9/20 (二) 16:00 - 16:30 7F

金錢或權力？
線上娛樂產業面對的 APT 行動

To loot or Not to Loot? That Is Not a Question !
When State-Nexus APT Targets Online Entertainment Industry !

Charles Li, Che Chang

TEAMT5
杜浦數位安全
Persistent Cyber Threat Hunters

Speaker

Charles Li

TeamT5

Chief Analyst

Speaker

Che Chang

TeamT5

Senior CTI Analyst

AGENDA

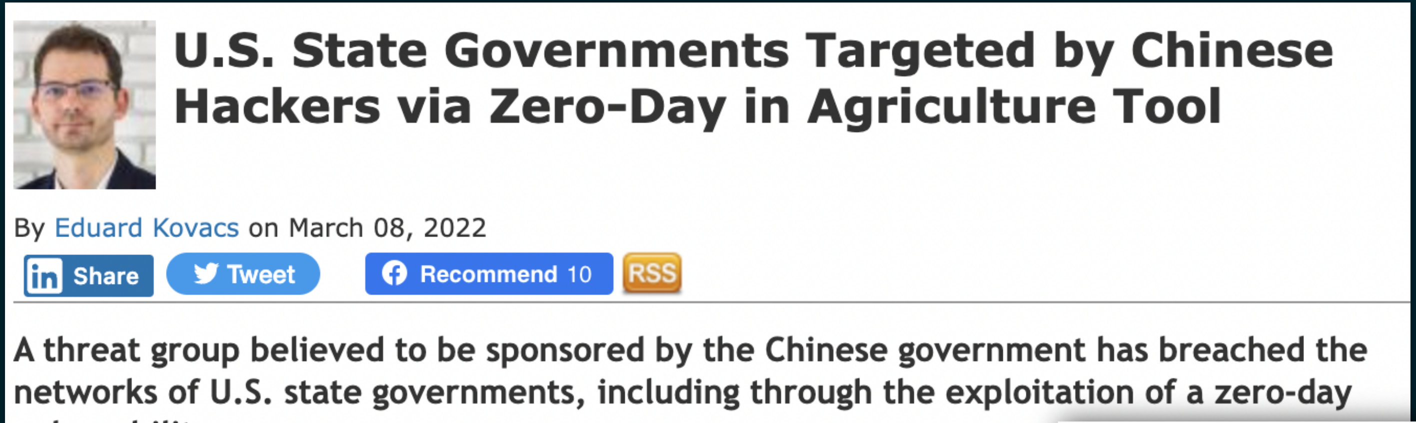
01 Introduction: What is Online Entertainment?

02 APTs in the Game

03 TTPs: What and How in Kill Chain

04 Strategic Analysis

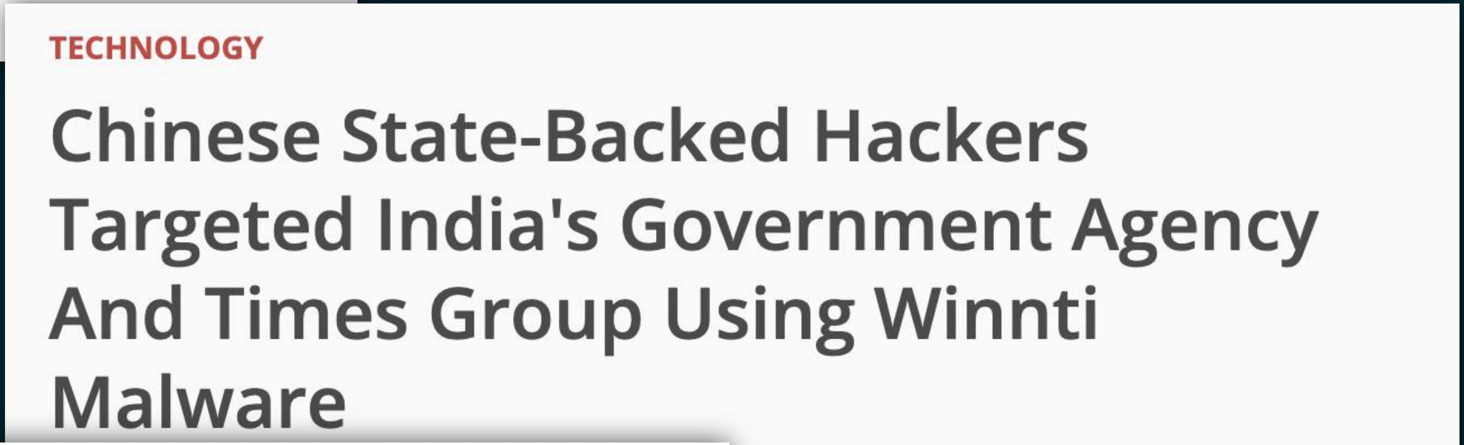
05 Mitigation and Key Takeaway



U.S. State Governments Targeted by Chinese Hackers via Zero-Day in Agriculture Tool

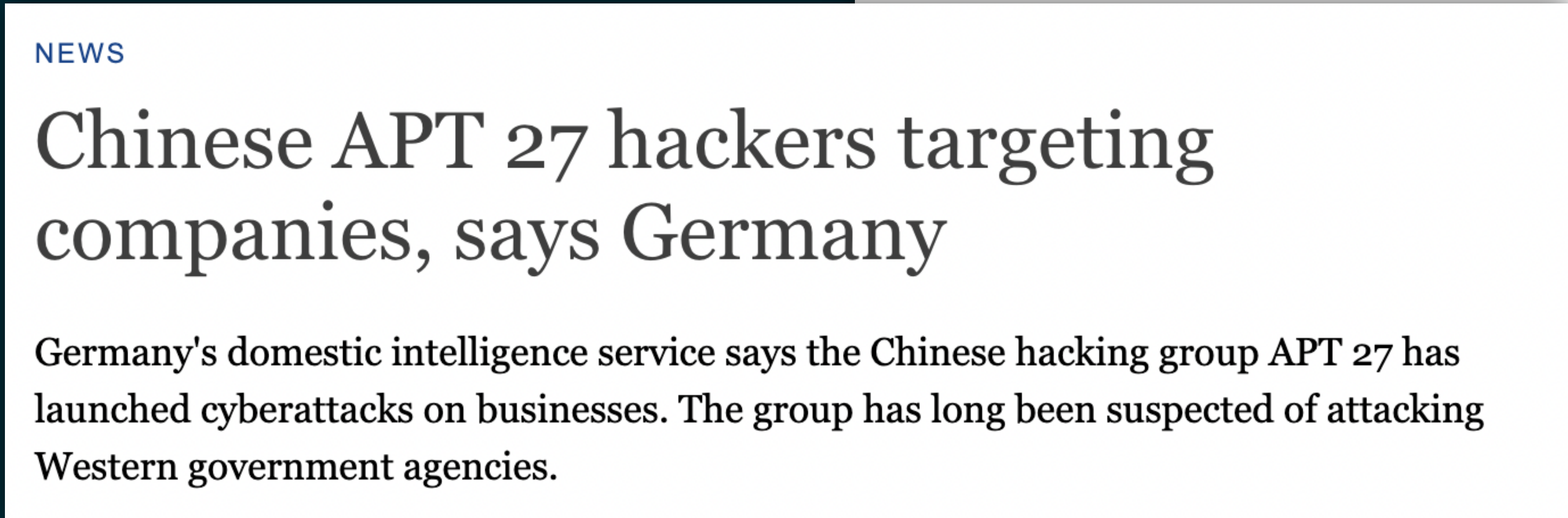
By Eduard Kovacs on March 08, 2022

A threat group believed to be sponsored by the Chinese government has breached the networks of U.S. state governments, including through the exploitation of a zero-day vulnerability.



TECHNOLOGY

Chinese State-Backed Hackers Targeted India's Government Agency And Times Group Using Winnti Malware



NEWS

Chinese APT 27 hackers targeting companies, says Germany

Germany's domestic intelligence service says the Chinese hacking group APT 27 has launched cyberattacks on businesses. The group has long been suspected of attacking Western government agencies.

What is Online Entertainment?

Online Entertainment Industry Chain

Money & Gamblers

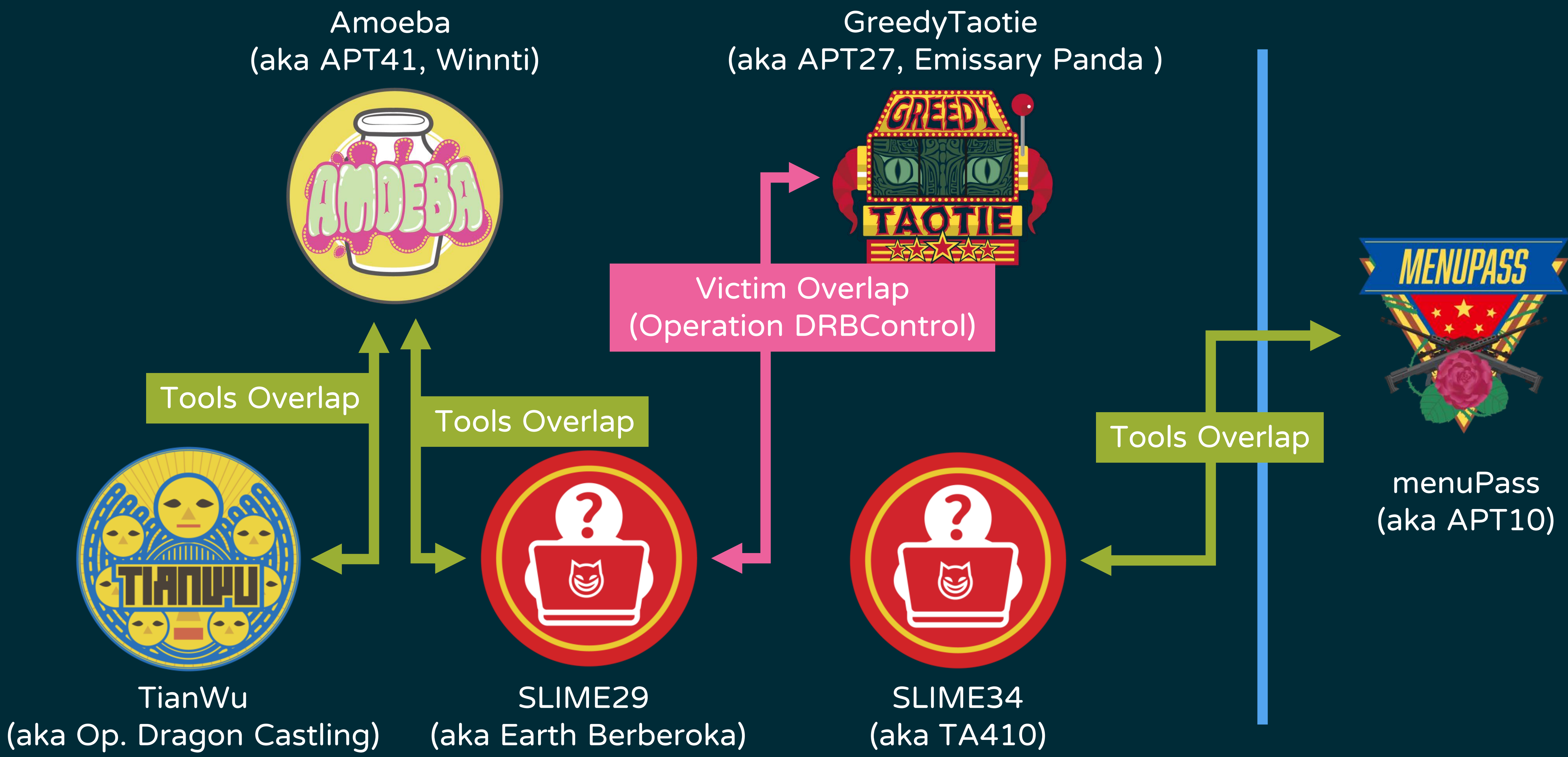
Engineers &
Customer Service

Headquarter

- Industry Chain Worldwide (most illegal)
- Lucrative Nature
- Various way to "Entertain" (to game/gamble)
  Board Games, Sports, Video games, lotteries…

