-chat-applications-abused-in-supply-chain-atta.html

ShadowPad

COMMAND & CONTROL

ShadowPad C&C Servers - IP addresses:

1.56.32[.]13
101.78.177[.]244
103.19.3[.]17
103.19.3[.]43
103.19.3[.]44
103.243.181[.]105
103.255.179[.]186
112.121.178[.]90
114.67.230[.]197
117.16.142[.]35
117.16.142[.]9
118.31.3[.]116
125.65.40[.]163
128.14.173[.]60
129.211.135[.]27
154.202.198[.]246
154.223.179[.]14
172.104.43[.]172
172.193.44[.]8
172.197.18[.]30



ADVANCED PERSISTENT THREAT

ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage

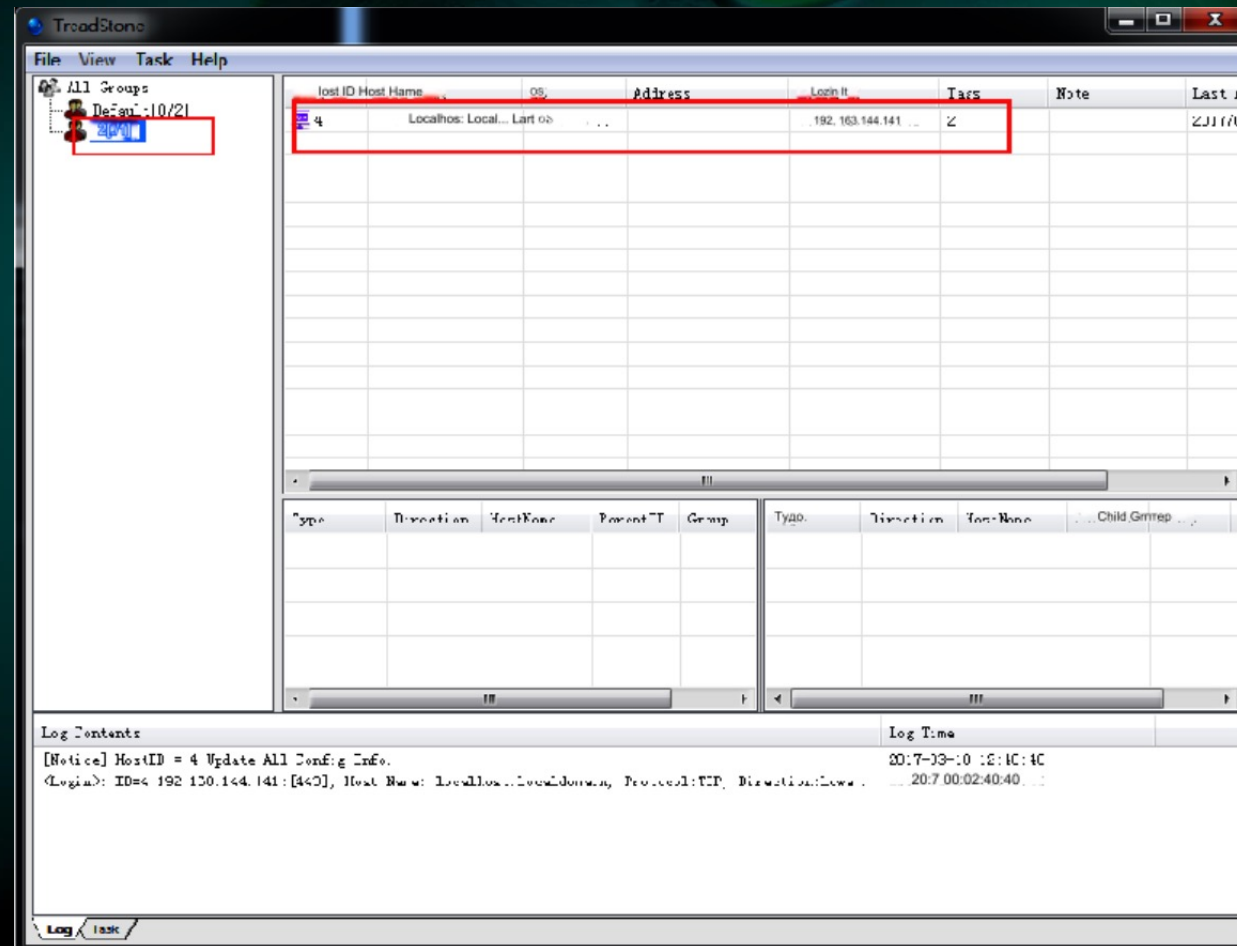
YI-JHEN HSIEH / AUGUST 19, 2021

By Yi-Jhen Hsieh & Joey Chen

Source: <https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/>

Linux RAT

- Features:
 - Command execution
 - File management
 - SOCKS5 proxying
 - TCP port reuse for communications
- “TreadStone”
 - Mentioned in the Chengdu 404 indictment
 - Controller for Winnti



