Ransomware-as-a-Service: An Evolving Business Model

Wednesday, April 29 at 11 AM Eastern

CyberCube

Advisen
Transforming • Insurance℠

Ransomware-as-a-Service: An Evolving Business Model

Visit **www.advisenltd.com** at the end of this webinar to download:

- Copy of these slides
- Recording of today's webinar

Today’s webinar is sponsored by:

CyberCube

Mark your Calendars!

LIVE WEBINAR
May 5 @ 11 AM

Will Coronavirus Strike the D&O Market?

REGISTER NOW

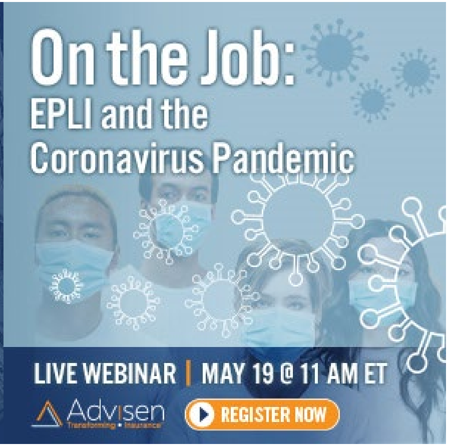
Advisen
Transforming • Insurance

Social Inflation
Truth or Fiction?

LIVE WEBINAR
May 12 @ 11 AM ET

REGISTER NOW

Advisen
Transforming • Insurance



On the Job:
EPLI and the Coronavirus Pandemic

LIVE WEBINAR | MAY 19 @ 11 AM ET

Advisen
Transforming • Insurance

REGISTER NOW

Register for all upcoming webinars at
www.advisenltd.com/media/webinars

Executive Summary
FREQUENCY
64
SEVERITY
82
25
Incident Type
Asset
Potential Impact
Low
Med
High
Data Privacy
Network Security
Business Income
Tech E&O

Today's Moderator

Chad Hemenway

Managing Editor

Advisen

Email at chemenway@advisen.com

Today's Panelists

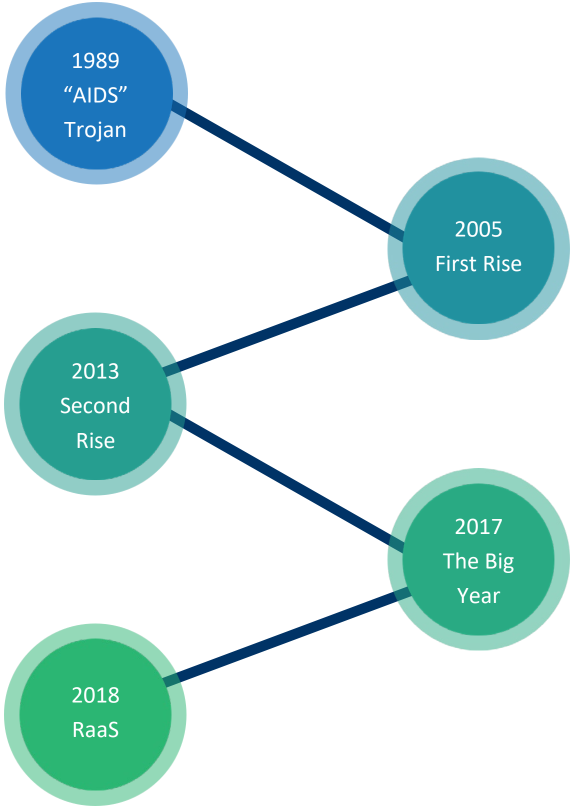
Oliver Brew
Head of Client Services
CyberCube Analytics

Lizzie Cookson
Associate Director, Cyber Investigations
Kivu Consulting, Inc.

Tony Kriesel
Senior Claims Underwriter
Hiscox London Market

Alejandro Sauter
Cyber Risk Analyst
CyberCube Analytics

What is ransomware-as-a-service?

