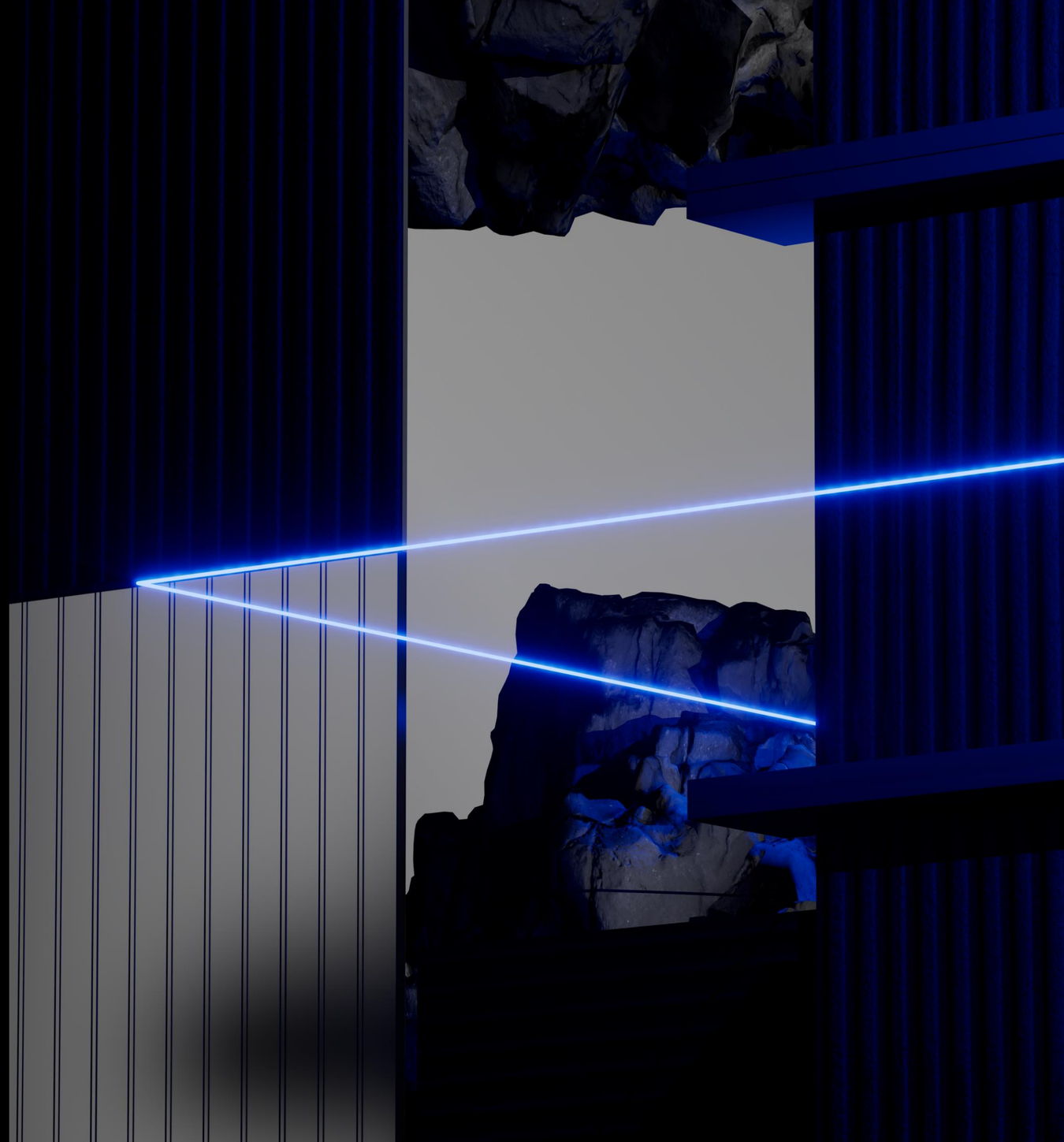
MỘT VỤ TRỘM TIỀN



- Lê Phương Nam

BỐI CẢNH

Một người đàn ông ngoại quốc rút tiền ở ATM

Cảnh sát của nước sở tại bắt anh tại trận

Khám xét nơi ở của anh ta và kiểm tra máy tính

Trên chiếc máy tính 2nd hand có sự hiện diện của phần mềm xử lý EMV

Ngân hàng kiểm tra thông tin của thẻ ATM thì thấy số dư trong tài khoản rất nhỏ

Tuy nhiên, số tiền rút được lớn hơn nhiều số dư trong tài khoản…

MÁY CHỦ XỬ LÝ GIAO DỊCH ATM

Không phát hiện phần mềm lạ được cài đặt

Không phát hiện service, schedule… đáng ngờ

Bản ghi Log không ghi lại về truy cập lạ hay các sự kiện đáng ngờ

HSM không bị tấn công

Về cơ bản, chưa phát hiện manh mối cho thấy máy chủ xử lý ATM bị tấn công…

MÁY CHỦ XỬ LÝ GIAO DỊCH ATM

Bắt gói tin giữa máy chủ ATM với HSM

Tiến hành giao dịch rút tiền sử dụng thẻ của người ngoại quốc thông tin từ HSM trả về luôn là “ok”…

MÁY CHỦ XỬ LÝ GIAO DỊCH ATM

Dump memory trên máy chủ ATM phát hiện kernel module

Bước đầu phân tích kernel module:

SyS_write:system call, có thể ghi dữ liệu tới bất kỳ file, socket …

SyS_delete_module: system call, có thể vô hiệu hóa lệnh nếu như root un-load module.

Filldir: không hiện module ở /sys

MÁY CHỦ XỬ LÝ GIAO DỊCH ATM

Tiến hành kiểm tra sâu hơn

/usr/sbin/atd
Là một backdoor trên Linux, Lưu cấu hình trên một file, và được khởi động cùng hệ thống như một dịch vụ (daemon), nó có thể đọc nội dung của file bất kỳ và gửi về máy chủ C2, nhận nội dung từ C2 server lưu thành file và tạo kết nối shell từ C2.
