viettel security

Dissecting a Ransomware Operation

From Propagation to Extortion

Minh Long

viettel security

viettel
security

Whoami

Minh Long

Cyber Threat Analyst
Viettel Cyber Security
https://viettelcybersecurity.com/

Perform malware analysis, APT tracking and incident response at Viettel Threat Intelligence. Interested in Malware, Windows and Embedded hardware

viettel
security

Agenda

- Introduction
- Ransomware at a glance, operation model
- Attacking methods
- Extortion tactics
- Takeaway

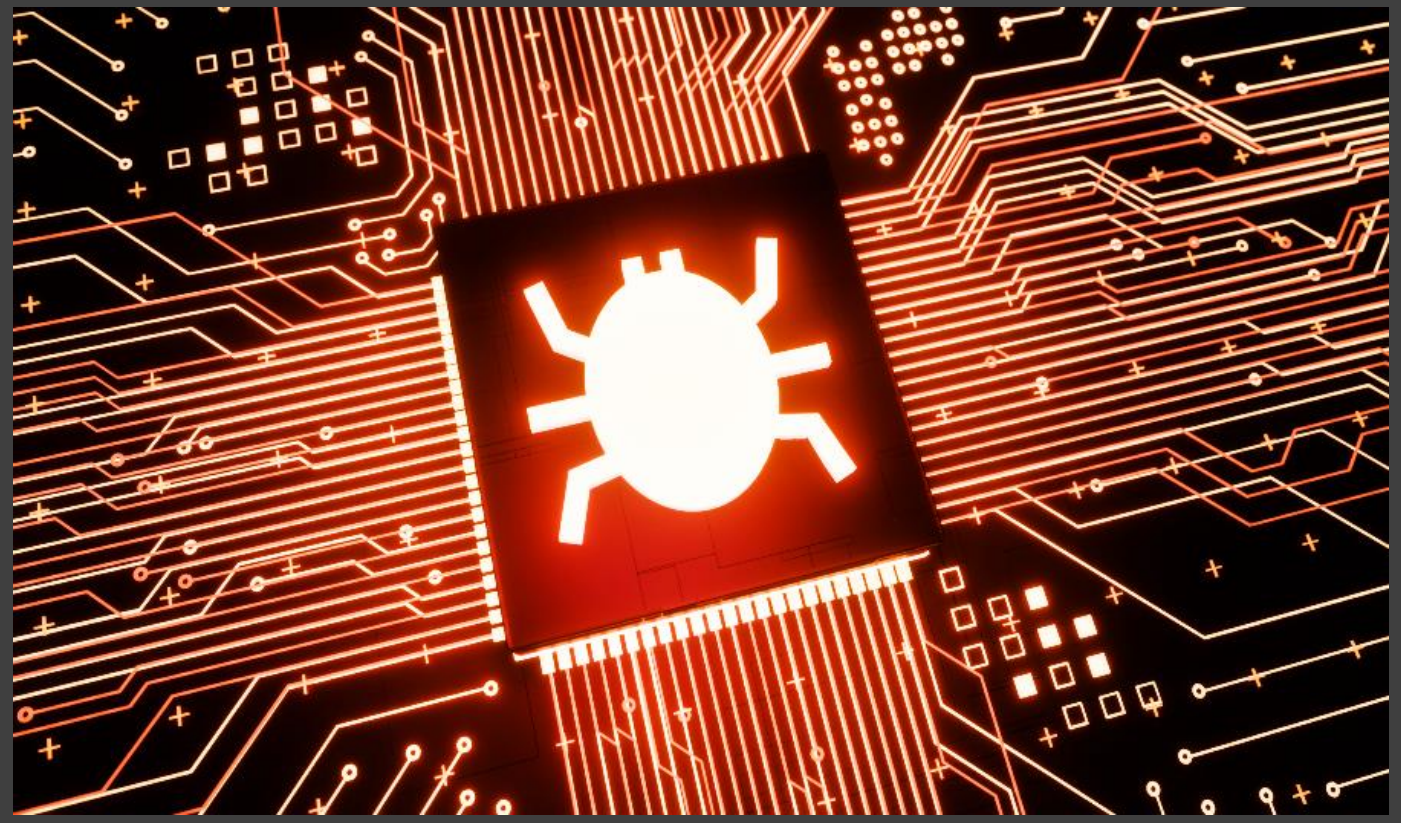
viettel
security

Introduction

viettel security

Evolution of malware

- Mostly self-replicated software try to infect as many machine it can
- A way to show off the hackers' skill, capability
- Data, credential theft
- Malware were made for espionage operation (APT1)
- Advanced malware is used to destroy or hinder enemy.



