
腾讯安全
云鼎实验室
锋刃无影
御见未来
腾讯安全沙龙第3期（成都站）
IFS

ScreenCrab, the Silent Gaze of the Red Team and How to Stop It

演讲嘉宾：伊万
Date：2025/04/26

Agenda

1. Who we are
2. Intro
3. Red Team use
4. Defense
5. Conclusions

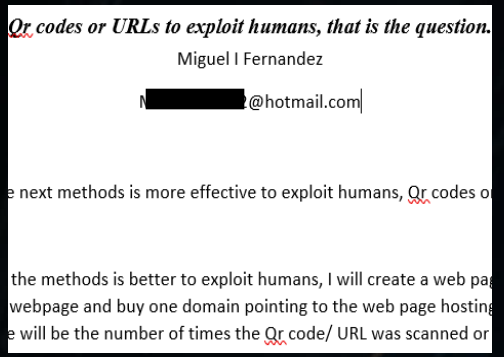
关于我
About me

Miguel Ivan Fernandez - 伊万

Lenovo™ 全球安全实验室 Global Security Lab

HackingGroup

DragonJAR


Qr codes or URLs to exploit humans, that is the question.

Miguel I Fernandez

[redacted]@hotmail.com

e next methods is more effective to exploit humans, Qr codes o

the methods is better to exploit humans, I will create a web pag
webpage and buy one domain pointing to the web page hosting
e will be the number of times the Qr code/ URL was scanned or