TEAMT5
杜浦數位安全

Players in the Game



Amoeba
(aka APT41, Winnti)

GreedyTaotie
(aka APT27, Emissary Panda)

Victim Overlap
(Operation DRBControl)

Tools Overlap

Tools Overlap

Tools Overlap

menuPass
(aka APT10)

TianWu
(aka Op. Dragon Castling)

SLIME29
(aka Earth Berberoka)

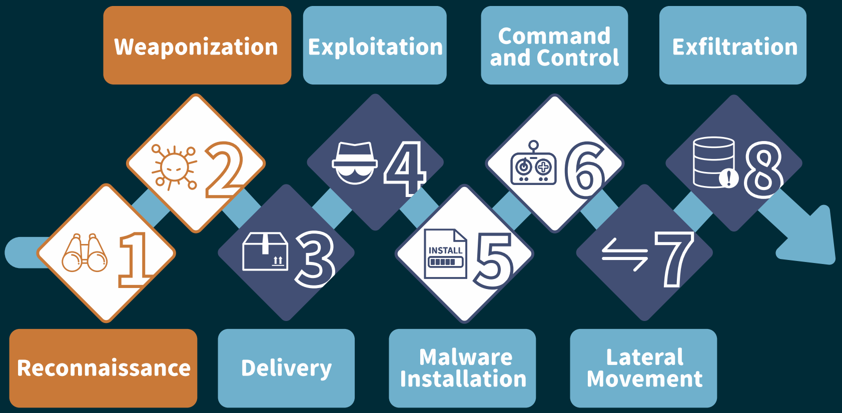
SLIME34
(aka TA410)

TTPs: Initial Access

Weaponization & Reconnaissance

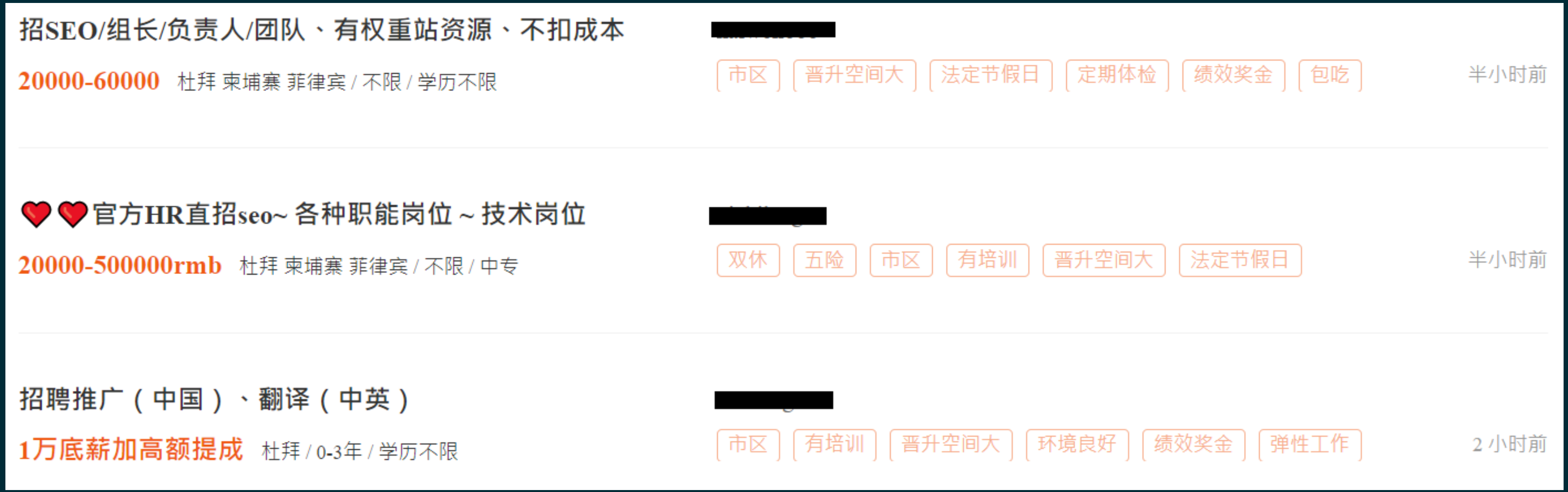
Weaponization

- Mostly applying off-the-shelf tools or modifying for operations
- Proprietary tools developed for maintaining access or LM



3 Hypotheses for Reconnaissance

- Scenario1: Underground or secret sources
- Scenario2: Recruiting websites or forums



招SEO/组长/负责人/团队、有权重站资源、不扣成本 [redacted]
20000-60000 杜拜 柬埔寨 菲律宾 / 不限 / 学历不限
市区 晋升空间大 法定节假日 定期体检 绩效奖金 包吃 半小时前

❤❤官方HR直招seo~ 各种职能岗位 ~ 技术岗位 [redacted]
20000-500000rmb 杜拜 柬埔寨 菲律宾 / 不限 / 中专
双休 五险 市区 有培训 晋升空间大 法定节假日 半小时前

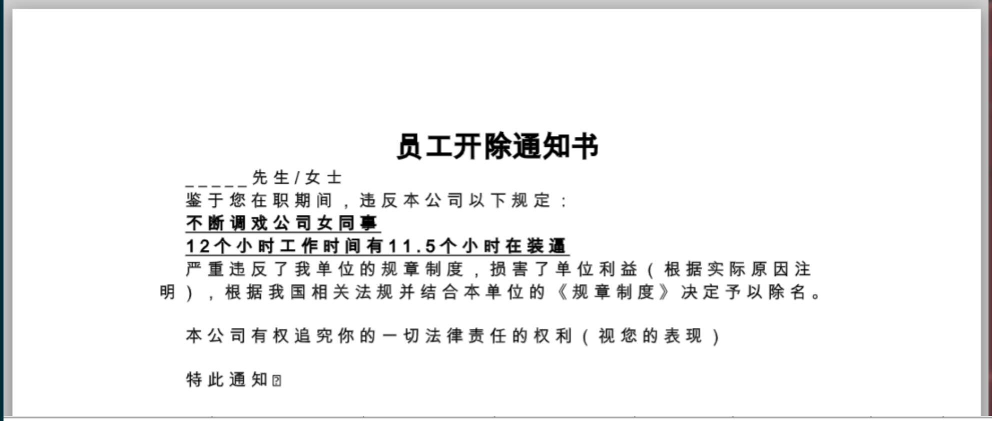
招聘推广（中国）、翻译（中英） [redacted]
1万底薪加高额提成 杜拜 / 0-3年 / 学历不限
市区 有培训 晋升空间大 环境良好 绩效奖金 弹性工作 2 小时前

- Scenario 3: Distributors

TEAMT5
杜 浦 數 位 安 全

Phishing Employees

- Spear phishing employees of targeted companies
- Using daily work related documents (web design photos, financial statements, pink slip) to lure users into opening