AIDS ransomware

- World's first ransomware, since 1989
- Spread through floppy disk
- Using symmetric algorithm to encrypt victim data
- Complicate extortion method

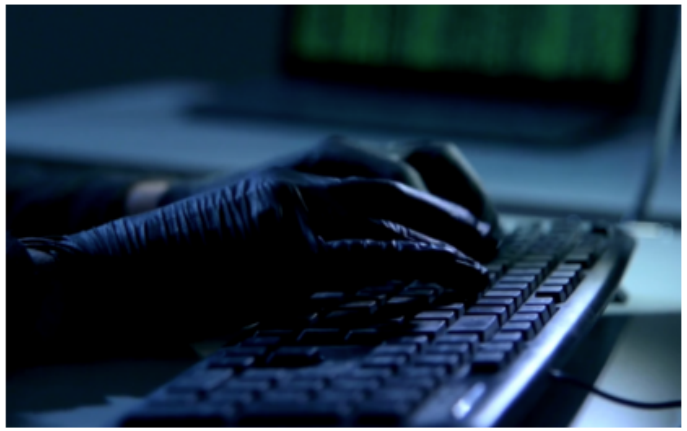
Ransomware become trend

- Cryptocurrency allows fast, obscure transactions
- Internet make everything connect
- The use of public key Public-key cryptography makes it near impossible to recover the data

Republic of the Philippines
PHILIPPINE NEWS AGENCY

Ransomware attacks in PH double in 2023

By Kris Crismundo
January 16, 2024, 6:55 pm



(File photo)

MANILA – A commissioned survey by a cybersecurity firm has found that ransomware incidents in the Philippines became more rampant and aggressive in 2023.

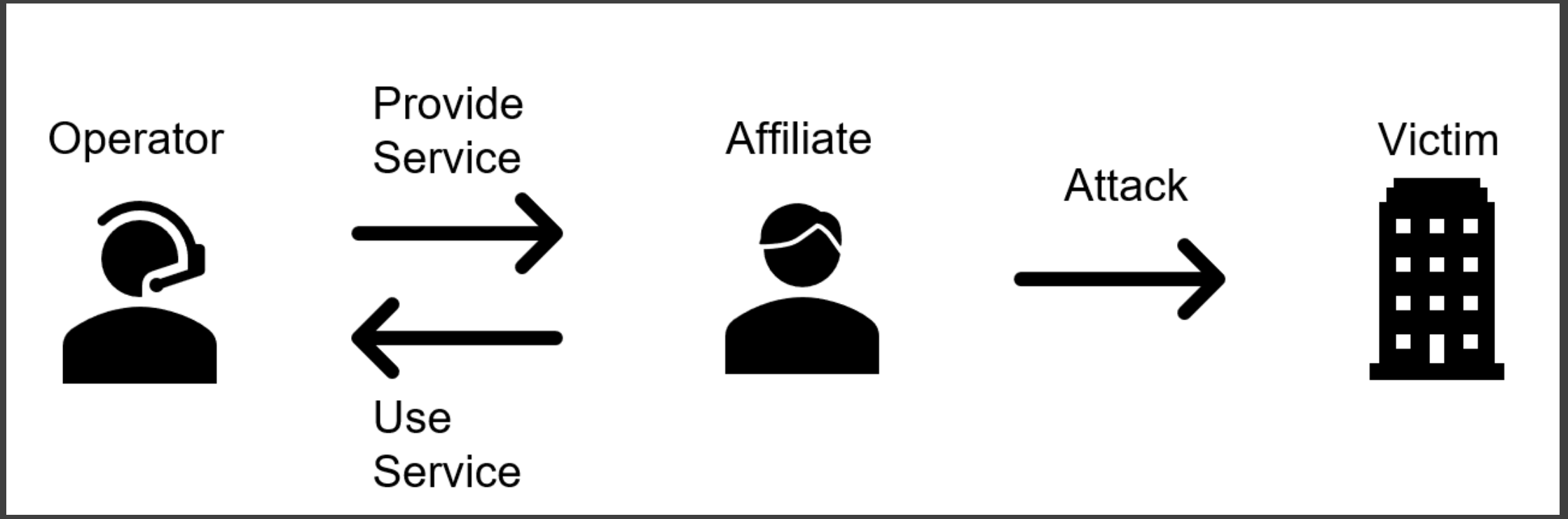
Fortinet Marketing and Communications for Asia and Australia and New Zealand vice president Rashish Pandey said in a media briefing in Makati City Tuesday that 56 percent of the surveyed organizations in the Philippines reported that ransomware attacks surged by at least two times in 2023 compared to 2022.

The International Data Corporation's Survey cited that phishing and ransomware were among the most common cyber threats in the country last year.

A phishing attack deceives an individual to reveal personal and sensitive information, while ransomware blocks victim to have access to one's personal data unless a ransom is paid.

"In the past, it used to be 'Alright, I have locked your system.' The bad actors will come and say 'You pay me money... and I will give you access back to the data.' Now, it has advanced even more. What we are seeing now is even if you pay the money, they will not give you the data back or just delete it," Padney said.