Lawsuit from Chengdu 404

- Chengdu 404 = APT41 (US DoJ)
- No details about the complaint
- Implies business connections between the two companies

案由	计算机软件合同纠纷	←→	Computer software development dispute
案号	(2023)川01知民初457号	开庭时间	2023-10-17 09:30:00
当事人信息	原告-成都市肆零网络科技有限公司	←→	Plaintiff: Chengdu 404
	被告-四川安询信息技术有限公司	←→	Defendant: Sichuan i-SOON
开庭法院	成都市中级人民法院	法庭	成都知识产权审判庭第二法庭
承办部门		主审人	C某某

Chengdu 404 == APT41 confirmed by I-Soon

2020-09-16 23:51:18	lengmo	Shutd0wn	FBI adds 5 Chinese APT41 hackers to its Cyber's Most Wanted List
2020-09-16 23:51:42	lengmo	Shutd0wn	Fuck
2020-09-16 23:51:44	lengmo	Shutd0wn	Fuck
2020-09-16 23:51:47	lengmo	Shutd0wn	Something happened
2020-09-16 23:51:53	lengmo	Shutd0wn	404 was exploded
2020-09-16 23:52:05	Shutd0wn	lengmo	Awesome
2020-09-16 23:52:26	lengmo	Shutd0wn	My day
2020-09-16 23:52:30	lengmo	Shutd0wn	All photos
2020-09-16 23:52:37	Shutd0wn	lengmo	Hahahahaha
2020-09-16 23:53:24	Shutd0wn	lengmo	No. 41
2020-09-16 23:53:38	Shutd0wn	lengmo	Tell them to drink 41 drinks next time

Non-poaching agreement with Chengdu 404

2020-09-24 04:30:15	lengmo	Shutd0wn	😬😬404, who is engaged in security development and research, submitted his resume
2020-09-24 04:30:18	lengmo	Shutd0wn	Embarrassing
2020-09-24 04:30:28	lengmo	Shutd0wn	Recruit or not
2020-09-24 04:30:46	Shutd0wn	lengmo	Recruit
2020-09-24 04:31:21	lengmo	Shutd0wn	What are the risks involved in the research?
2020-09-24 04:31:24	lengmo	Shutd0wn	Asking me
2020-09-24 04:31:42	Shutd0wn	lengmo	What does this person do, it doesn't matter if it doesn't involve business
2020-09-24 04:31:57	lengmo	Shutd0wn	Technical person
2020-09-24 04:32:12	lengmo	Shutd0wn	The development of some tools and 🐶
2020-09-24 04:48:18	lengmo	Shutd0wn	Still a girl
2020-09-24 04:48:22	lengmo	Shutd0wn	Fresh graduates
2020-09-24 04:48:29	lengmo	Shutd0wn	Looking pretty good, Ji Yunhui is very excited
2020-09-24 04:48:44	Shutd0wn	lengmo	Haha
2020-09-24 04:49:05	Shutd0wn	lengmo	Do you have any photos?
2020-09-24 04:49:19	lengmo	Shutd0wn	HR and I emphasized that 404 is mainly not for us to take the initiative to recruit people. This is not possible and cannot be done. They actively submitted it and can be recruited

Negative feedback

- Sales:
 - Products don't receive enough updates
 - Poor delivery quality & negative feedback from customers
 - Sales process is too complex, disorganized channel pipeline
- Salary issues
 - 2,000¥/mo (\approx 250€/mo, secretary); 5,000-8,000¥/mo on average?

2020-08-19 04:18:43	lengmo	Shutd0wn	Embarrassing, another piece of technology was poached by Qi Anxin from Xiaoliang's case
2020-08-19 04:19:08	lengmo	Shutd0wn	In our 7K, Qi Anxin gives 12K
2020-08-19 04:19:19	Shutd0wn	lengmo	Awesome, I dug a few
2020-08-19 04:19:37	Shutd0wn	lengmo	Which department of Qi Anxin did you go to? It should not be the public security line
2020-08-19 04:20:33	lengmo	Shutd0wn	3-4
2020-08-19 04:20:42	lengmo	Shutd0wn	Our salary level is really embarrassing