Trong trường hợp này, C2 server là một máy chủ nội bộ.

pam_unix.so
Là một module chứng thực của Linux, với khả năng có thể thu thập thông tin đăng nhập của người dùng và là một backdoor. File pam_unix.so của tin tặc thay đổi file pam_unix.so (của hệ điều hành), khi nhận được yêu cầu chứng thực từ người dùng, nó mã hóa và lưu thông tin đăng nhập vào «/var/tmp/.font-unix». Bên cạnh đó nó có môt số mật khẩu mặc định, khi nhận được chuỗi mật khẩu này, kèm theo một số token thì nó có thể thực hiện xóa file, thực thi câu lệnh.

File /var/tmp/.font-unix được sử dụng thủ thuật anti-forensic, nhằm mục đích che giấu khoảng thời gian file được tạo ra.

libmm.so.1.0/pulse-shm-1489710120
Log cleaner, được định nghĩa sẵn để xóa một số thông tin nhất định trên log hệ thống và user bash history:

- /var/run/utmp
- /var/log/wtmp
- /var/log/btmp
- /var/log/lastlog
- /var/log/faillog
- /var/log/syslog
- /var/log/messages
- /var/log/secure
- /var/log/auth.log

TÌM KIẾM TRÊN TOÀN CÁC BỘ MÁY CHỦ

Threat Hunting

Tin tặc

PC bị lây nhiễm

Máy chủ jump host

Máy chủ ATM

MỘT SỐ THỦ THUẬT

- Sửa file ssh binary trên máy chủ để load thư viện selinux.so.1, mã hóa mà lưu trữ thông tin thu thập được vào /var/tmp/.zmanDwJ2Og

- Gói malware vào trong một payload được mã hóa, key giải mã được lưu trong environment variable, khi session kết thúc thì key giải mã cũng tự động được xóa, không thể khôi phục.

- File binary được ascii encode để có thể copy thông qua cửa sổ terminal.

- Sử dụng DirtyCow để tấn công chiếm quyền root.