Ransomware-as-a-Service



Interaction between Operator and Affiliate

viettel security

Transaction

Pay monthly (subscription)

According to the source from IBM and zvelo, affiliate can subscribe monthly with the price ranging from $40

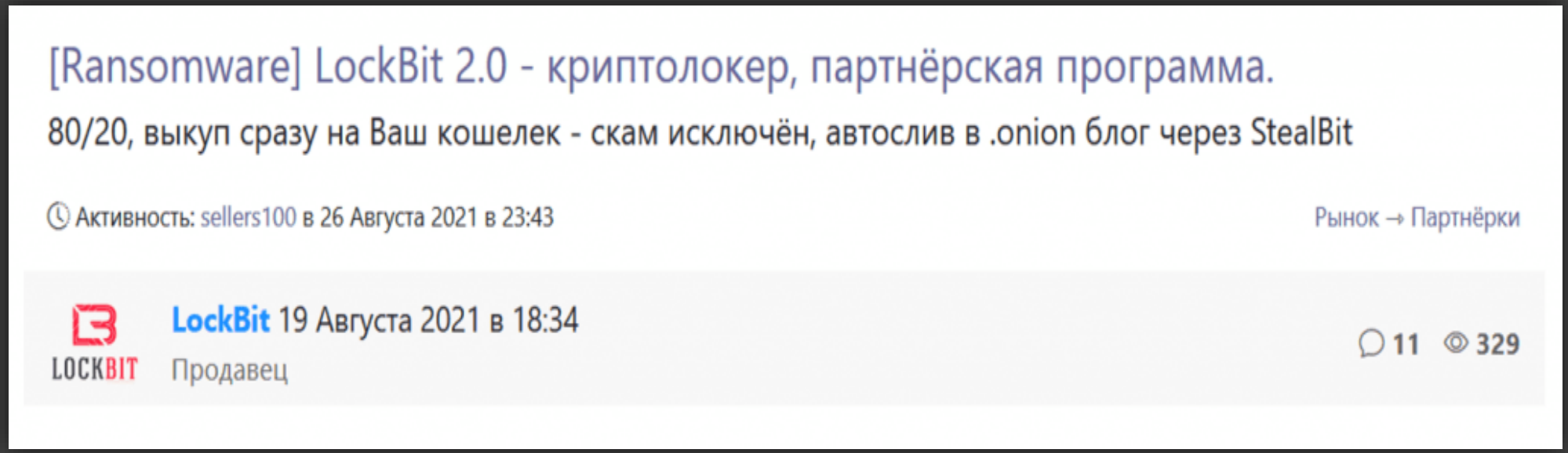
Pay according to each extortion

Typically the affiliate and operator share the profit 80-20

One-time payment

The affiliate and operator share the profit 80-20

Transaction



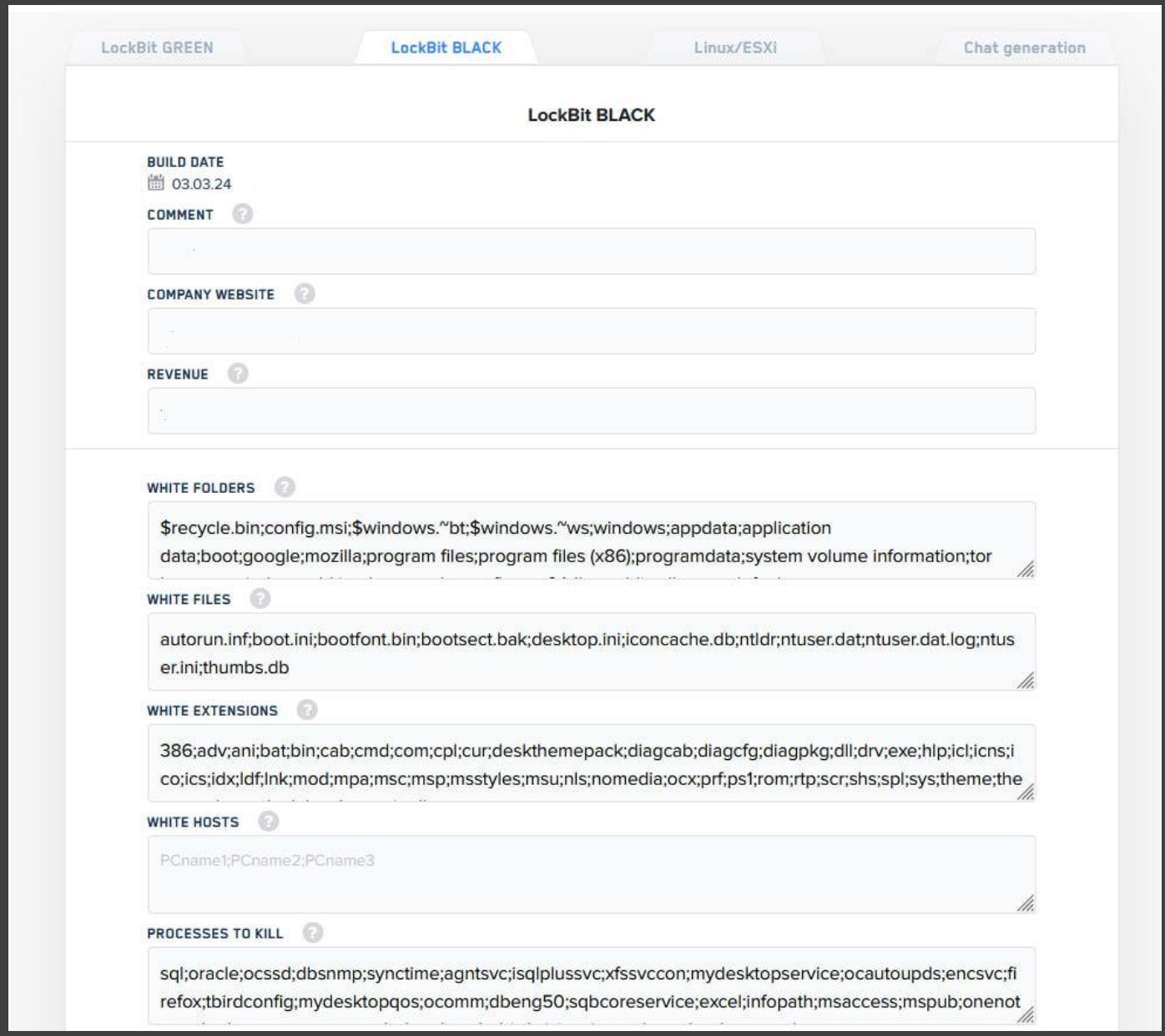
80/20 profit sharing with payments made to your crypto address! No scam! Automatically post data to onion blog via Stealbit