OverDrive

HACKPROVE

DEFCON GROUP 010 HACKER COMMUNITY

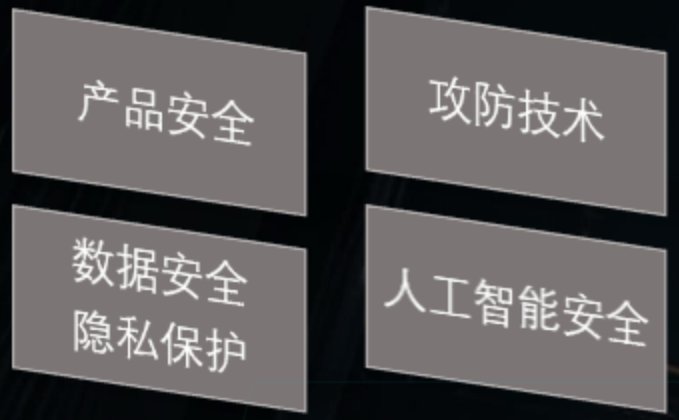
CODEGATE

CIS

联想GIC全球安全实验室

Lenovo 全球安全实验室 Global Security Lab

- 持续提升产品安全质量
- 安全技术创新助力业务发展

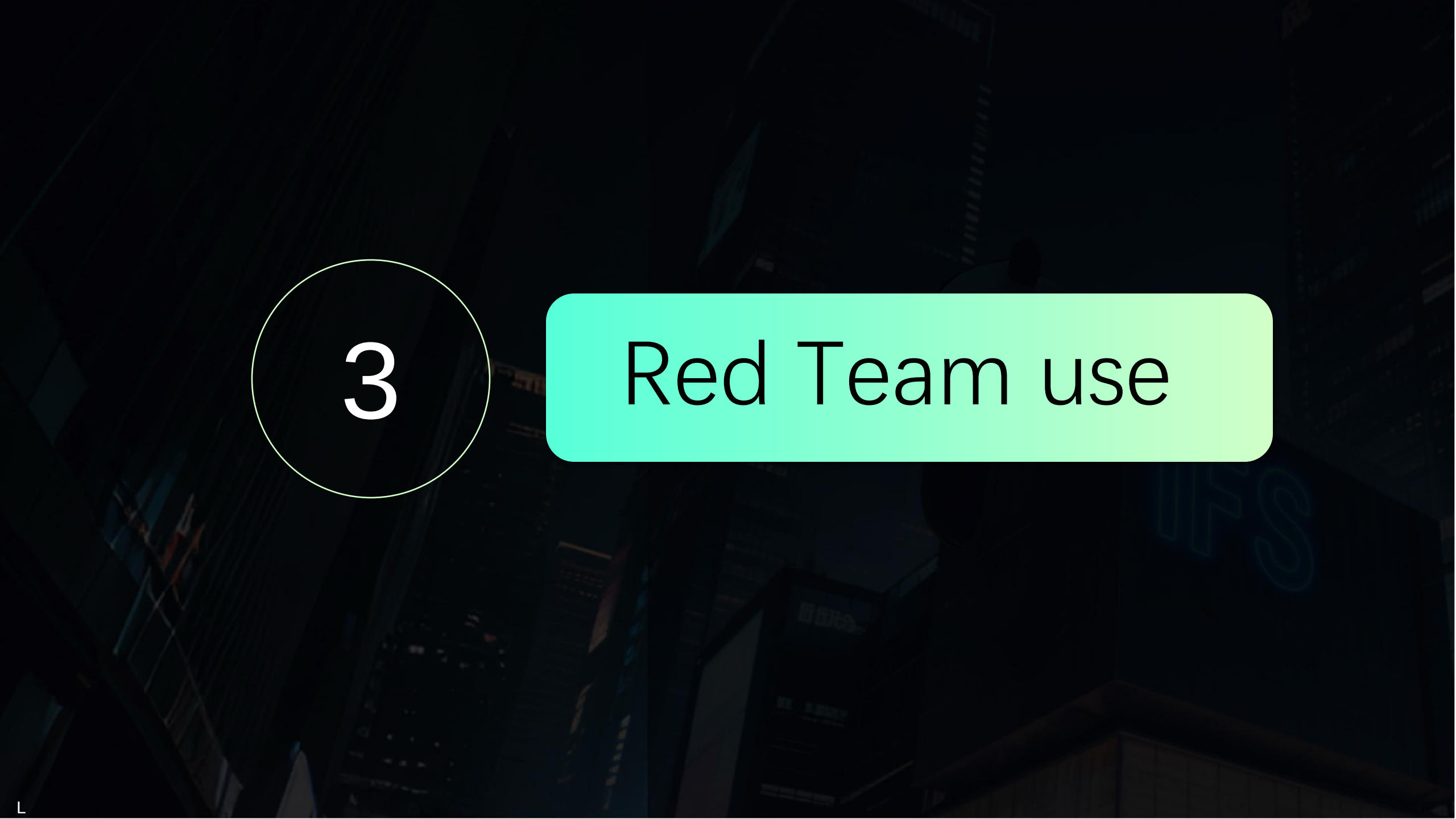


致力于打造全球领先的、端到端的产品安全解决方案，为用户提供更加安全的智能化产品、方案和服务。

ScreenCrab - Intro

- 获取显示信号
- 视频或图片
- 本地或C2存储
- WiFi功能

M


3
Red Team use

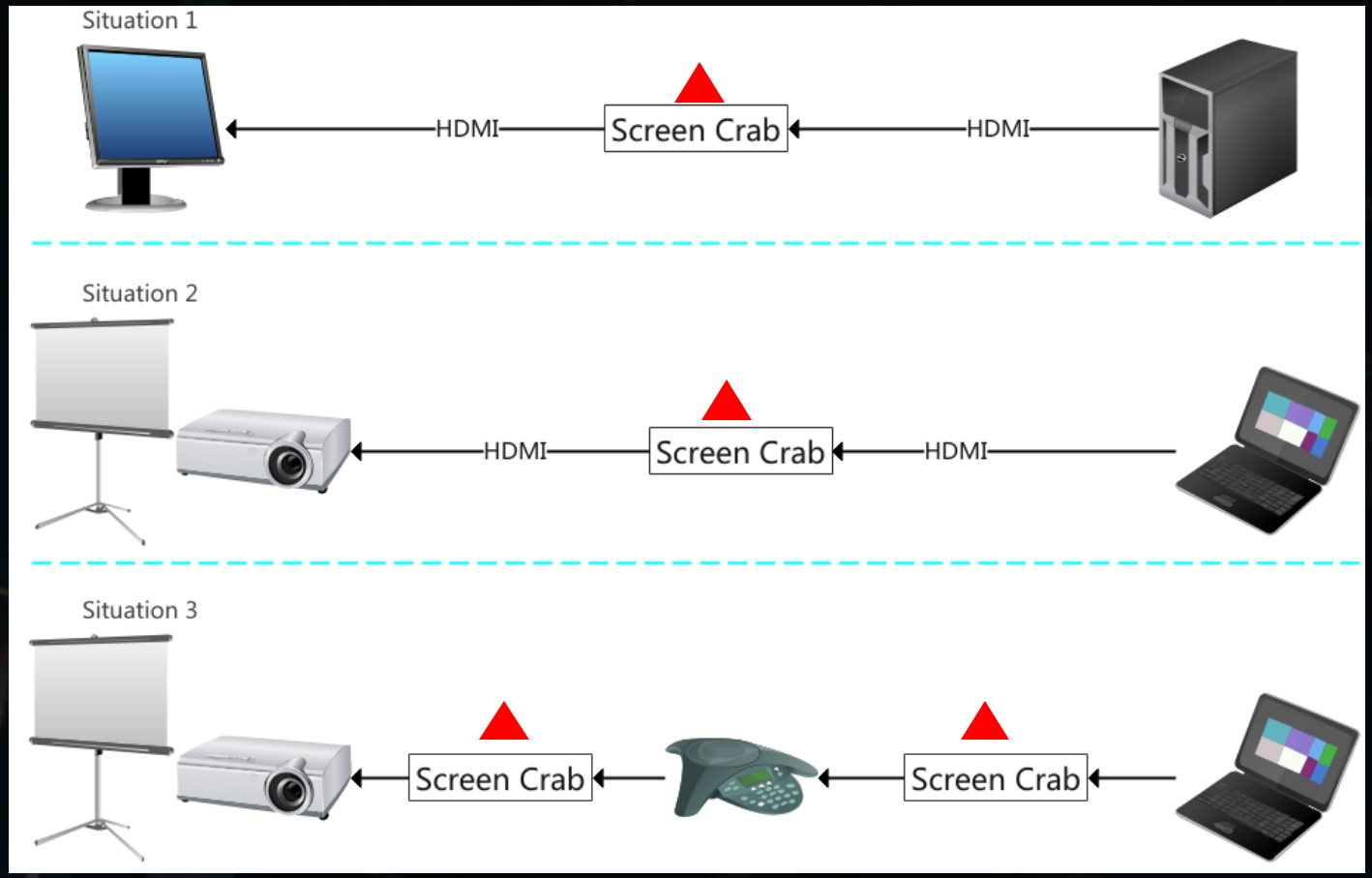
为什么

网络信息