员工开除通知书

_____先生/女士

鉴于您在职期间，违反本公司以下规定：

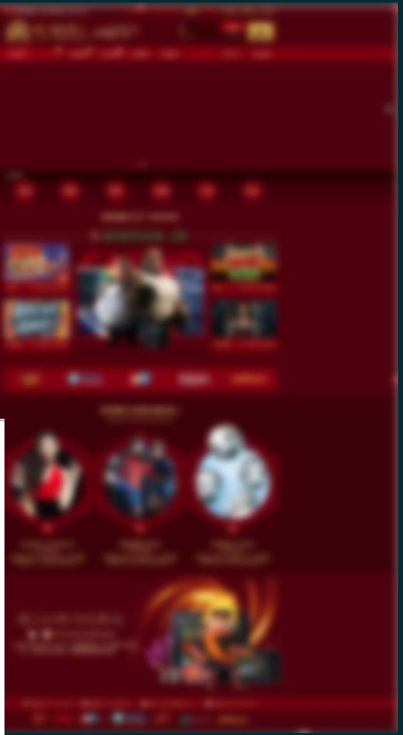
不断调戏公司女同事

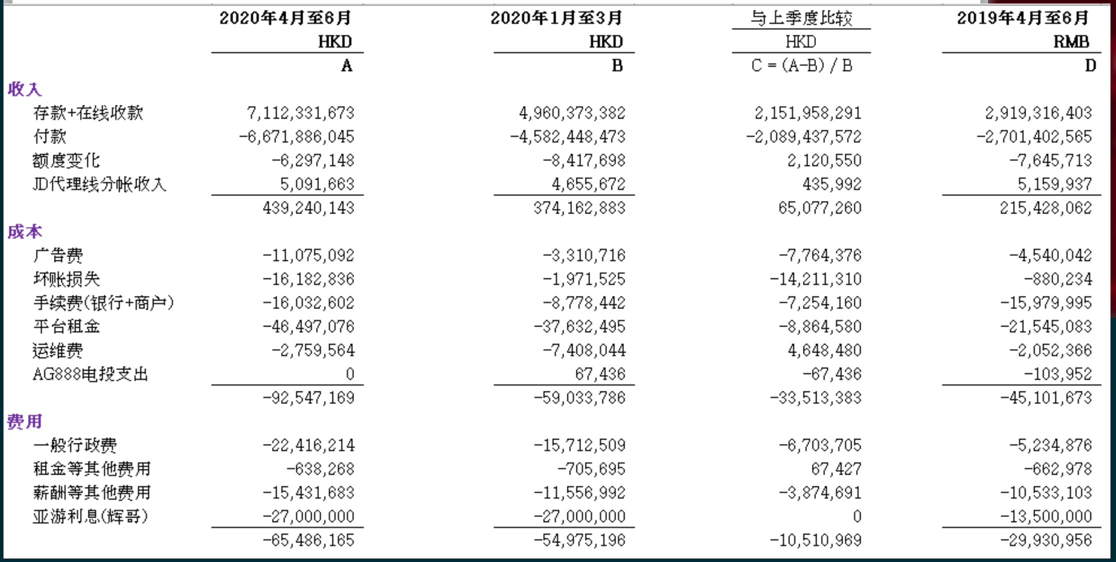
12个小时工作时间有11.5个小时在装逼

严重违反了我单位的规章制度，损害了单位利益（根据实际原因注明），根据我国相关法规并结合本单位的《规章制度》决定予以除名。

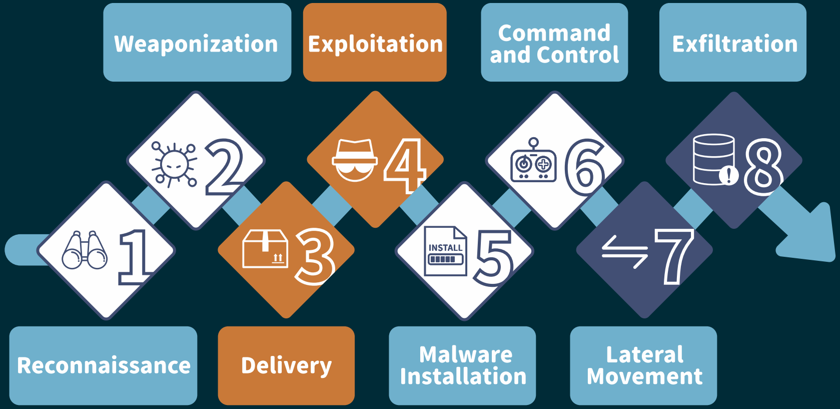
本公司有权追究你的一切法律责任的权利（视您的表现）

特此通知□



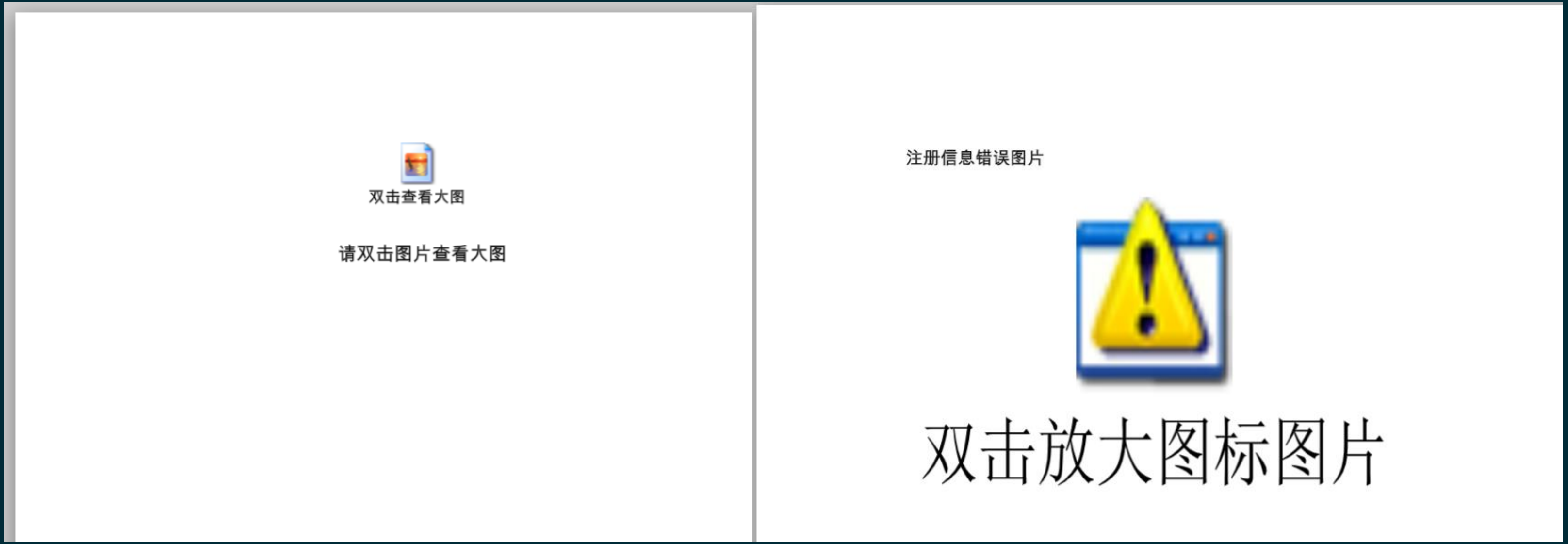


	2020年4月至6月	2020年1月至3月	与上季度比较	2019年4月至6月
	HKD	HKD	HKD	RMB
	A	B	C = (A-B) / B	D
收入				
存款+在线收款	7,112,331,673	4,960,373,382	2,151,958,291	2,919,316,403
付款	-6,671,886,045	-4,582,448,473	-2,089,437,572	-2,701,402,565
额度变化	-6,297,148	-8,417,698	2,120,550	-7,645,713
JD代理线分帐收入	5,091,663	4,655,672	435,992	5,159,937
	439,240,143	374,162,883	65,077,260	215,428,062
成本				
广告费	-11,075,092	-3,310,716	-7,764,376	-4,540,042
坏账损失	-16,182,836	-1,971,525	-14,211,310	-880,234
手续费(银行+商户)	-16,032,602	-8,778,442	-7,254,160	-15,979,995
平台租金	-46,497,076	-37,632,495	-8,864,580	-21,545,083
运维费	-2,759,564	-7,408,044	4,648,480	-2,052,366
AG888电投支出	0	67,436	-67,436	-103,952
	-92,547,169	-59,033,786	-33,513,383	-45,101,673
费用				
一般行政费	-22,416,214	-15,712,509	-6,703,705	-5,234,876
租金等其他费用	-638,268	-705,695	67,427	-662,978
薪酬等其他费用	-15,431,683	-11,556,992	-3,874,691	-10,533,103
亚游利息(辉哥)	-27,000,000	-27,000,000	0	-13,500,000
	-65,486,165	-54,975,196	-10,510,969	-29,930,956



Phishing Customer supports

- Spear phishing customer supports of the target
- Complaining about system issues and asking supports to open attachments to check

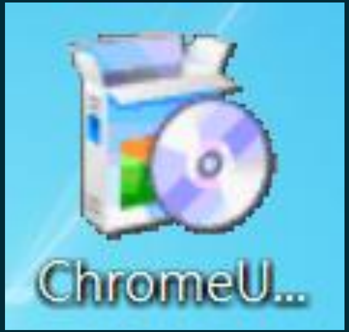


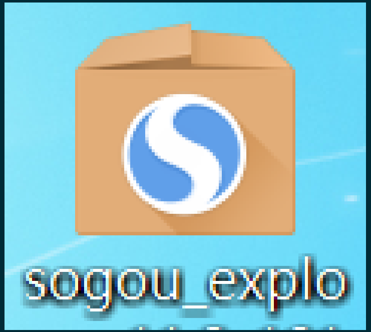
双击查看大图

请双击图片查看大图

注册信息错误图片

双击放大图标图片





Weaponization
Exploitation
Command and Control
Exfiltration

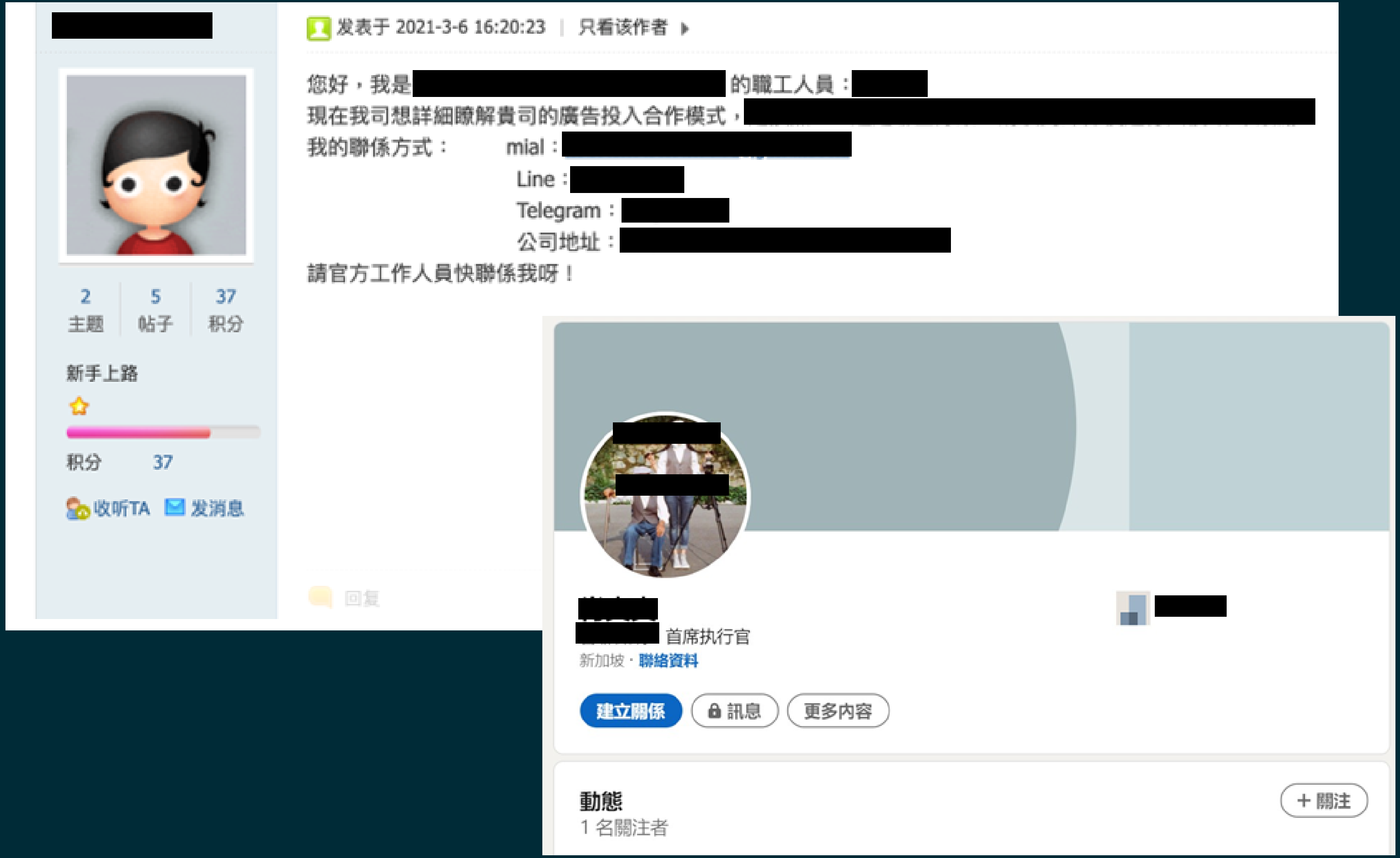
1
2
3
4
INSTALL
5
6
7
8

Reconnaissance
Delivery
Malware Installation
Lateral Movement

TEAMT5 杜浦數位安全

Phishing via SNP

- Crafting profiles on social network platforms, forums
- Approaching sales, ITs, RDs of targeted companies
- Delivering malware by cloud drives or custom web servers



[redacted]

2 主题 5 帖子 37 积分

新手上路

积分 37

收听TA 发消息

发表于 2021-3-6 16:20:23 | 只看该作者

您好，我是[redacted]的職工人員：[redacted]

現在我司想詳細瞭解貴司的廣告投入合作模式，[redacted]

我的聯係方式： mial：[redacted]

Line：[redacted]

Telegram：[redacted]

公司地址：[redacted]

請官方工作人員快聯係我呀！

回复

[redacted]

[redacted]