The builder

The output of the builder contain 2 main file:

- Encryptor: Drop to victim infrastructure and encrypt victim data.
- Decrypt: Use to decrypt the data encrypted by Encryptor.

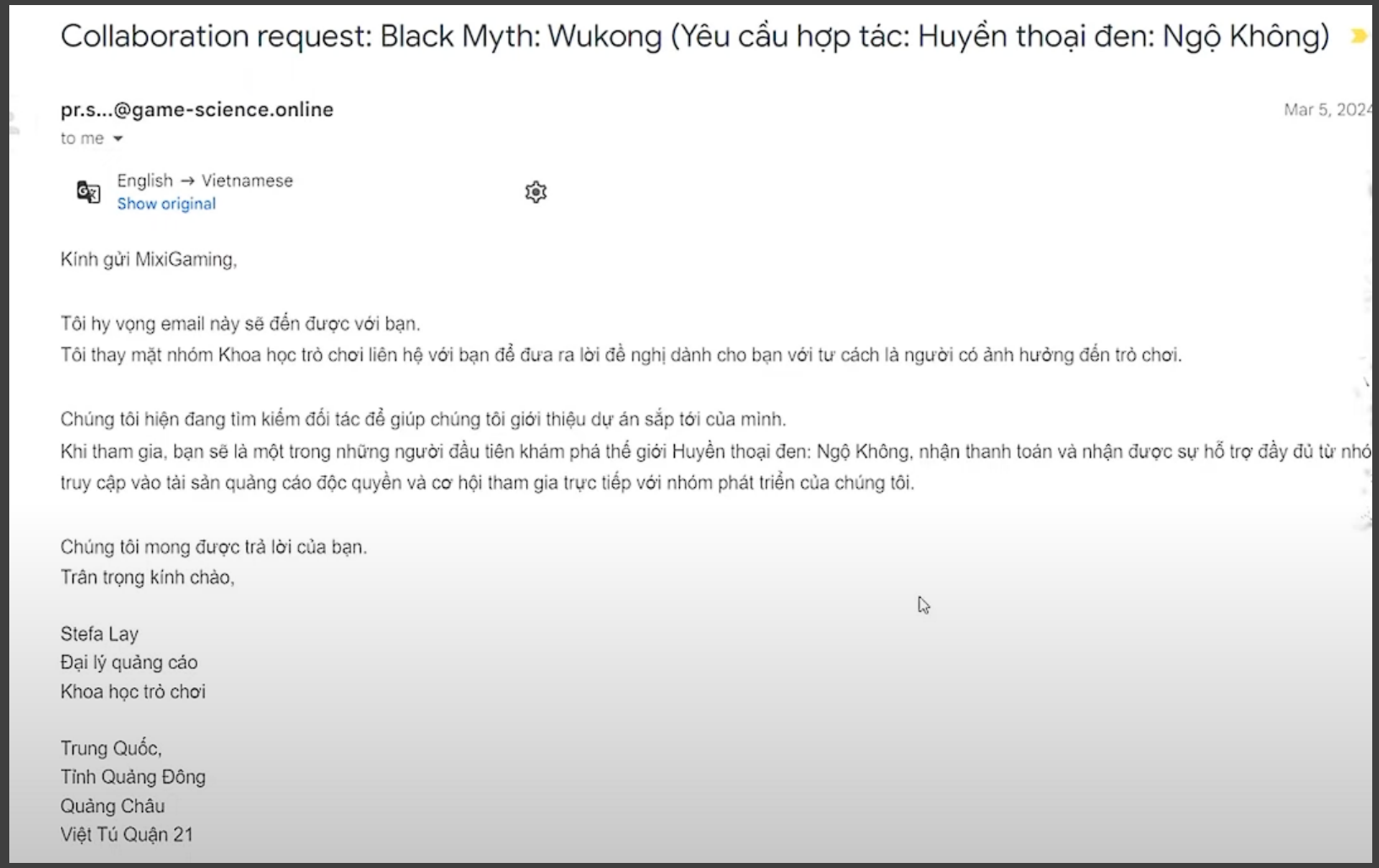
In addition to the builder, operator provide a chat portal to negotiate with the victim.