MITRE ATT&CK

PERSISTENCE	DEFENCE EVASION	CREDENTIAL ACCESS	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	IMPACT
T1556.003 - Modify Authentication Process: Pluggable Authentication Modules	T1027.002 - Obfuscated Files or Information: Software Packing	T1556.003 - Modify Authentication Process: Pluggable Authentication Modules	T1021.004 - Remote Services: SSH	T1056.001 - Input Capture: Keylogging	T1572 - Protocol Tunneling	T1565.002 - Data Manipulation: Transmitted Data Manipulation
T1554 - Compromise Client Software Binary	T1036.005 - Masquerading: Match Legitimate Name or Location	T1056.001 - Input Capture: Keylogging			T1571 - Non-Standard Port	
	T1070.002 - Indicator Removal on Host: Clear Linux or Mac System Logs					
	T1070.006 - Indicator Removal on Host: Time-stomp					
	T1556.003 - Modify Authentication Process: Pluggable Authentication Modules					

MALWARE OVERVIEW

#	Malware	Mô tả
1	ATD	Backdoor
2	PAM	Credential harvesting, remote execution, TCP-Proxy
3	SSH, PAM	Keylogger
4	libmm.so.1.0 pulse-shm-1489710120	Log Cleaner
5	memory	Kernel rootkit

PERSISTENCE

File binary sau bị thay đổi:
/usr/bin/ssh và /usr/sbin/atd
File “ssh” binary bị thay đổi để load thư viện “/usr/lib/x86_64-linux-gnu/selinux.so.1”

File “atd” binary bị thay đổi và được thực thi cùng hệ thống như một daemon.

PAM (pluggable authentication module) “pam_unix.so”

PRIVILEGE ESCALATION

Tin tặc sử dụng ascii encode để truyền file Dirtycow tới “/dev/shm/gconf-root”

Dirty COW sử dụng lỗ hổng CVE-2016-5195 để tấn công các máy chủ Linux để chiếm quyền root.

DEFENSE EVASION

- LOG CLEANER “liblbch-2.4.so.2.5.6” và MIGLOGCLEANER “libmig.so.1”. Có thể xóa toàn bộ log hoặc xóa một số từ khóa.
- Tin tặc đặt tên malware gần giống với tên các tệp tin hệ thống.

#	Tên Malware	Tên file của hệ thống
Log Cleaner	libm**i**g.so.1	libm**n**g.so.1
Thư viện load bởi SSH	selinux.so.1	**lib**selinux.so.1
ATD	libsystemd**cfgnome**.so	libsystemd.so.**0**
ATD	libxcb-glx.so.**1**	libxcb-glx.so.**0**

CREDENTIAL ACCESS

- PAM module được thay đổi trên máy chủ bị tấn công, file PAM nguyên bản của hệ thống được đổi tên thành “pam_unix,so”.
- Tất cả dữ liệu để chứng thực vào hệ thống được mã hóa và lưu trữ tại file “/var/tmp/.font-unix”.
- Nếu như trường mật khẩu khớp với một số chuỗi ký tự được định nghĩa sẵn thì hệ thống chứng thực thành công và thực hiện một số câu lệnh.
- Thông tin được lưu trữ tại “/var/tmp/.font-unix” có format:

| DATE | PROTOCOL | USERNAME | PASSWORD | SOURCE HOST | AUTHENTICATION STATUS |

LATERAL MOVEMENT

- Với tài khoản và mật khẩu thu thập được, tin tặc có thể sử dụng để truy cập vào các máy chủ khác.
- Có môt số mật khẩu mặc định, khi nhận được chuỗi mật khẩu này, kèm theo một số token thì nó có thể thực hiện thực thi câu lệnh, mở proxy.
- “#sh” và “#tcp”:

- Câu lệnh “#sh” sẽ thực thi lênh lên máy chủ.
- Câu lệnh “#tcp” sẽ mở kết nối TCP tới máy chủ được định sẵn để thực hiện việc nhận và truyền dữ liệu.