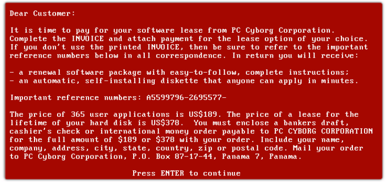

1989 "AIDS" Trojan

2005 First Rise

2013 Second Rise

2017 The Big Year

2018 RaaS


```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                        Press ENTER to continue
```

First known malware extortion attack

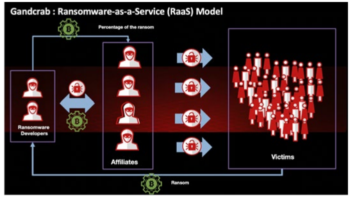
Liberty Reserve

PGPCoder & stronger encryption

BITCOIN
ACCEPTED HERE

CryptoLocker & Bitcoin

WannaCry, NotPetya, BadRabbit

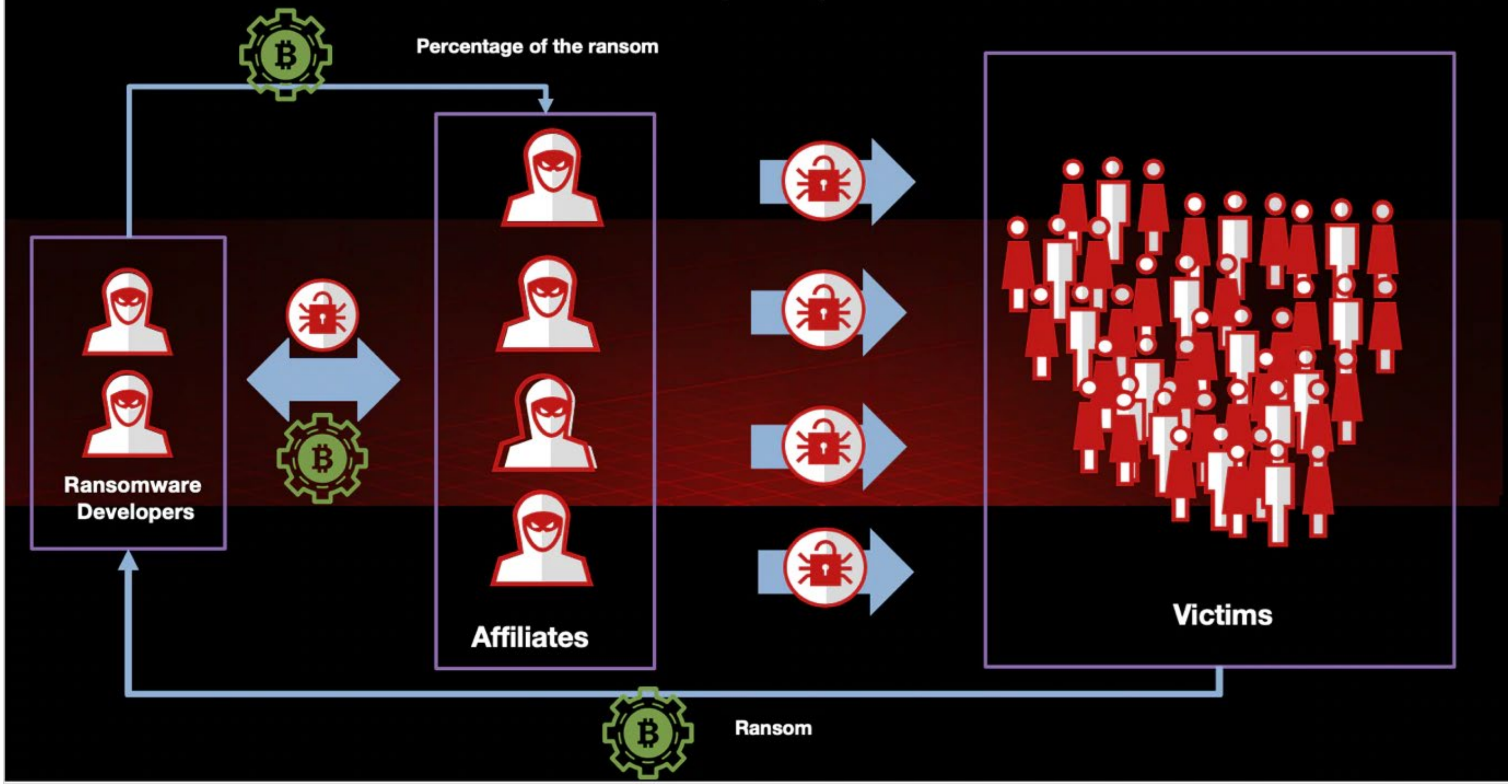


GandCrab RaaS

Affiliate marketing business model

Advisen
Transforming • Insurance℠

Gandcrab : Ransomware-as-a-Service (RaaS) Model



Advisen
Transforming • Insurance

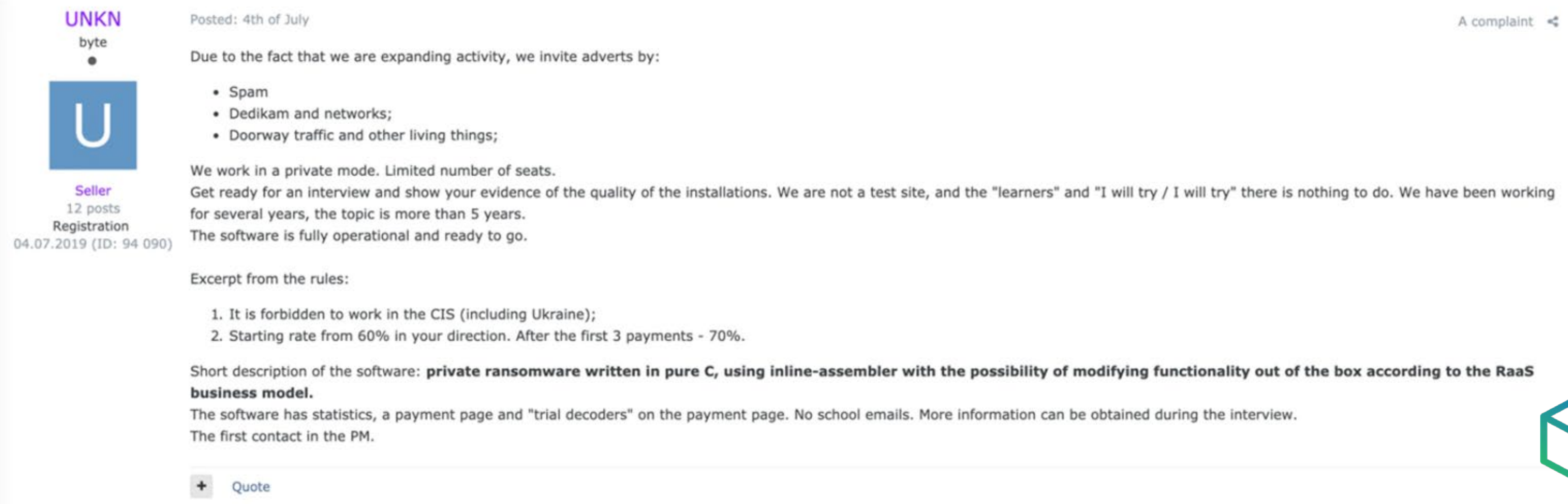
How does the business model work?

Developers:

- Buy source code + modify or build from scratch
- Advertise ransomware
- Recruit affiliates
- Set targets (i.e. amount of infections)
- Percentage (30-40%) per payment obtained
- Maintenance (updates, open spots, etc)
- Take less risk (not spreading malware themselves)
- Authors have safe haven sometimes (certain countries don’t criminalize malware development, only distribution)

Affiliates:

- Ransomware is made accessible
- Utilize skills and reputations to join “better” programs
- Allows for specialization (i.e. different methods to reach goals)
- Percentage (60-70%) per payment obtained
- Potential hand-offs involved
- Certain affiliates can rise to become top performers



UNKN

byte

Seller

12 posts

Registration

04.07.2019 (ID: 94 090)

Posted: 4th of July

A complaint

Due to the fact that we are expanding activity, we invite adverts by:

- Spam
- Dedikam and networks;
- Doorway traffic and other living things;