Attack vector

Initial access: Phishing

Case example



Collaboration request: Black Myth: Wukong (Yêu cầu hợp tác: Huyền thoại đen: Ngộ Không)

pr.s...@game-science.online Mar 5, 2024

to me

English → Vietnamese

Show original

Kính gửi MixiGaming,

Tôi hy vọng email này sẽ đến được với bạn.
Tôi thay mặt nhóm Khoa học trò chơi liên hệ với bạn để đưa ra lời đề nghị dành cho bạn với tư cách là người có ảnh hưởng đến trò chơi.

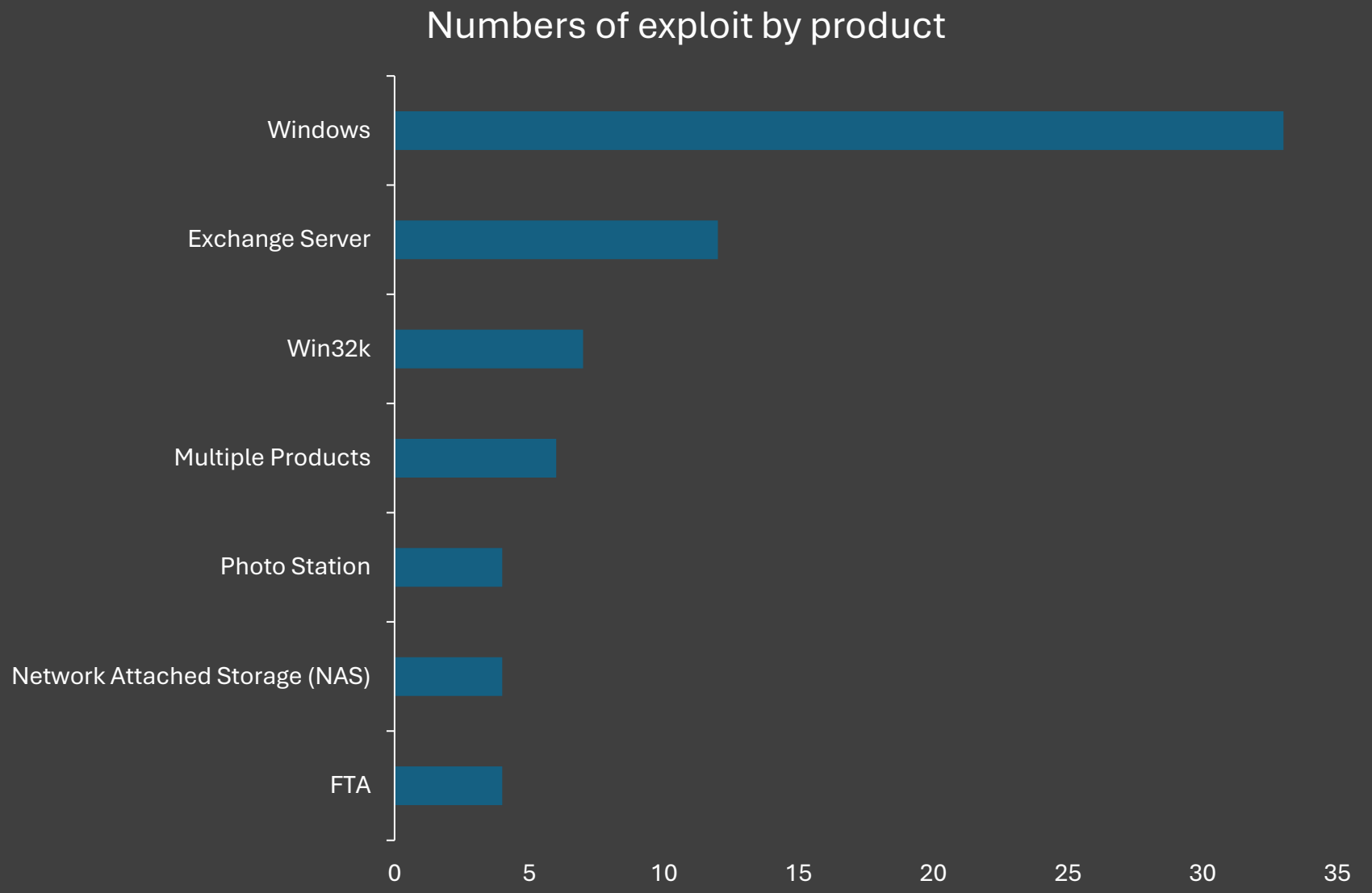
Chúng tôi hiện đang tìm kiếm đối tác để giúp chúng tôi giới thiệu dự án sắp tới của mình.
Khi tham gia, bạn sẽ là một trong những người đầu tiên khám phá thế giới Huyền thoại đen: Ngộ Không, nhận thanh toán và nhận được sự hỗ trợ đầy đủ từ nhó
truy cập vào tài sản quảng cáo độc quyền và cơ hội tham gia trực tiếp với nhóm phát triển của chúng tôi.