COMMAND & CONTROL

- /usr/sbin/atd sử dụng file cấu hình: /var/yp/yp.cache, /usr/lib/libatdcf.so, /usr/lib64/libsystemdcf.so
- Sử dụng các port lạ (được định nghĩa trong file cấu hình) để thực hiện việc kết nối CnC

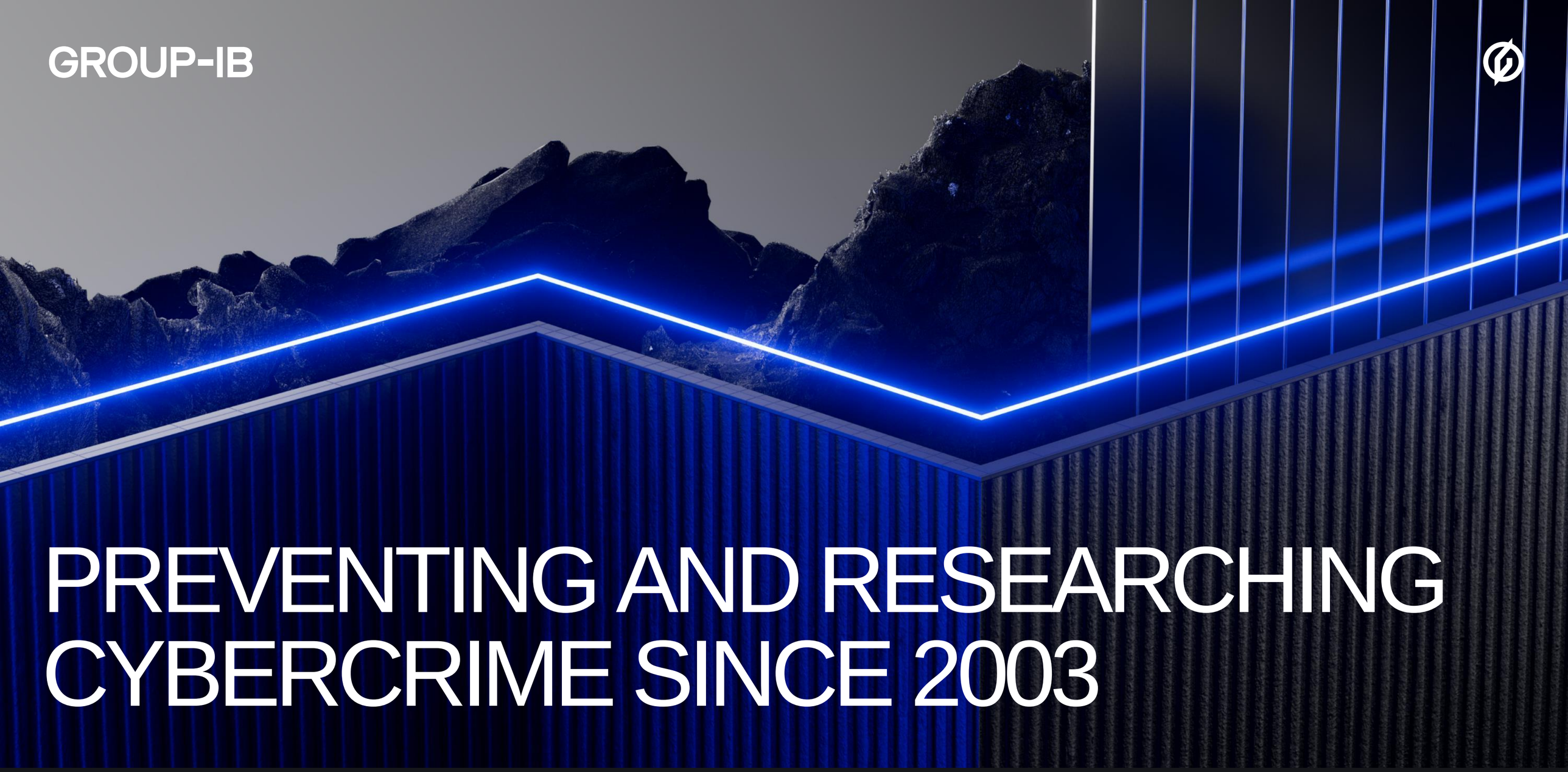
IMPACT

- Rootkit thu thập dữ liệu được gửi từ máy chủ ATM tới máy chủ HSM và kiểm tra với những thông tin được định sẵn, nếu như thông số khớp thì dữ liệu sẽ bị thay đổi tới máy chủ HSM

TABLE 01

Just an example of a table

GROUP-IB



PREVENTING AND RESEARCHING CYBERCRIME SINCE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM
GROUP-IB.COM/BLOG
+65 3159 37 98

LINKEDIN FACEBOOK TWITTER INSTAGRAM