[redacted] 首席执行官

新加坡・聯絡資料

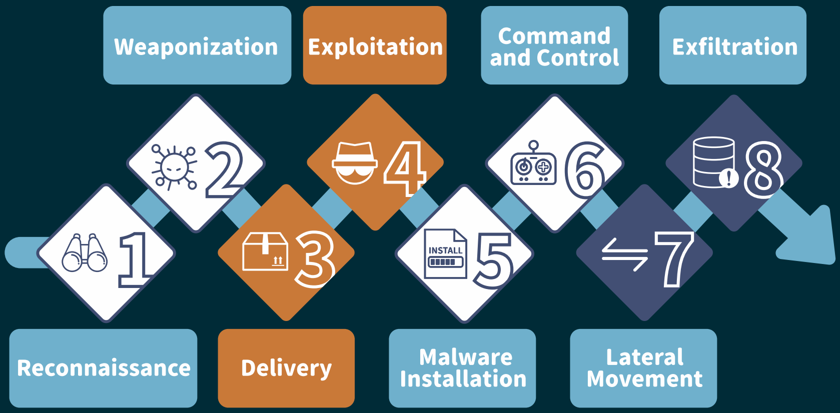
建立關係 訊息 更多內容

[redacted]

動態

1 名關注者

+ 關注



Vulnerability

Weaponization
Exploitation
Command and Control
Exfiltration
2
4
6
8
1
3
5
7
INSTALL
Reconnaissance
Delivery
Malware Installation
Lateral Movement

Exchange server (CVE-2021-34473)

Using ProxyShell exploit to gain a foothold on an exchange server

VPN Server (CVE-2018-13379)

The actor intruded by using a Fortigate exploit to gain VPN credentials

Browser (CVE-2021-38001)

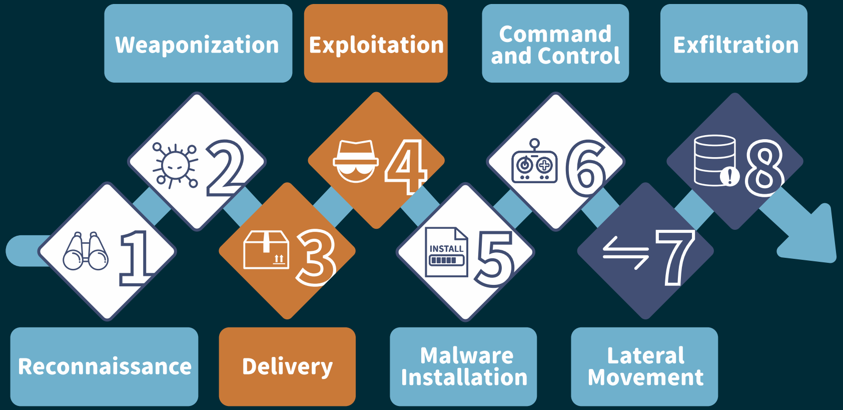
The actor used watering hold attacks and hosted exploit codes on seebug[.]updetasrvers.org

Web and NAS server vulnerabilities

Supply Chain Attack

Compromised ERP System

- first compromised ERP system of the victim via some web vulnerability
- used ERP to distribute several malware include, CrossWalk and FunnySwitch



TEAMT5 杜浦數位安全

Supply Chain Attack

Compromised Official Websites

- Compromised the official website of a cryptocurrency company
- Replaced some installation package with trojanized version

Weaponization
Exploitation
Command and Control
Exfiltration
1
2
3
4
5
6
7
8
INSTALL
Reconnaissance
Delivery
Malware Installation
Lateral Movement

TTPs: Malware & Post Exp.

Malware

Amoeba

- Winnti
- FunnySwitch
- CrossWalk
- Spyder
- Sqlcmsps
- IISAccept

SLIME34

- CobaltStrike beacon
- PlugX
- HelloKety

TianWu

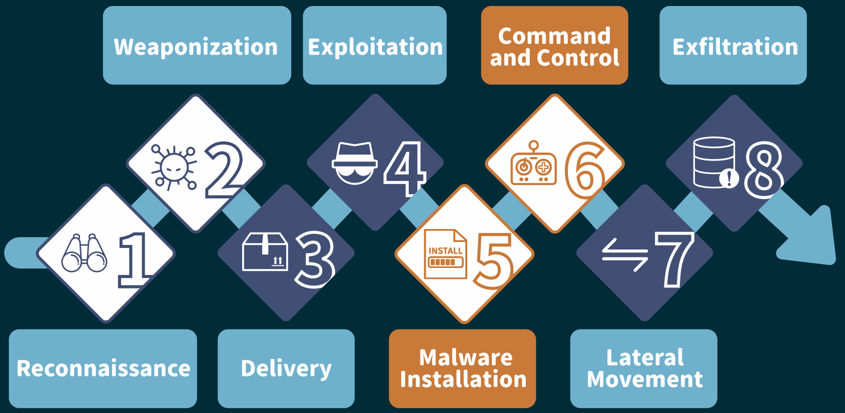
- Pangolin8RAT
- CobaltStrike Beacon

GreedyTaotie

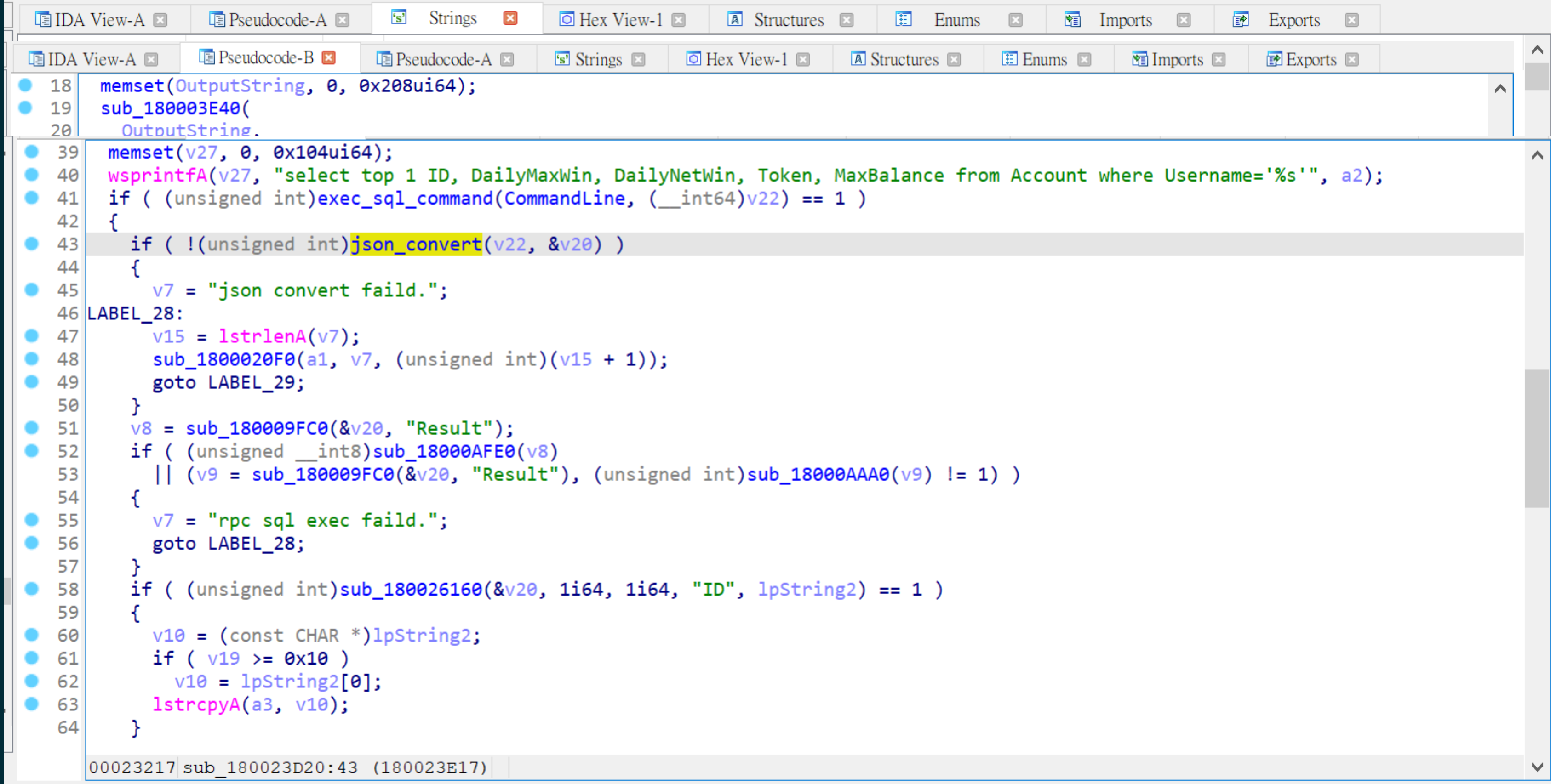
- HyberBro
- ChinaChopper

SLIME29

- PlugX*
- CoinDrop
- Hehedalinux
- RKORAT



IIS Backdoor

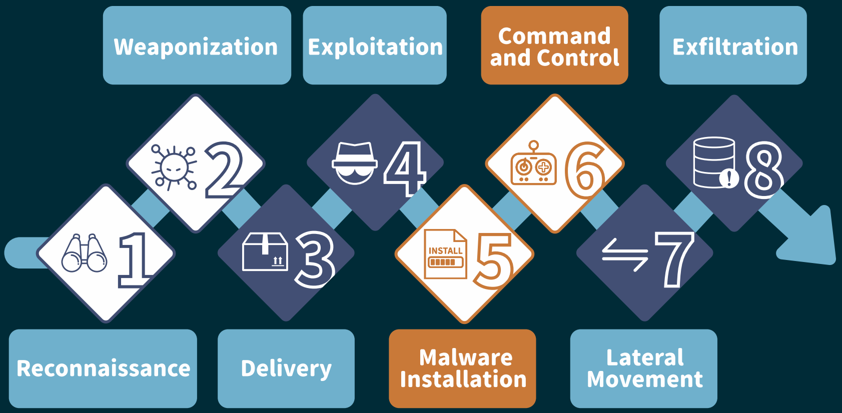


```
memset(OutputString, 0, 0x208ui64);
sub_180003E40(
  OutputString,
```