Chúng tôi mong được trả lời của bạn.
Trân trọng kính chào,

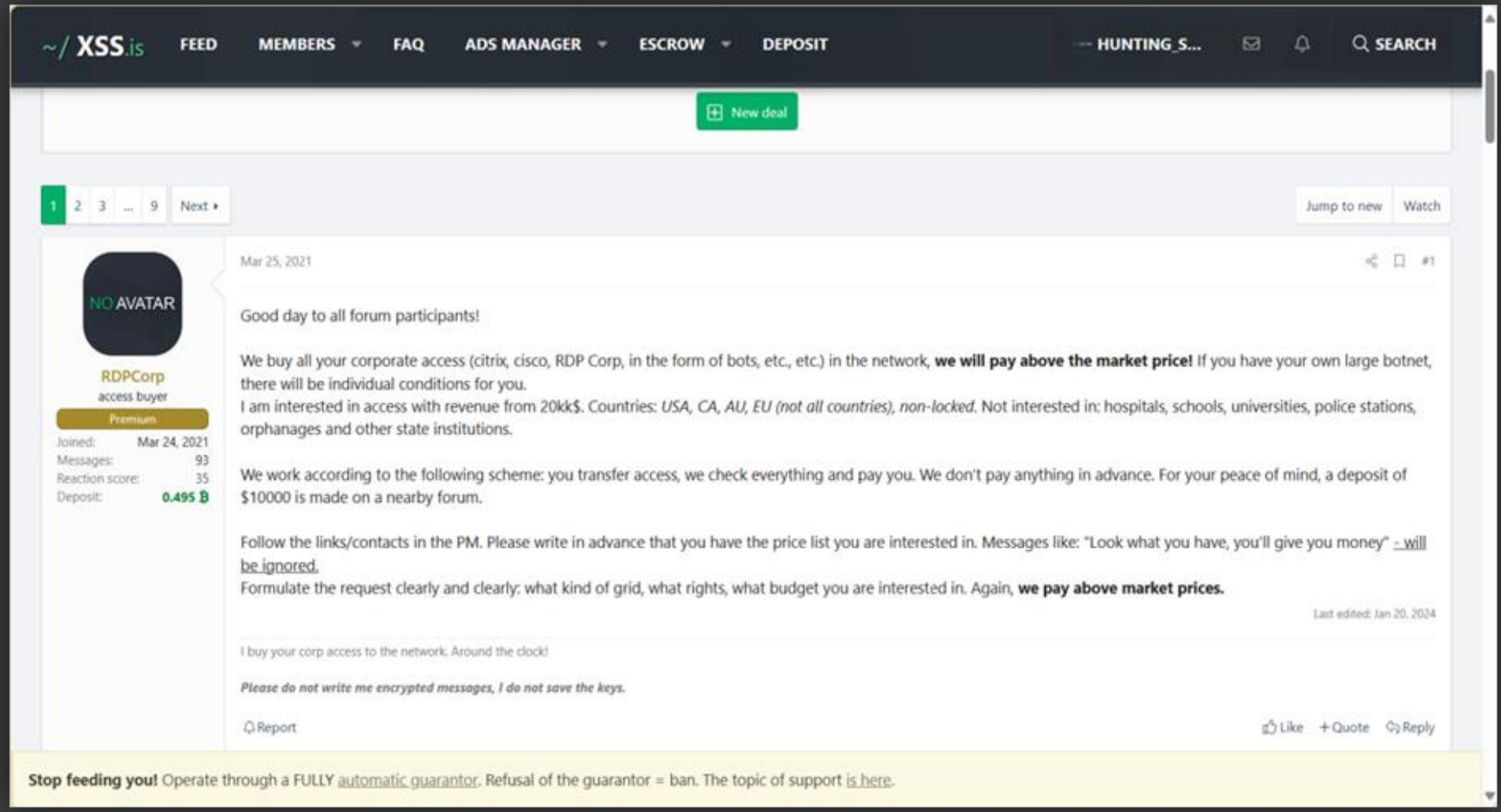
Stefa Lay
Đại lý quảng cáo
Khoa học trò chơi