容易:-被发现 -防御

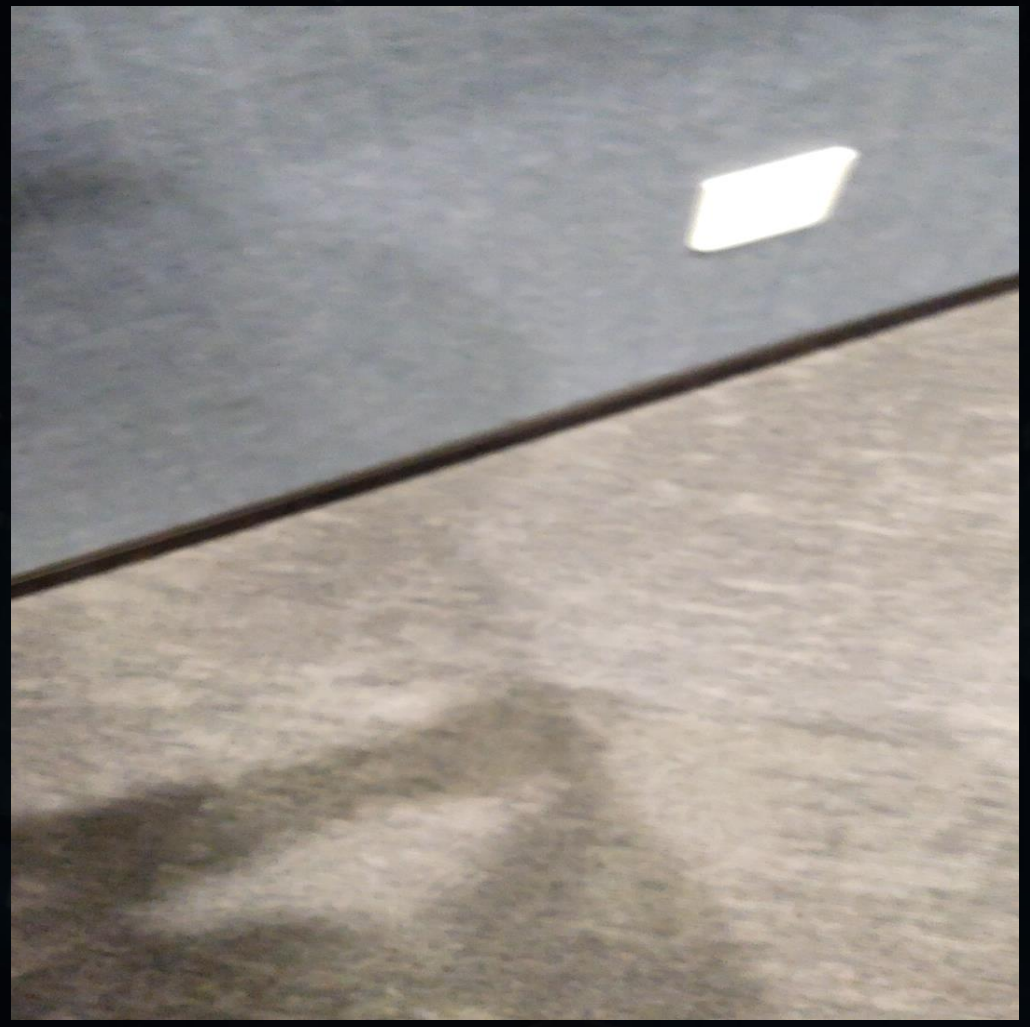
图形信息

难: -被发现 -防御

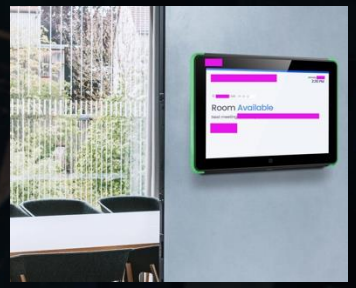


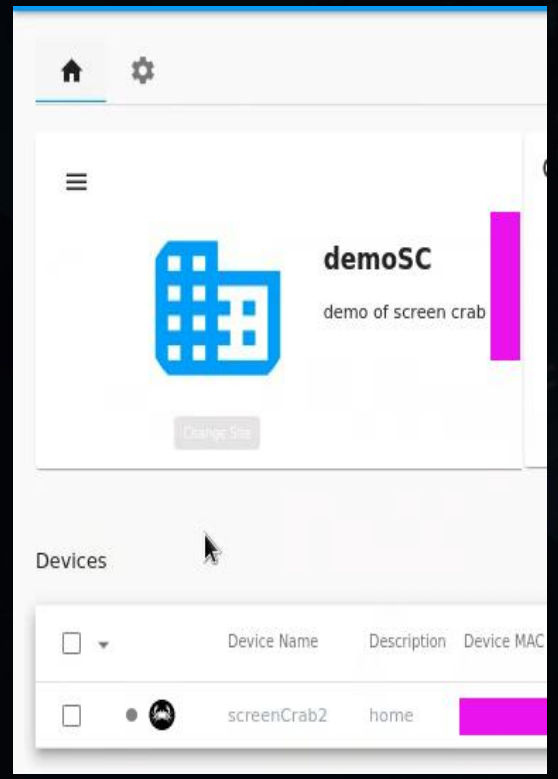
M

图形中间人监听

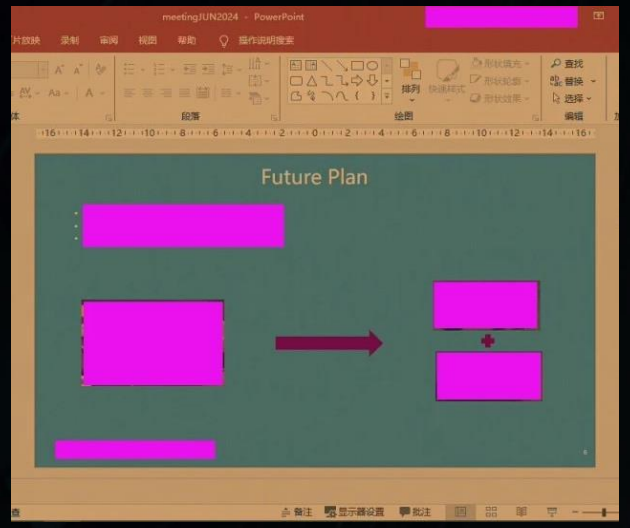