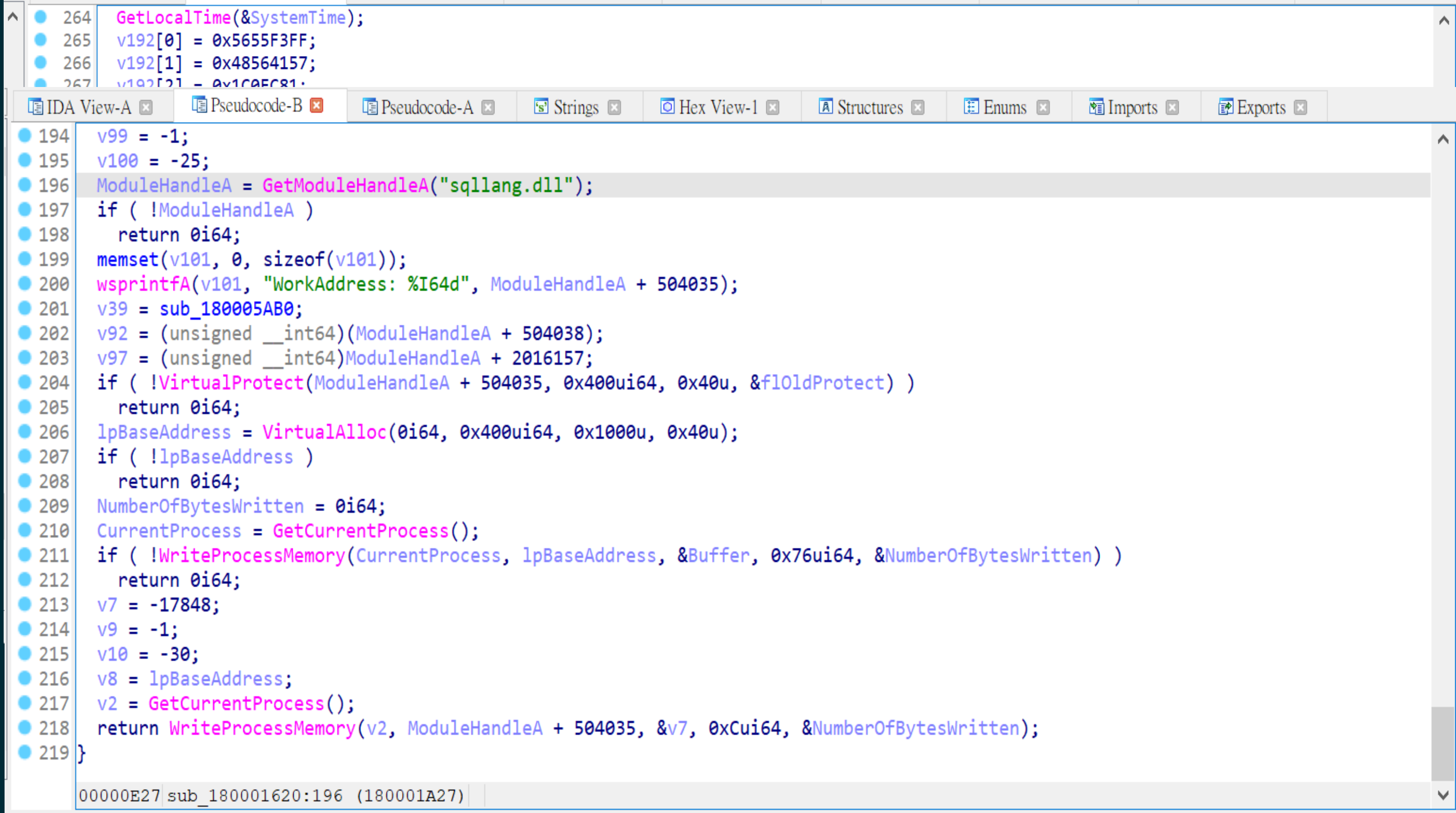
```
memset(v27, 0, 0x104ui64);
wsprintfA(v27, "select top 1 ID, DailyMaxWin, DailyNetWin, Token, MaxBalance from Account where Username='%s'", a2);
if ( (unsigned int)exec_sql_command(CommandLine, (__int64)v22) == 1 )
{
  if ( !(unsigned int)json_convert(v22, &v20) )
  {
    v7 = "json convert faild.";
LABEL_28:
    v15 = lstrlenA(v7);
    sub_1800020F0(a1, v7, (unsigned int)(v15 + 1));
    goto LABEL_29;
  }
  v8 = sub_180009FC0(&v20, "Result");
  if ( (unsigned __int8)sub_18000AFE0(v8)
    || (v9 = sub_180009FC0(&v20, "Result"), (unsigned int)sub_18000AAA0(v9) != 1) )
  {
    v7 = "rpc sql exec faild.";
    goto LABEL_28;
  }
  if ( (unsigned int)sub_180026160(&v20, 1i64, 1i64, "ID", lpString2) == 1 )
  {
    v10 = (const CHAR *)lpString2;
    if ( v19 >= 0x10 )
      v10 = lpString2[0];
    lstrcpyA(a3, v10);
  }
```

```
00023217 sub_180023D20:43 (180023E17)
```

F:\XProject\Project\Salon4\IISAccept\x64\Release\IISAccept.pdb



SQL Backdoor



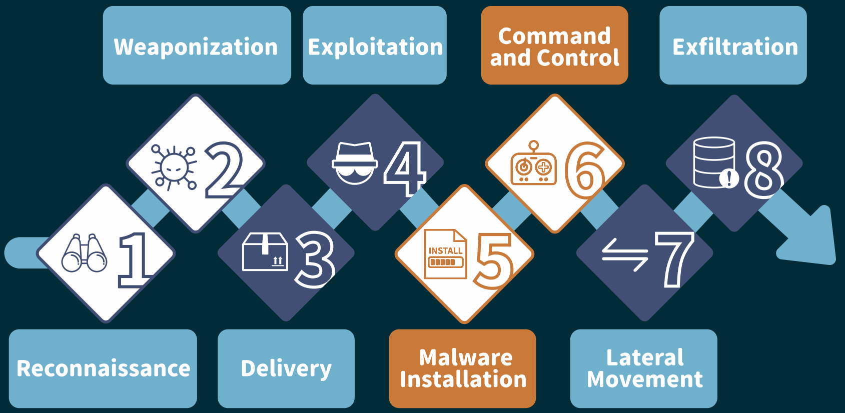
```
GetLocalTime(&SystemTime);
v192[0] = 0x5655F3FF;
v192[1] = 0x48564157;
v192[2] = 0x1C0EC81;
```

```
  v99 = -1;
  v100 = -25;
  ModuleHandleA = GetModuleHandleA("sqllang.dll");
  if ( !ModuleHandleA )
    return 0i64;
  memset(v101, 0, sizeof(v101));
  wsprintfA(v101, "WorkAddress: %I64d", ModuleHandleA + 504035);
  v39 = sub_180005AB0;
  v92 = (unsigned __int64)(ModuleHandleA + 504038);
  v97 = (unsigned __int64)ModuleHandleA + 2016157;
  if ( !VirtualProtect(ModuleHandleA + 504035, 0x400ui64, 0x40u, &flOldProtect) )
    return 0i64;
  lpBaseAddress = VirtualAlloc(0i64, 0x400ui64, 0x1000u, 0x40u);
  if ( !lpBaseAddress )
    return 0i64;
  NumberOfBytesWritten = 0i64;
  CurrentProcess = GetCurrentProcess();
  if ( !WriteProcessMemory(CurrentProcess, lpBaseAddress, &Buffer, 0x76ui64, &NumberOfBytesWritten) )
    return 0i64;
  v7 = -17848;
  v9 = -1;
  v10 = -30;
  v8 = lpBaseAddress;
  v2 = GetCurrentProcess();
  return WriteProcessMemory(v2, ModuleHandleA + 504035, &v7, 0xCui64, &NumberOfBytesWritten);
}
```

```
00000E27 sub_180001620:196 (180001A27)
```

https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

F:\XProject\Salon\sqlcmsPS\x64\Release\sqlcmsPS.pdb



Weaponization

Exploitation

Command and Control

Exfiltration

1 2 3 4 5 6 7 8

Reconnaissance

Delivery

Malware Installation

Lateral Movement

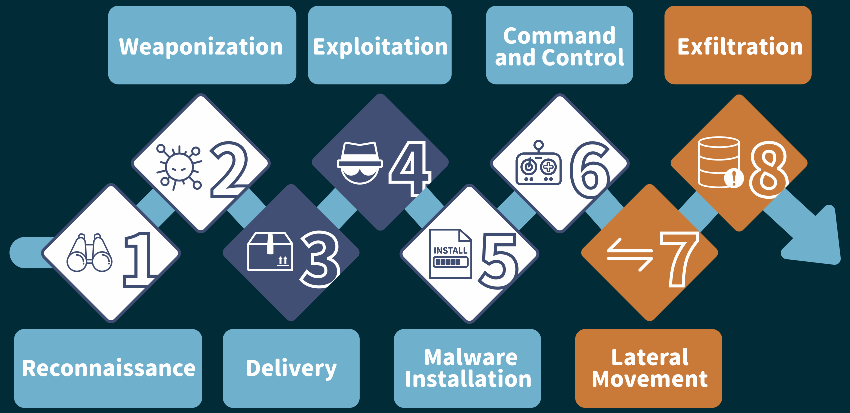
TEAMT5 杜浦數位安全

Lateral Movement

- Mostly Off-the-shelf tools: Nbtscan, PsExec, PwDumps, mimikatz

- RAT harvested credentials, dictionary attacks or exploits (e.g., EternalBlue) are used for privileges escalation

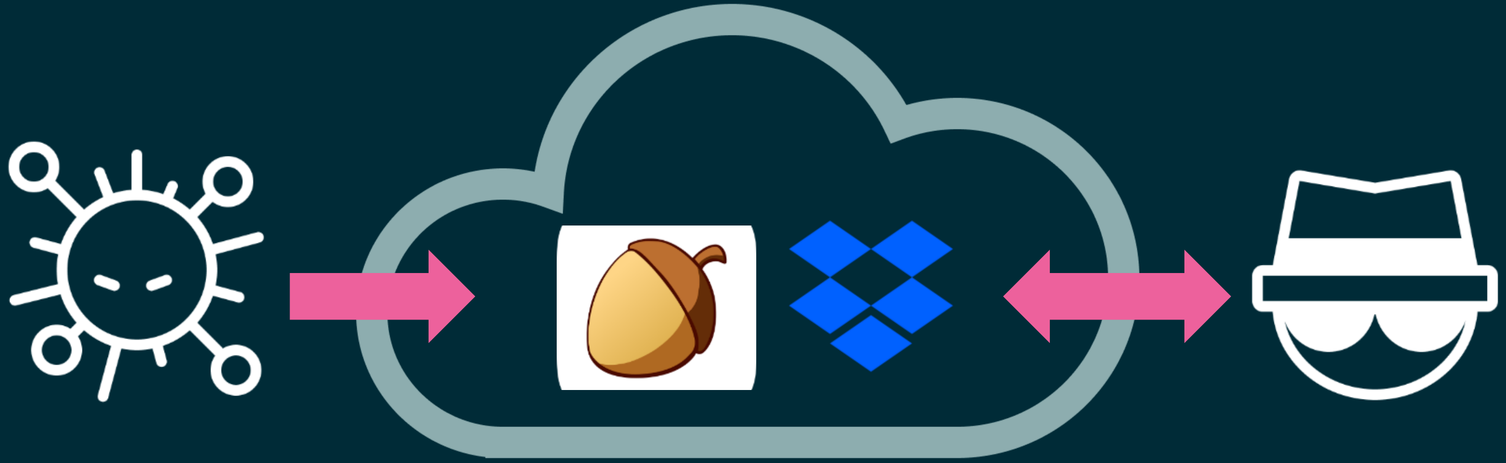
- Two stages of operations are usually adopted:
  Stage1: automatic tools or scripts for environment reconnaissance
  Stage2: manually penetrations interleaved with automatic tools for precise strikes