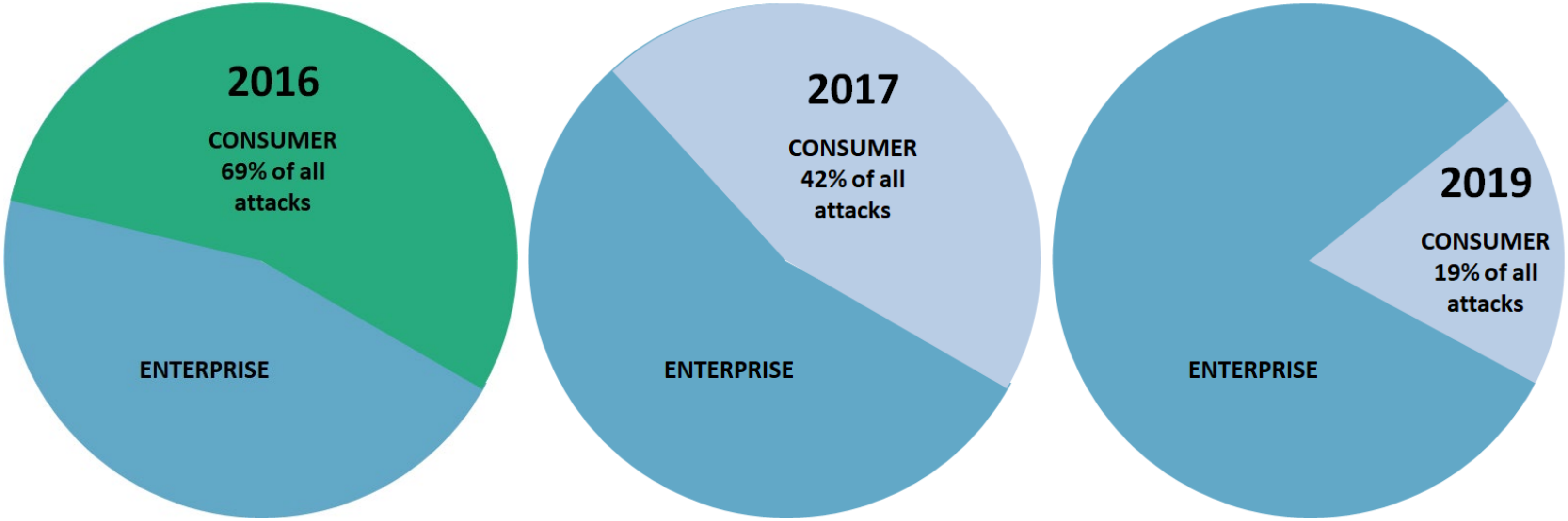
We work in a private mode. Limited number of seats.
Get ready for an interview and show your evidence of the quality of the installations. We are not a test site, and the "learners" and "I will try / I will try" there is nothing to do. We have been working for several years, the topic is more than 5 years.
The software is fully operational and ready to go.

Excerpt from the rules:

1. It is forbidden to work in the CIS (including Ukraine);
2. Starting rate from 60% in your direction. After the first 3 payments - 70%.

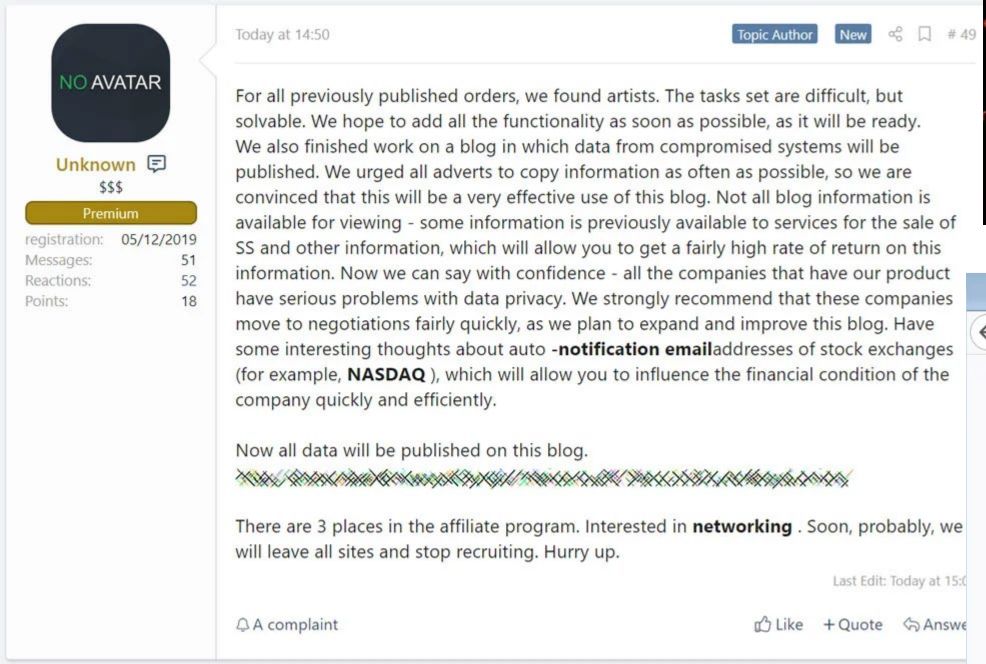
Short description of the software: **private ransomware written in pure C, using inline-assembler with the possibility of modifying functionality out of the box according to the RaaS business model.**
The software has statistics, a payment page and "trial decoders" on the payment page. No school emails. More information can be obtained during the interview.
The first contact in the PM.