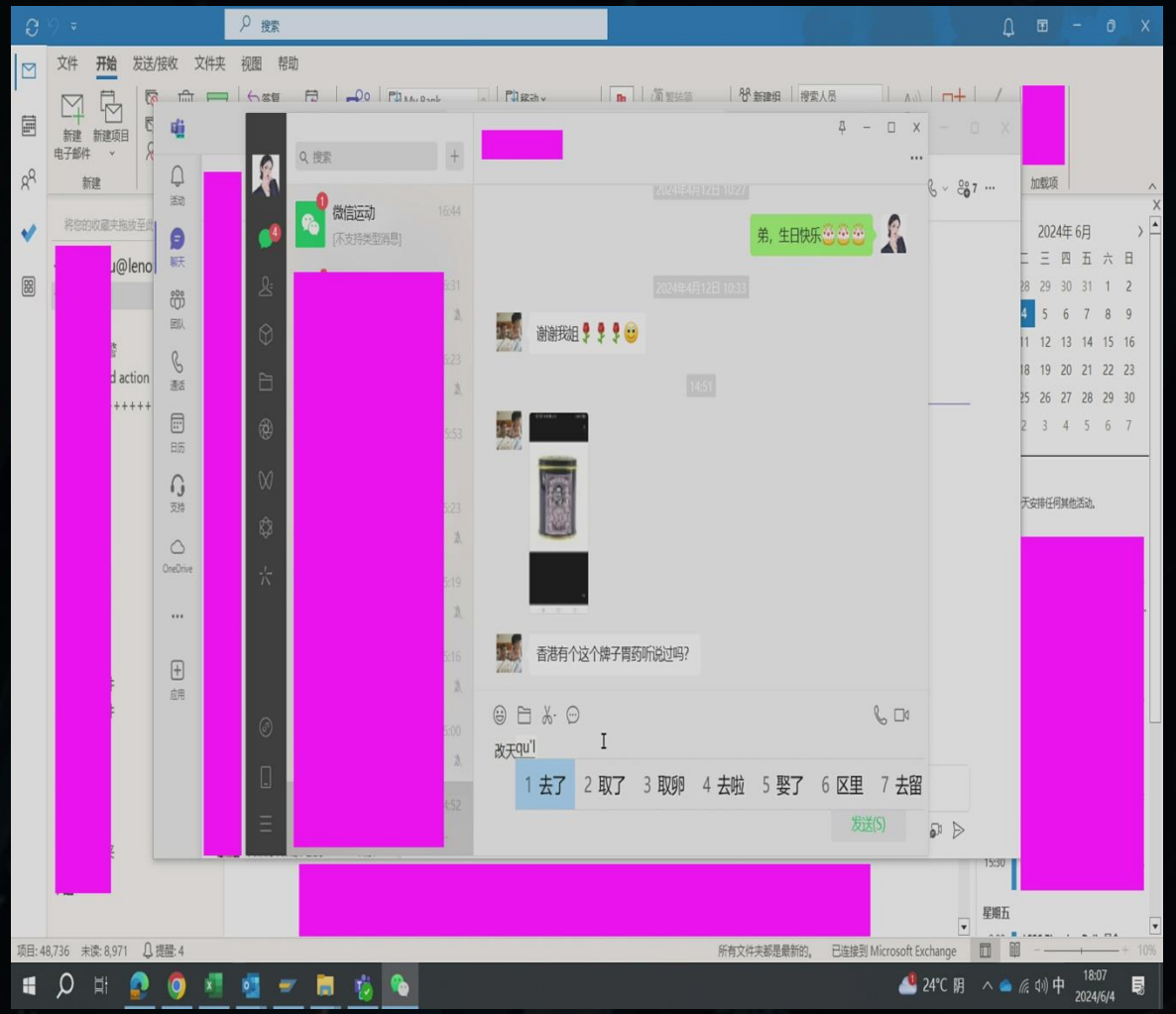
信息窃取（外转发）

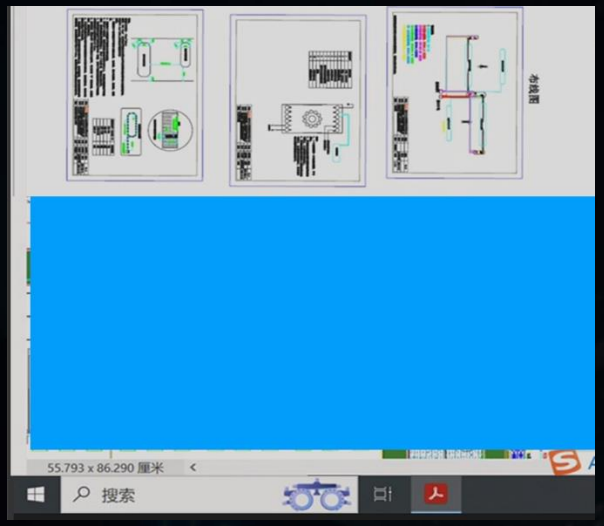

Room Available


demoSC
demo of screen crab
Devices
Device Name
Description
Device MAC
screenCrab2
home