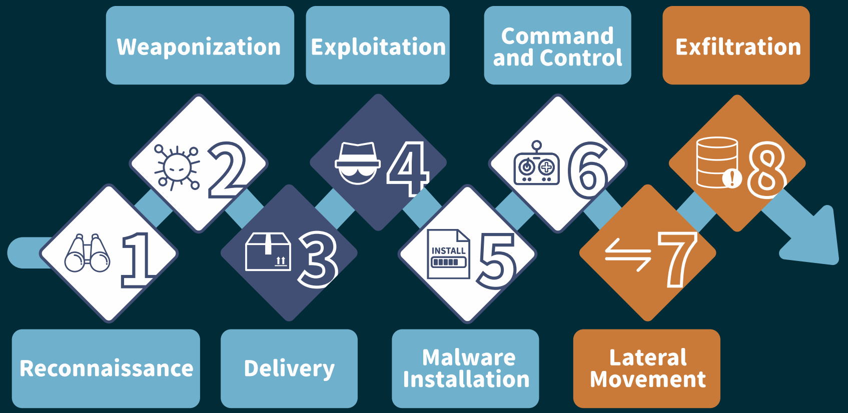


TEAMT5 杜浦數位安全

Exfiltration

- Actors created free accounts on cloud storage platform (堅果雲, DropBox…)
- Malware communicates with clouds for concealment



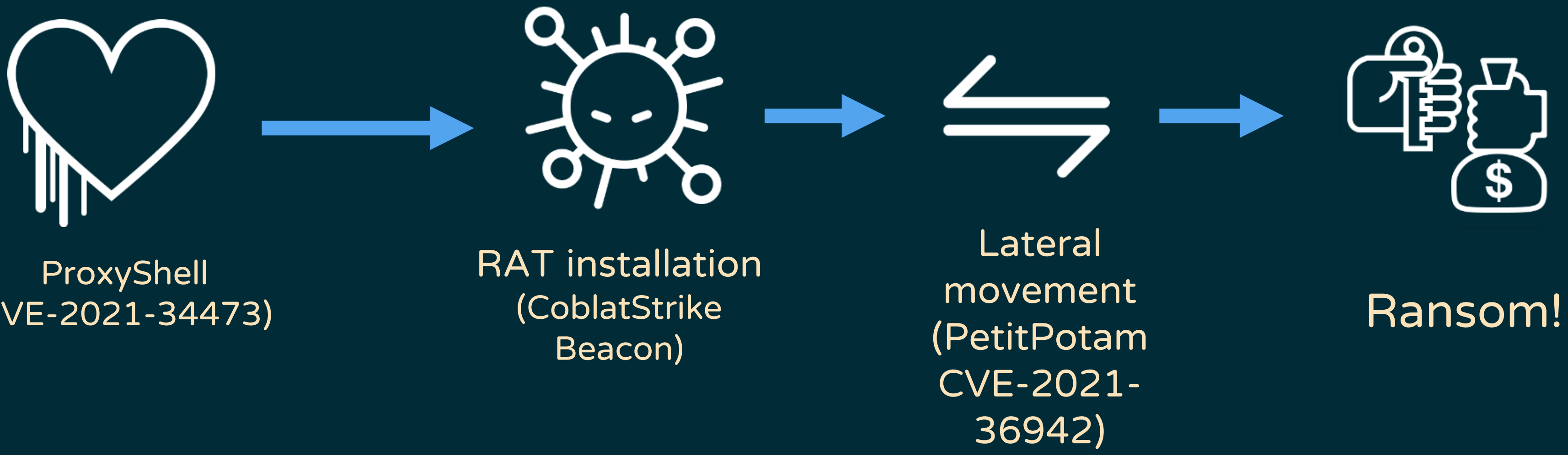


TEAMT5 杜浦數位安全

TTPs: Deploying Ransomware?

SLIME34’s Ransomware

- LockFile, AtomSilo, Rook, NightSky, PandoraRansomware
- Time: 2021 H2 ~ 2022 H1
- Target: the manufacturing, financial services, engineering, legal, business services, and travel and tourism sectors.
- TTP:



ProxyShell (CVE-2021-34473)

RAT installation (CoblatStrike Beacon)

Lateral movement (PetitPotam CVE-2021-36942)

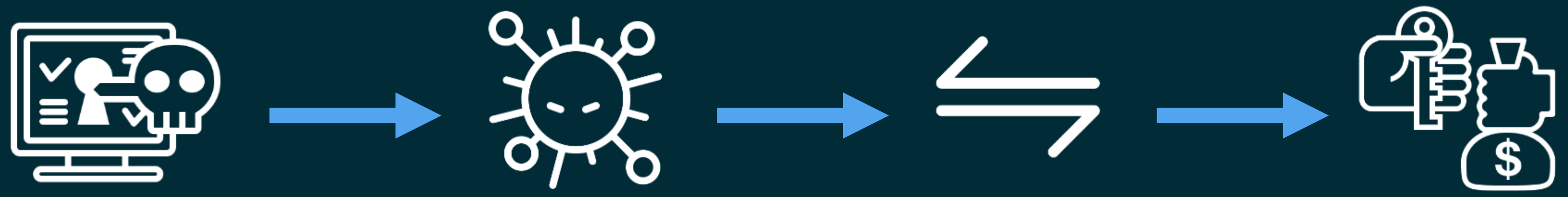
Ransom!

SLIME34

ColdLock

- Time: 2020/05
- Target: Critical Infrastructure, High Tech

- TTP:

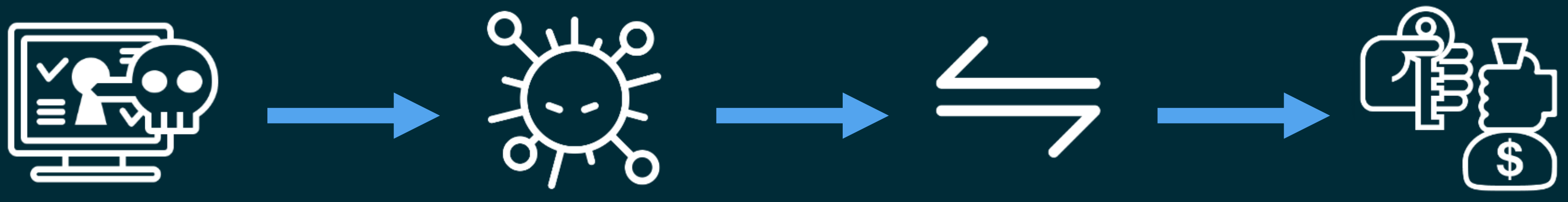


Web compromise → RAT installation (CoblatStrike Beacon) → Lateral movement → Ransom!

Amoeba

Polar Ransomware

- Time: 2020/04
- Target: Media outlet
- TTP:



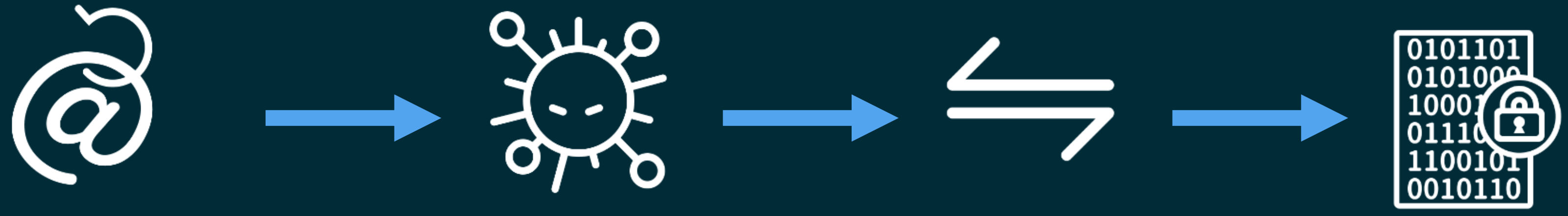
Web compromise → RAT installation (Sysupdate) → Lateral movement → Ransom!

GreedyTaotie

Bitlocker

- Time: Early 2020
- Target: Online Entertainment

- TTP:



Spear phishing → RAT installation → Lateral movement → Encrypt!

SLIME29

Political Motivation behind those APT?

TEAMT5
杜浦數位安全

Should pay much attention to it because…

Money Driven

Information Collection

Of Course !!

Based on our observation, only SLIME29 focused on financial-gain intrusion operations, the rest all have strong political related operations.

SLIME34

Amoeba

GreedyTaotie

TianWu

Cybercrime VS Cyber Espionage: “Indicator of Money”

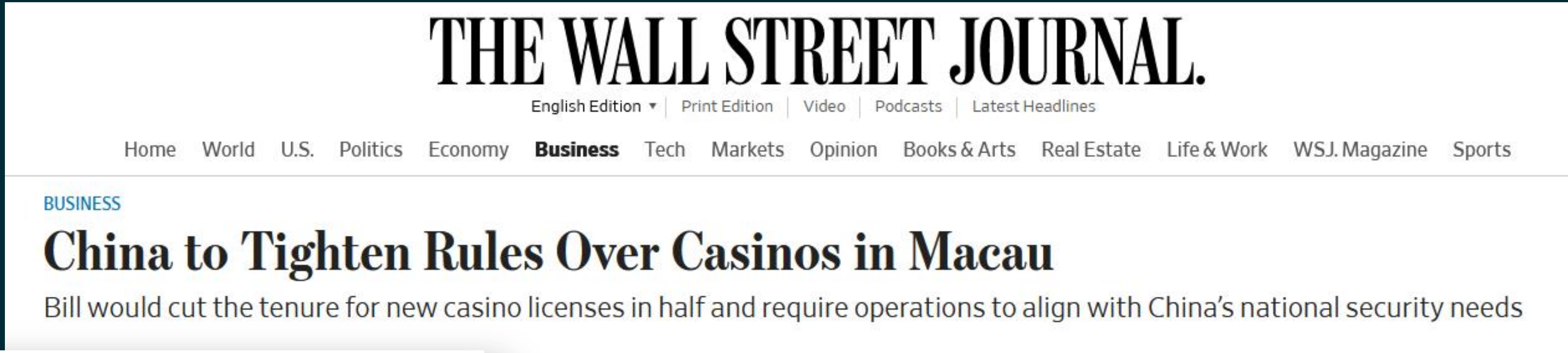
TEAMT5 杜浦數位安全

“Indicator of Money”	Amoeba	GreedyTaoTie	Slime 34	TianWu	Slime 29
Deploy Ransomware	Y	Y	Y	N	Y
Deploy Crypto Miners	Y	Y	N	N	N
Hacker for Hire	Y	Y	N/A	N/A	N/A
Only Targeting Industry with Strong Cash Flow	N	N	N	N	Y

Why the Chinese Government Puts Significant Pressure to Online Entertainment Industry?