Trung Quốc,
Tỉnh Quảng Đông
Quảng Châu
Việt Tú Quận 21

Initial access: Exploit critical vulnerabilities



Initial access: Insider threat



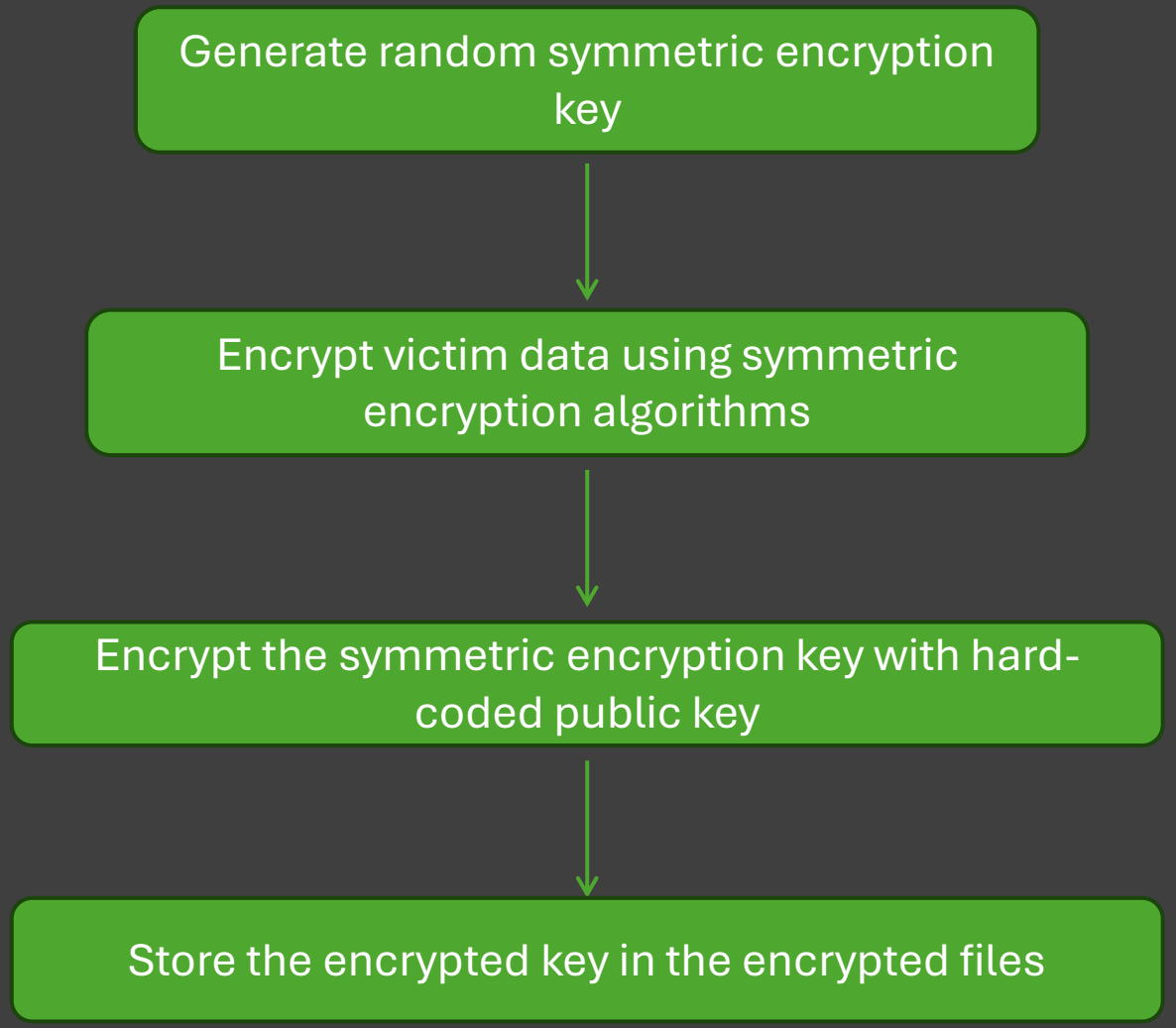
Propagation

The goal

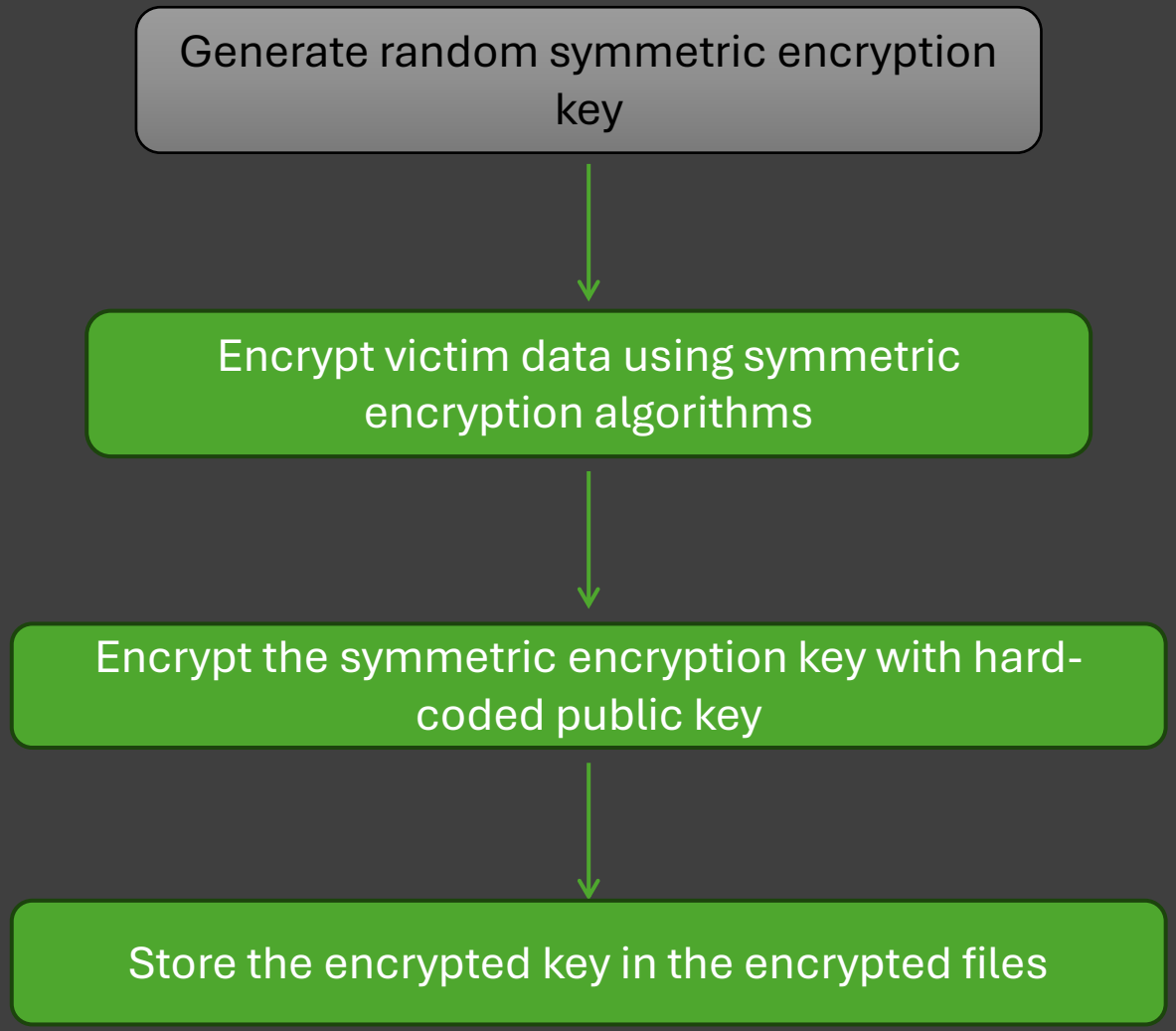
- Try to get infected as many machine as possible
- Server with sensitive databases
- Remote tools are friends: SMB, SSH, RDP,....
- High value target: Active Directory, ESXI server,....

viettel security

Encryption process



Encryption process



```
// Generate AES key and IV
for (int i = 0; i < 16; i++) {
  aes_key[i] = srand(time(NULL));
  aes_iv[i] = srand(time(NULL));
}
```

Extortion

Double-extortion

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.

2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to help.

3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.

4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion.

5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.

2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id.onion.

3. Use this code - [redacted] - to log into our chat.

Keep in mind that the faster you will get in touch, the less damage we cause.

Timing

Wannacry

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

12 May 2017

Colonial Pipeline

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

7 May 2021

Boeing Incident

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

28 Oct 2023

Takeaway

viettel security

3-2-1 Backup Rule

3

Create al least three copies of your data

2

Store the copies on two different storage media

1

Store one copy on an offsite storage

viettel
security

Thank you