信息窃取





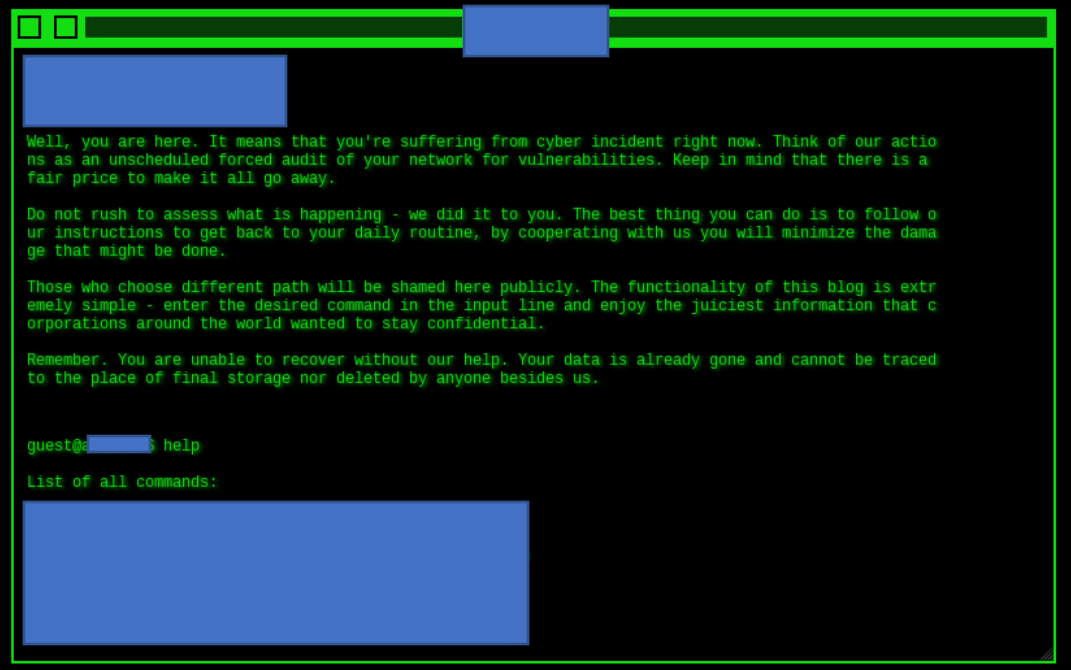


Office文档
邮件
会议
报告
内部工具与网站
保密信息

没有获取

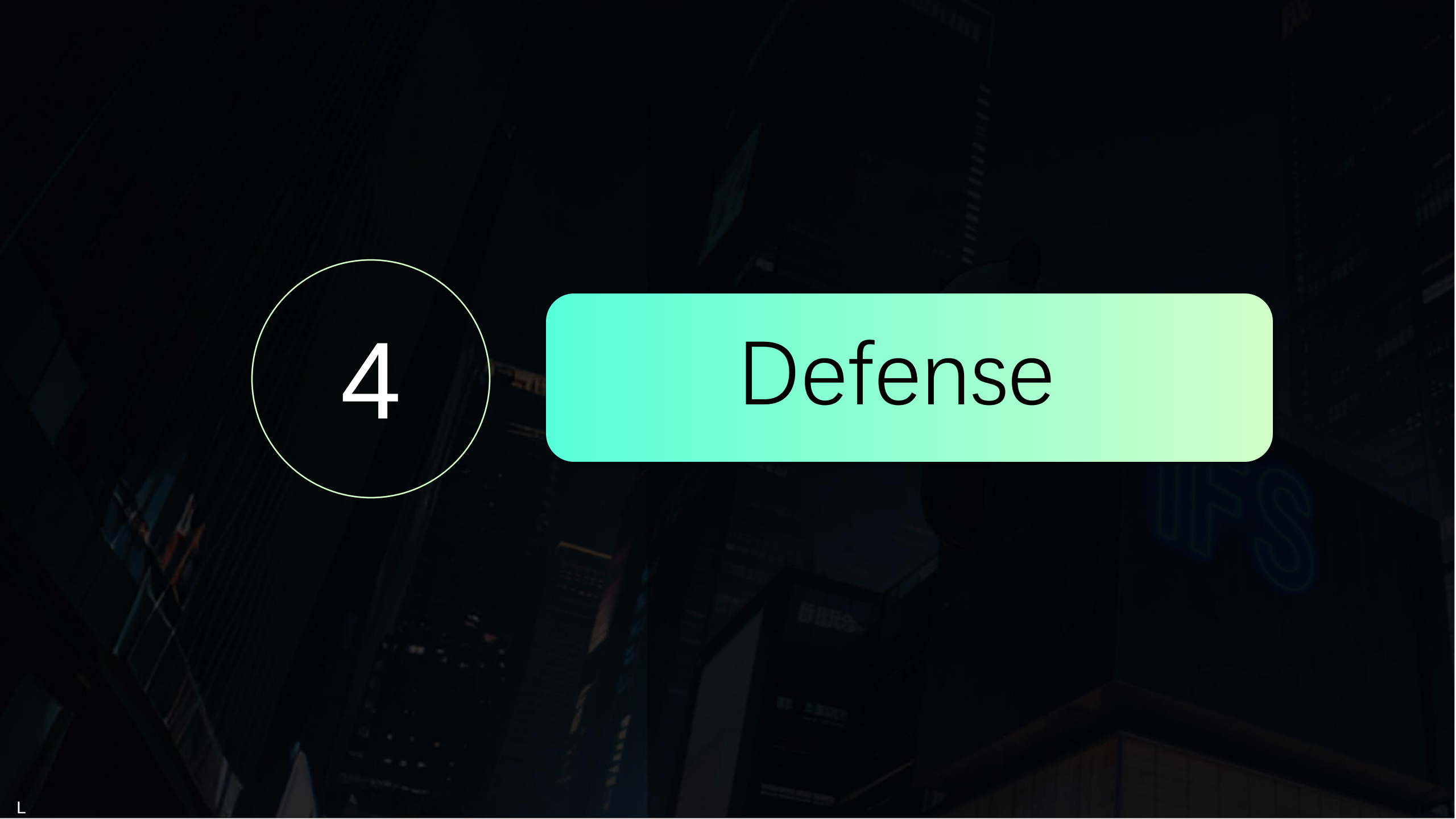
- root
- Access
- 凭据