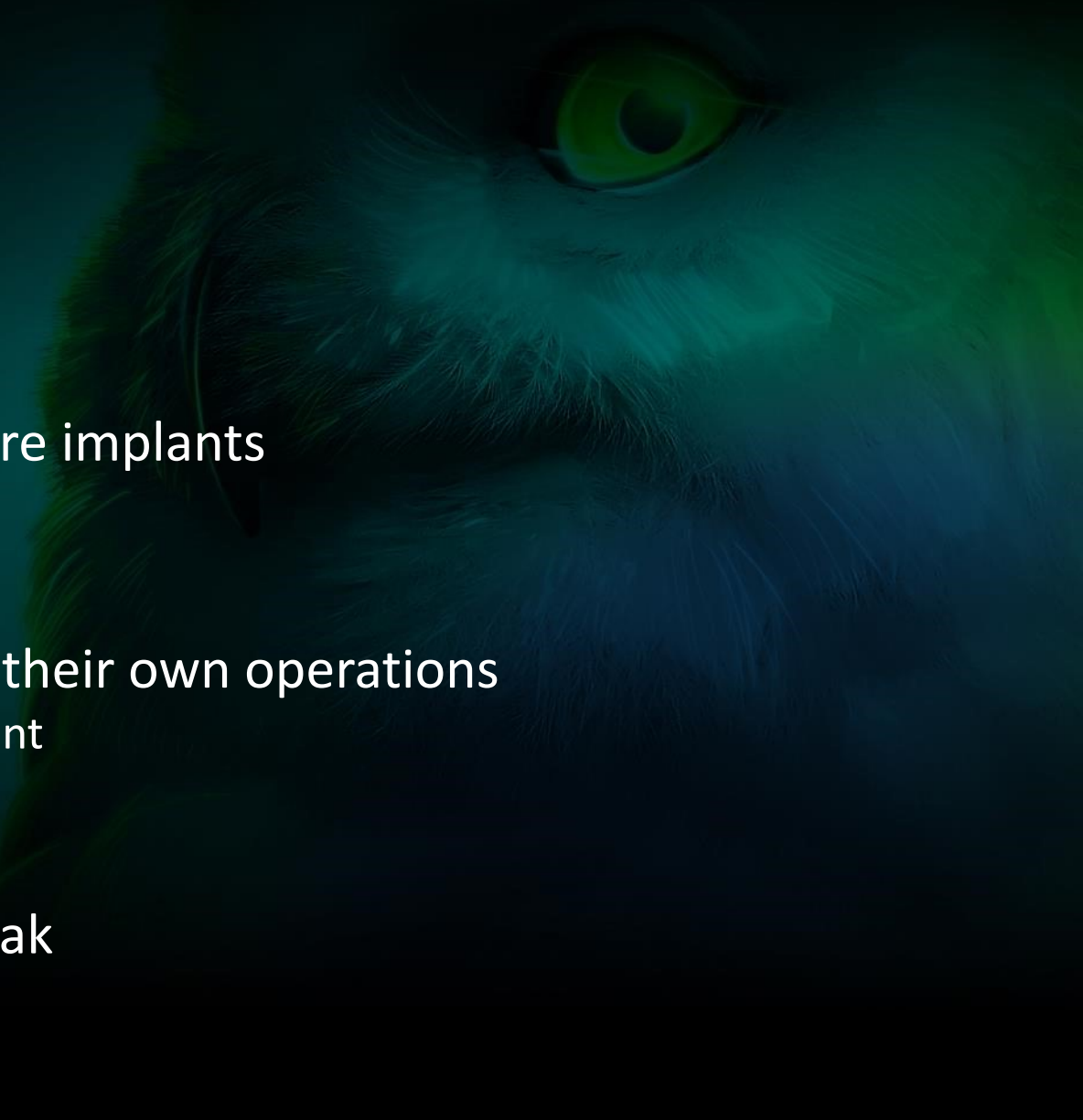
Assessment



- Huge focus on post-post-exploitation
 - Platforms to process, manage and visualize stolen data
 - Strongly marketed towards LEA (“case” management)
- Repackaging of OSS tools into “homemade” GUIs or appliances
 - Aiming for ease of use, not sophistication
 - Public customers in the process of scaling up operations, but facing a skill gap?
 - Talent acquisition a challenge for I-Soon as well despite university partnerships
- Apparent redundancy across all the products
 - Same codebase / engine repackaged to cover multiple verticals
- Auditing / logging / task assignment features in all products
 - Vertical work organization; micromanagement-oriented tooling