TEAMT5
杜浦數位安全

China’s Crackdown

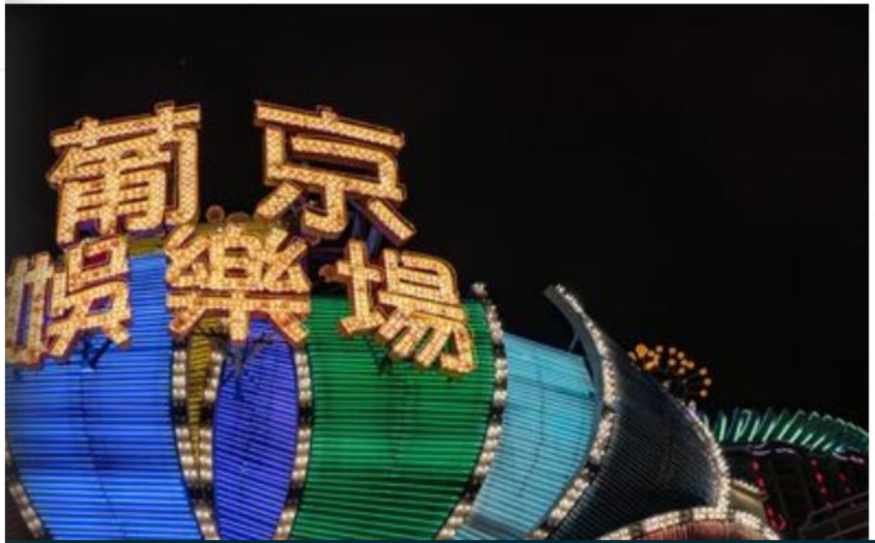


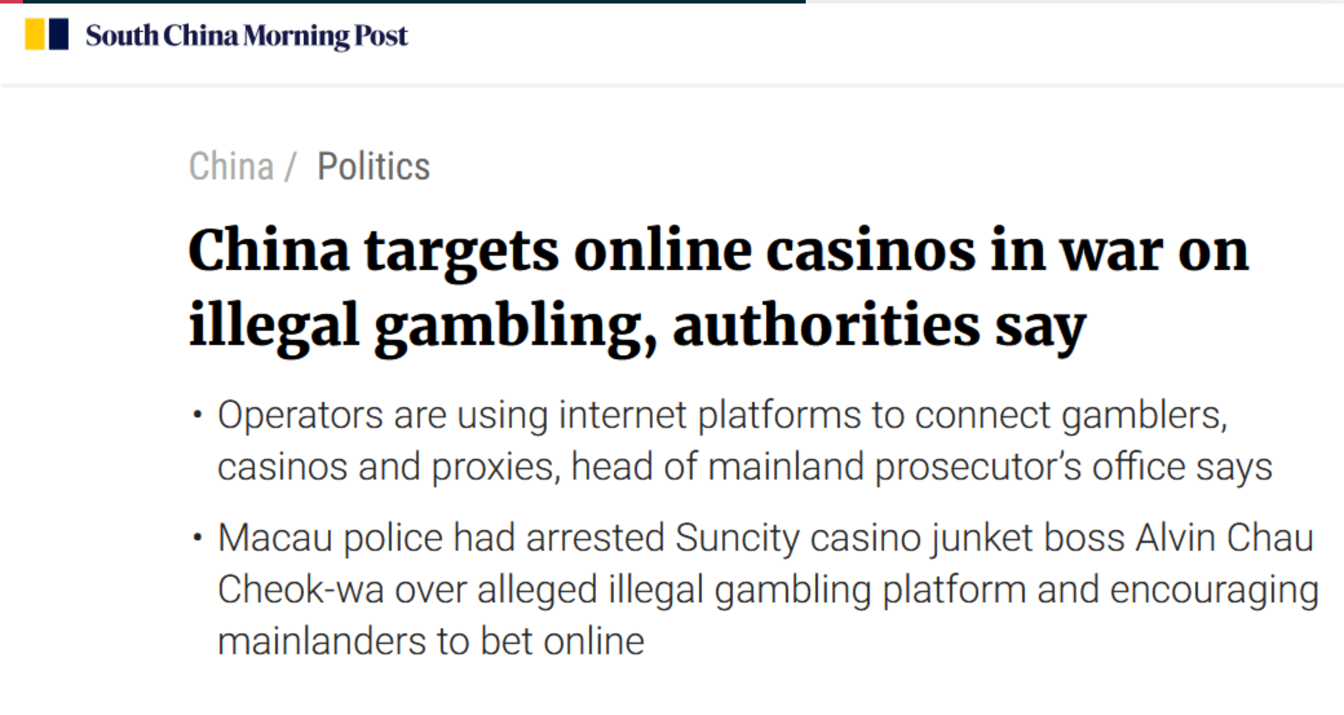
THE WALL STREET JOURNAL.

BUSINESS

China to Tighten Rules Over Casinos in Macau

Bill would cut the tenure for new casino licenses in half and require operations to align with China’s national security needs





South China Morning Post

China / Politics

China targets online casinos in war on illegal gambling, authorities say

- Operators are using internet platforms to connect gamblers, casinos and proxies, head of mainland prosecutor’s office says
- Macau police had arrested Suncity casino junket boss Alvin Chau Cheok-wa over alleged illegal gambling platform and encouraging mainlanders to bet online

Geo-politics/threat landscape

China’s crackdown on gambling industry

- China’s crackdown on Macau gambling industry forced gamblers to move online
- Online gambling skyrocketed during the time of pandemic
- Abundant money and data (personal info and cash flow)

Reason I: Stability

Info collected

Stop Bribery

*Anti-corruption Campaign

Clean up related Infrastructures in China

Take down involved companies

Reason II: The Money

TEAMT5 杜浦數位安全

So how do we Mitigate such Threats?

5 Chinese APT Groups:

- Amoeba (APT41, Winnti)
- GreedyTaotie (APT27, Emissary Panda)
- TianWu
- SLIME34
- SLIME29

ADVERSARY

CAPABILITY

- Reconnaissance techniques: off-the-shelf tools
- Delivery methods: Phishing, Supply Chain Attack
- Attacking exploit / vulnerability in Exchange server, Web, NAS, etc
- Specially Designed RAT, Ransomware
- Lateral movement skills and tools: Mostly Off-the-shelf tools

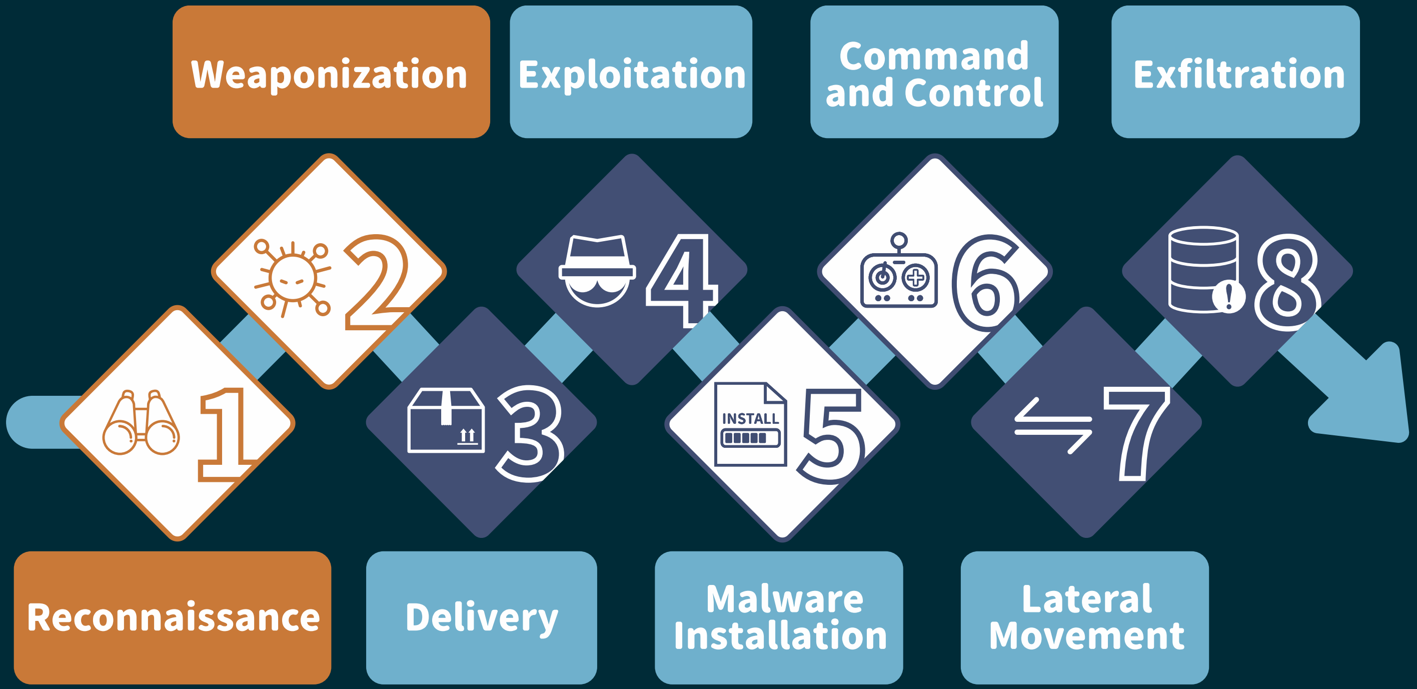
INFRASTRUCTURE

- VPS, 堅果雲, Dropbox, etc

TARGET

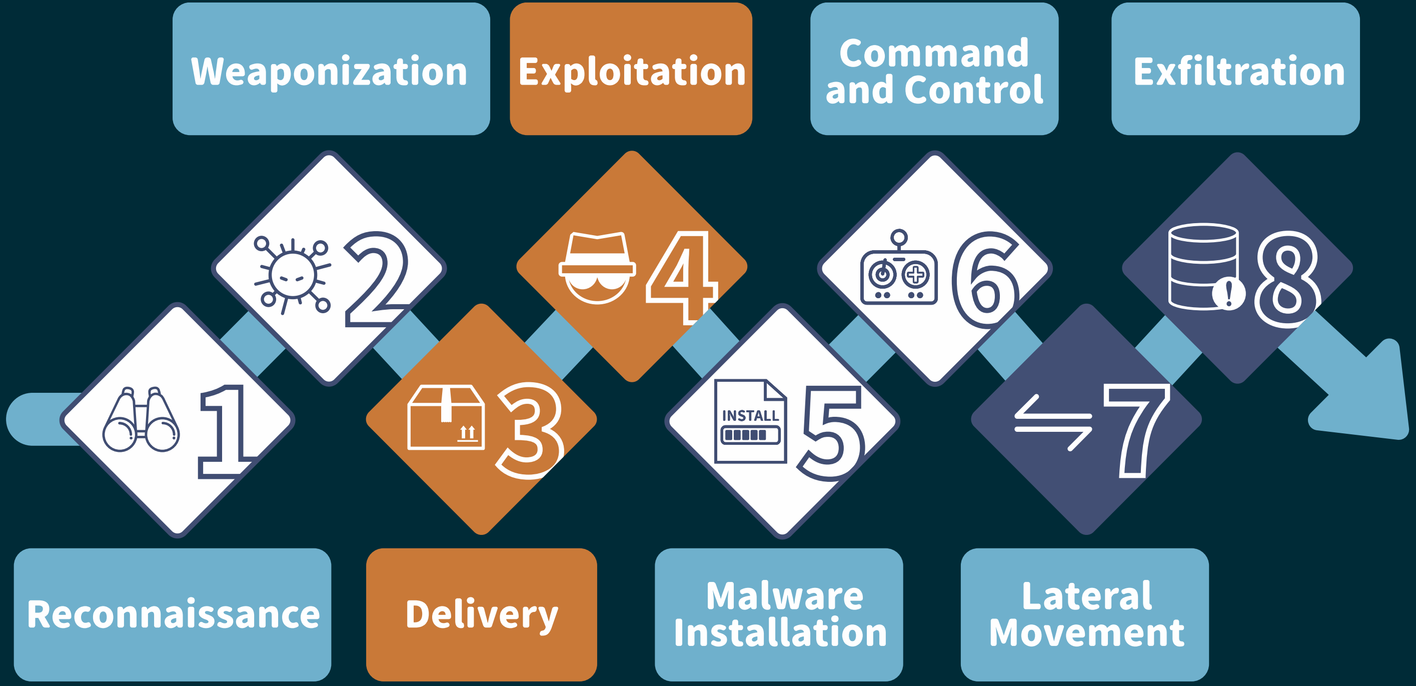
- Purpose: Money and Sensitive Data
- Target countries / regions: APAC
- Target sectors: Online Entertainment industry