那没用吗?



这是什么威胁?

类似事件平均成本
$5百万


4
Defense

防御 1 - 安全意识

1. 威胁存在
2. 连接前先检查
3. 有疑问就说出来

防御 2 - 技术

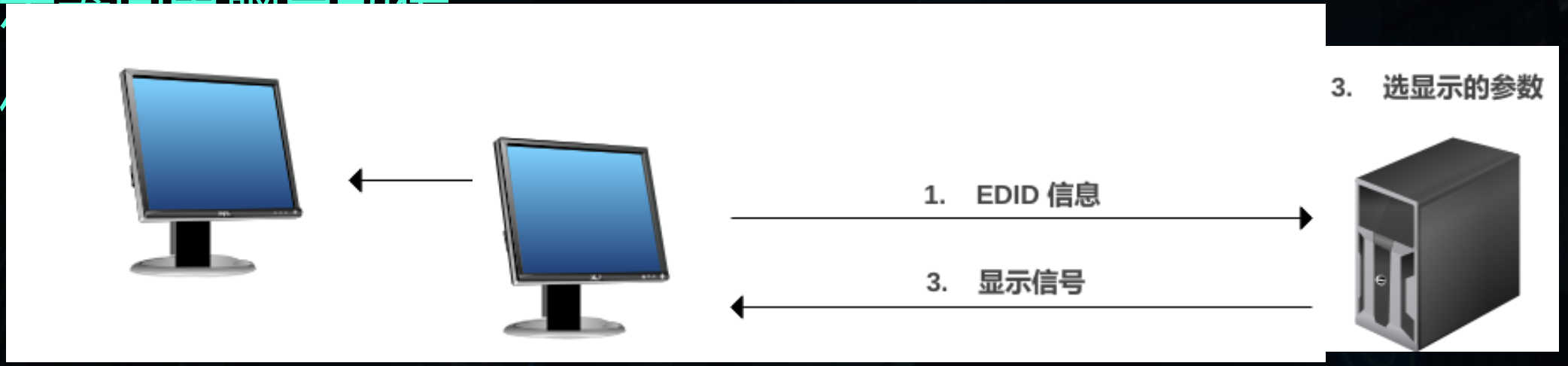
EDID

设备怎么通信?