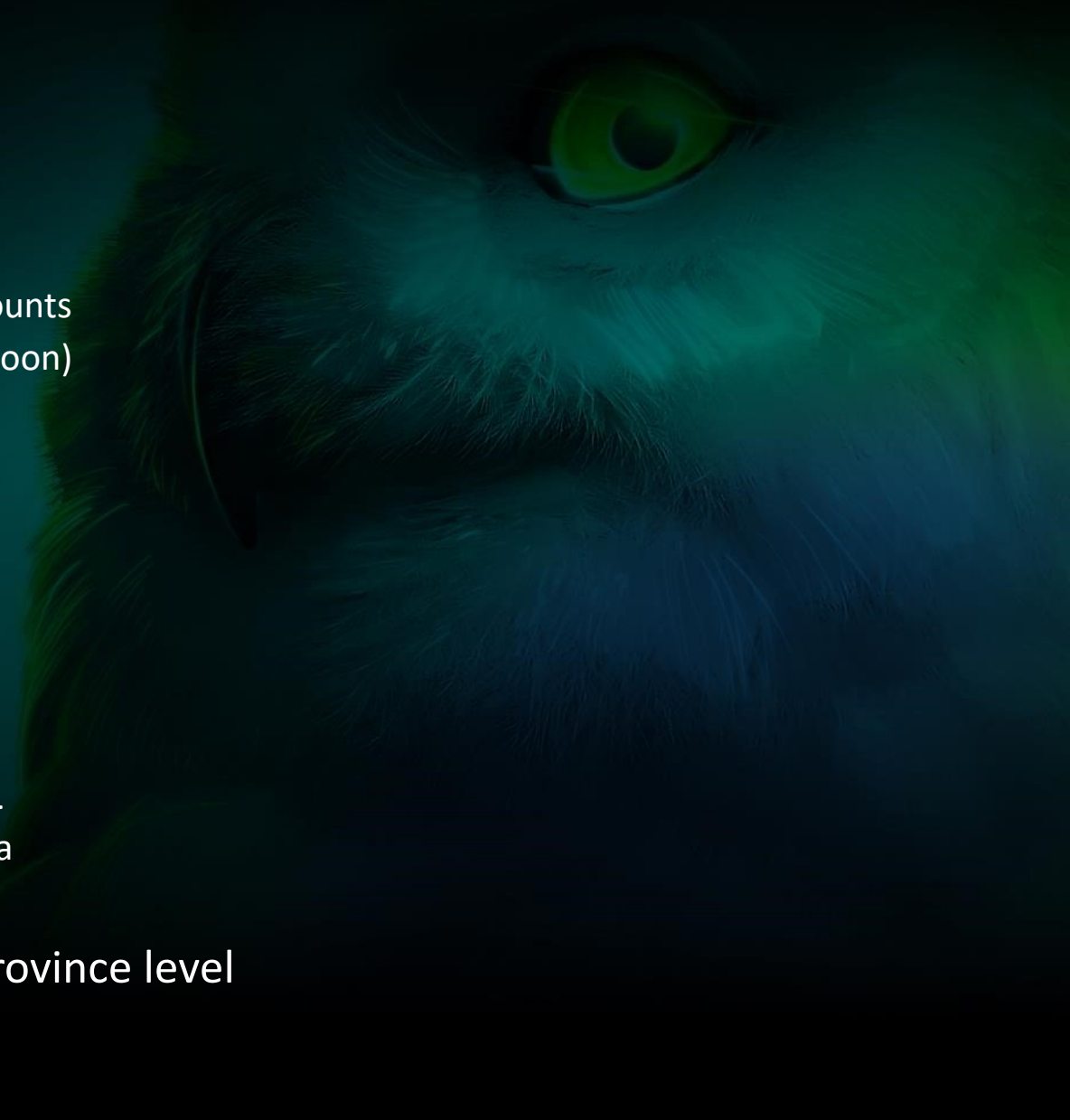
Assessment

- Somewhat crude APT operations
 - Limited to no 0day research capabilities
 - Phishing as the main attack vector
 - Apparent difficulties for sourcing malware implants
- Questionable OPSEC
 - Implants sold to customers are used for their own operations
 - Customer implants can be used for a discount
 - Tasking over IM
 - Cleartext victim / target organizations
 - I-Soon had been identified before the leak



Assessment

- Oversold social media products
 - Doesn't appear to do anything beyond monitor specific accounts
 - Influence / psyops capabilities limited at best (at least for I-Soon)
- But!
 - Impressive number of victims
 - Targets across many verticals
 - Obvious operational successes
 - Ability to infiltrate telcos and extract key data
 - Operational independence
 - Can be tasked by customers...
 - ...or proactively breach and pitch the stolen data to customers.
 - Core technology focus: handling huge volumes of stolen data
 - NOT: be better at breaching victims
- Confirms the autonomy in cyber operations at the province level



Assessment

- Hugely damaging leak
 - Blown operations
 - Reputation
 - Internal employee list with salaries
 - Embarrasses the Chinese Government
- Prediction: I-Soon will keep operating

The image shows a screenshot of a large data table, likely an internal employee list. The table has numerous columns, including names, IDs, and various numerical values. The data is organized into several sections, with some rows highlighted in yellow. The table appears to be a spreadsheet or a database export, containing a significant amount of information.



My View Following Saved

Chinese embassy in Netherlands says China would never allow cyberattacks

Reuters

February 6, 2024 8:23 PM EST · Updated 3 hours ago

Questions?