Countermeasures



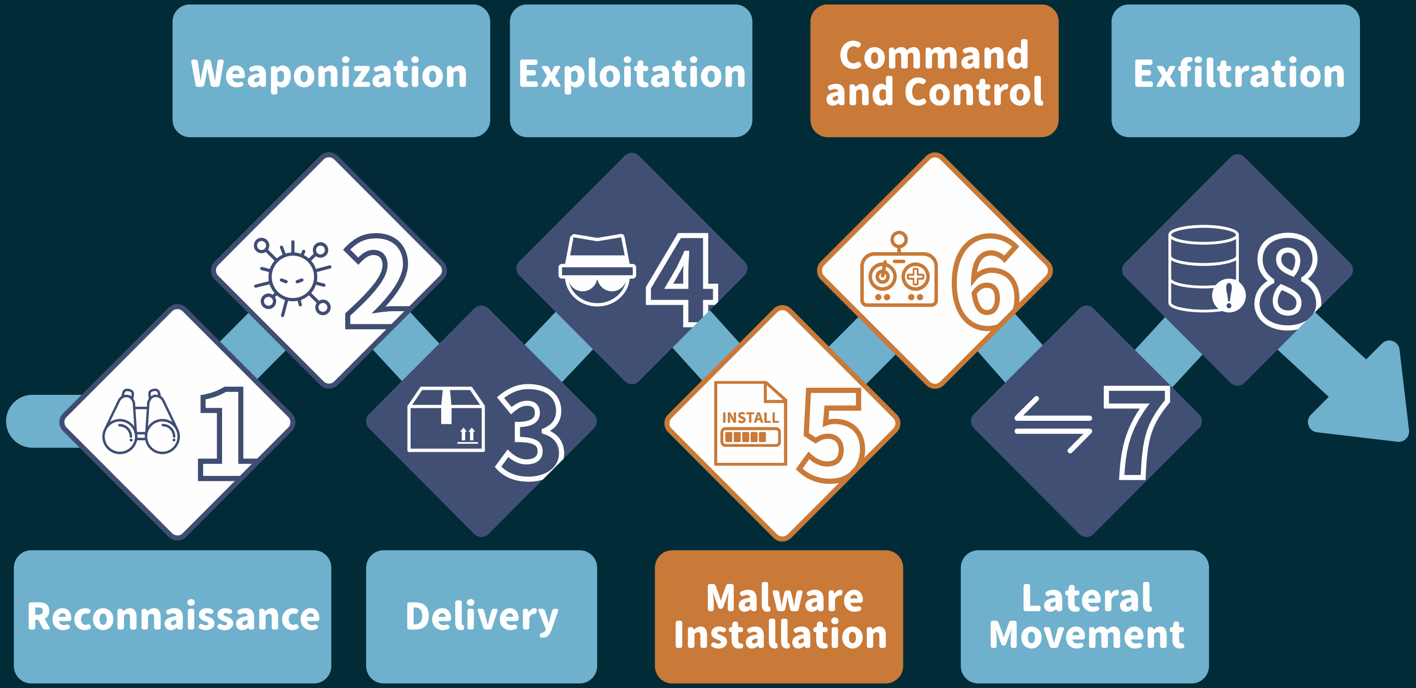
- Isolation between Op. Dev. and OA environment.
- Catch-up with new hacking tools, techniques, etc.. discussed in security community

Countermeasures



- Patch! Patch & Patch, not only for machines but also humans.
- Regular drills will help.

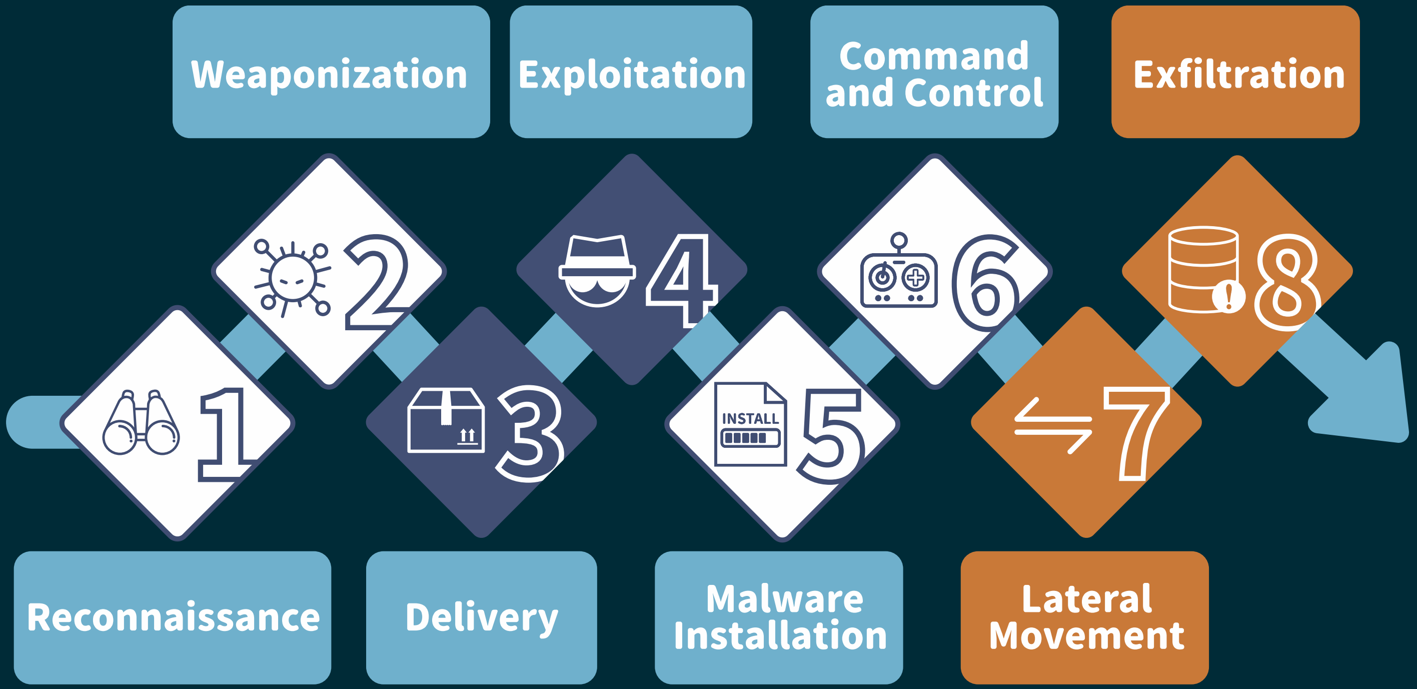
Countermeasures



- RATs usually support various protocols, or leveraging cloud platforms
- Protocols or C2 information are seldom covered in firewalls, IPS, IDS and AV products

TEAMT5 杜浦數位安全

Countermeasures



- Patch for intra-net is a headache, but you must do it.
- Backdoor accounts for management is hackers' good friends
- You need tailored and accurate threat intelligence

TEAMT5 杜浦數位安全

Key Takeaway:
Start the Threat Intelligence Cycle

1. China-nexus APT groups have launched massive attacks against the online entertainment business in APAC region.

2. Dissecting the current TTPs is merely the first step.

3. China-nexus APT are closely aligned with the national interests of the Chinese government.

Indicator of Compromise (IoC): Command and Control Server (C2)

AMOEBA

35.187.194.33
47.106.112.106
23.106.123.236
support.office365excel.org
update.office365excel.org
update.huobibtc.net
ssl.360antivirus.org
support.symanteprotection.com
103.255.179.54
www.omgod.org
yt-sslvpn.itcom888.live
158.247.220.169
vappvcsa.itcom888.live
156.240.104.149
45.77.174.106

GREEDY TAOTIE

103.79.78.48
52.163.225.199
40.122.105.12
VSVRS3DC02.bren-lnc.com
13.76.136.18
104.209.198.177
47.75.49.32
167.179.92.82
mail.bren-inc.info
bren-inc.email
89.35.178.105
103.79.78.48
107.148.131.210
35.187.148.253
ns162.nsakadns.com
104.168.211.246
45.77.250.141

TIANWU

cs.full-subscription.com
full-subscription.com
line.full-subscription.com
yd.full-subscription.com
zk.full-subscription.com
206.189.156.0
api.gpk-demo.com
api.geming8888.com
45.153.242.41
23.106.123.244
23.106.122.225
45.138.172.138
23.106.125.132
23.106.124.156
45.76.188.46
23.106.122.182
23.106.122.205
23.106.123.16
23.106.122.58

23.106.122.5
backup.microsupdate.com
line.full-subscription.com
time.daytimegamers.com
yd.full-subscription.com
login.good-enough-8fe4.com
www.orientbate.com
23.19.58.13
cdn2.twmicrosoft.com
139.180.156.45

SLIME34

27.102.106.132
27.102.106.183
27.102.114.246
27.102.115.249
27.102.127.182
27.50.162.19
42.51.22.68
54.180.89.244
api.kaspresksy.com
api.microsofts.info
microsofts.info
onedrive.miscrosofts.com
smsapi.tencentchat.net
update.kaspresksy.com

normostat.com
www.normostat.com
185.99.133.209
nenasporte.com
update.microsoftlab.top
www.microsofts.info
caibi379.com
weixin.dptoutiao.cn
162.33.178.57
172.105.162.84

SLIME29

BETWLN520.COM
www.kkxx888666.com
172.16.2.1
update.googletvi.com
112.175.238.60
103.24.205.128
mod.goodyouxi.com
xinmod.goodyouxi.com
167.179.92.82
mail.bren-inc.info
bren-inc.email
112.121.165.138
117.18.14.20

ogag.daji8.me
plus.daji8.me
shopingchina.net
www.shopingchina.net
linux.shopingchina.net
tools.daji8.me
linux.daji8.me
www.daji8.me
182.16.71.234
103.253.40.126
182.255.63.53
wmgnews.daji8.me
daji8.me
av.daji8.me

THANK YOU!

TEAMT5
杜浦數位安全

為您量身訂製　專屬勒索防護

立即前往 主題攤位 L04 量身

品牌專頁
QR Code

Website: teamt5.org　　　Twitter: @TeamT5_Official