是一种显[illegible]

送其参数[illegible]

- 分辨率
- 刷新率
- 品牌型号等



防御 2 - 技术

怎么获取EDID信息?

- Linux - i2cdump

实验 - 20个设备

- Control
- vga, hdmi
- 3 个screen crab
- 指纹

```
     0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f    0123456789abcdef
00: 00 ff ff ff ff ff ff 00 63 18 30 00 01 00 00 00    ........c?0.?...
10: 08 1e 01 03 80 90 52 78 0a cf 74 a3 57 4c b0 23    ??????Rx??t?WL?#
20: 09 48 4c 00 00 00 01 01 01 ff 01 ff ff 01 01 01    ?HL...???.?..???
30: 01 01 01 01 01 20 04 74 00 30 f2 70 5a 80 b0 58    ????? ?t.0?pZ??X
40: 8a 00 c4 8e 21 00 00 1e 02 3a 80 18 71 38 2d 40    ?.??!..??:??q8-@
50: 58 2c 45 00 8c 20 53 00 00 1e 00 00 00 fc 00 4c    X,E.? S..?...?.L
60: 58 0a 20 20 20 20 20 20 20 20 20 20 00 00 00 fd    X?          ...?
70: 00 3b 46 1f 8c 3c 00 0a 20 20 20 20 20 20 01 39    .;F??<.?      ?9
80: 02 03 4e f2 56 05 84 03 01 12 13 14 16 07 90 1f    ??N?V???????????
90: 20 22 5d 5f 60 61 5e 02 06 11 15 26 09 07 07 11     "]_`a^????&????
a0: 07 06 83 01 00 00 e2 00 ff 6e 03 0c 00 20 00 78    ????..?..n??. .x
b0: 44 20 40 84 01 02 03 04 67 d8 5d c4 01 78 80 07    D @?????g?]??x??
c0: e3 05 c3 01 e5 0f 00 80 19 00 e3 06 05 01 8c 0a    ??????.??.??????
d0: d0 8a 20 e0 2d 10 10 3e 96 00 c4 8e 21 00 00 18    ?? ?-??>?.??!..?
e0: 8c 0a a0 14 51 f0 16 00 26 7c 43 00 c4 8e 21 00    ????Q??.&|C.??!.
f0: 00 98 00 00 00 00 00 00 00 00 00 00 00 00 00 cc    .?.............?
```

```
     0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f    0123456789abcdef
00: 00 ff ff ff ff ff ff 00 63 18 30 00 01 00 00 00    ........c?0.?...
10: 08 1e 01 03 80 90 52 78 0a cf 74 a3 57 4c b0 23    ??????Rx??t?WL?#
20: 09 48 4c 00 00 00 01 01 01 ff 01 ff ff 01 01 01    ?HL...???.?..???
30: 01 01 01 01 01 20 04 74 00 30 f2 70 5a 80 b0 58    ????? ?t.0?pZ??X
40: 8a 00 c4 8e 21 00 00 1e 02 3a 80 18 71 38 2d 40    ?.??!..??:??q8-@
50: 58 2c 45 00 8c 20 53 00 00 1e 00 00 00 fc 00 4c    X,E.? S..?...?.L
60: 58 0a 20 20 20 20 20 20 20 20 20 20 00 00 00 fd    X?          ...?
70: 00 3b 46 1f 8c 1e 00 0a 20 20 20 20 20 20 01 57    .;F???.?      ?W
80: 02 03 31 f2 56 05 84 03 01 12 13 14 16 07 90 1f    ??1?V???????????
90: 20 22 5d 5f 00 00 5e 02 06 11 15 26 09 07 07 11     "]_..^????&????
a0: 07 06 6e 03 0c 00 20 00 78 44 20 40 84 01 02 03    ??n??. .xD @????
b0: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ?...............
c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c4    ...............?
```

防御 1+2

安全意识 + 技术

防御 3

TSCM

M

5 Conclusions

- Screen crab is good tool for the Red Team arsenal (Stealt, no traditional detection)
- Defense is better if is combined

Security is a Process