How has the strategy of a ransomware attacker changed?



Advisen
Transforming • Insurance℠

- **Some RaaS operators adding data exfiltration capabilities**
- **Threat to sell, leak, and/or publicize stolen data**
- **Further pressure on victim to pay ransom**
  - Avoid disclosure of attack
  - Avoid leaking sensitive information



registration:	05/12/2019
Messages:	51
Reactions:	52
Points:	18

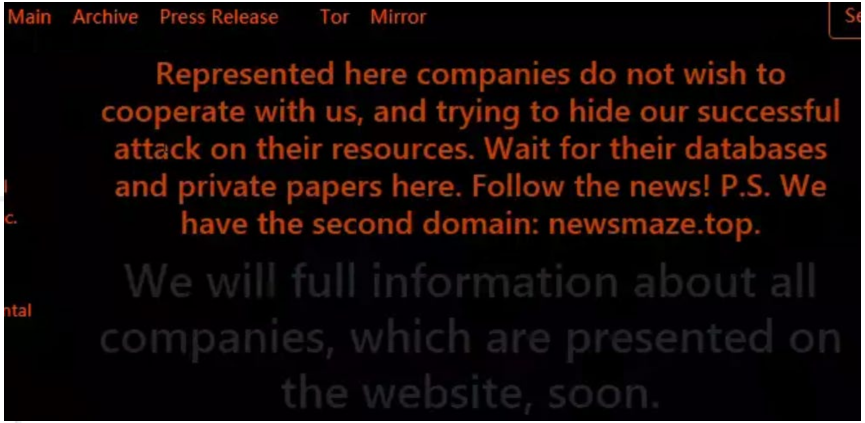
Today at 14:50

For all previously published orders, we found artists. The tasks set are difficult, but solvable. We hope to add all the functionality as soon as possible, as it will be ready. We also finished work on a blog in which data from compromised systems will be published. We urged all adverts to copy information as often as possible, so we are convinced that this will be a very effective use of this blog. Not all blog information is available for viewing - some information is previously available to services for the sale of SS and other information, which will allow you to get a fairly high rate of return on this information. Now we can say with confidence - all the companies that have our product have serious problems with data privacy. We strongly recommend that these companies move to negotiations fairly quickly, as we plan to expand and improve this blog. Have some interesting thoughts about auto -**notification email**addresses of stock exchanges (for example, **NASDAQ**), which will allow you to influence the financial condition of the company quickly and efficiently.

Now all data will be published on this blog.
[redacted]

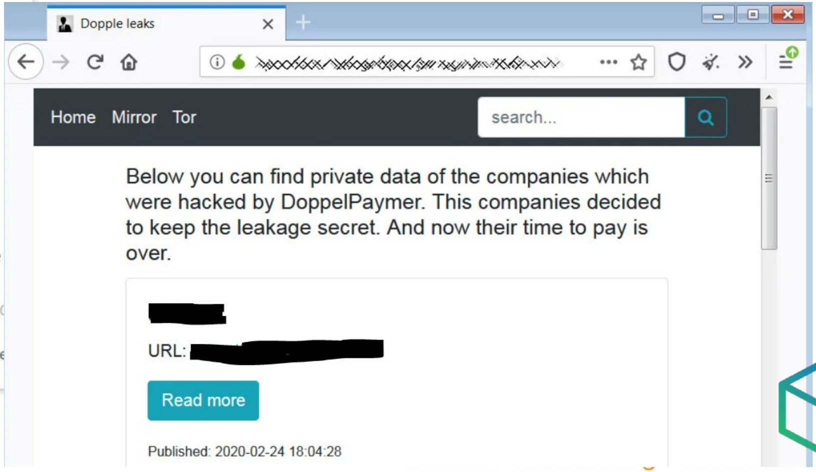
There are 3 places in the affiliate program. Interested in **networking** . Soon, probably, we will leave all sites and stop recruiting. Hurry up.

Last Edit: Today at 15:(



Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news! P.S. We have the second domain: newsmaze.top.

We will full information about all companies, which are presented on the website, soon.



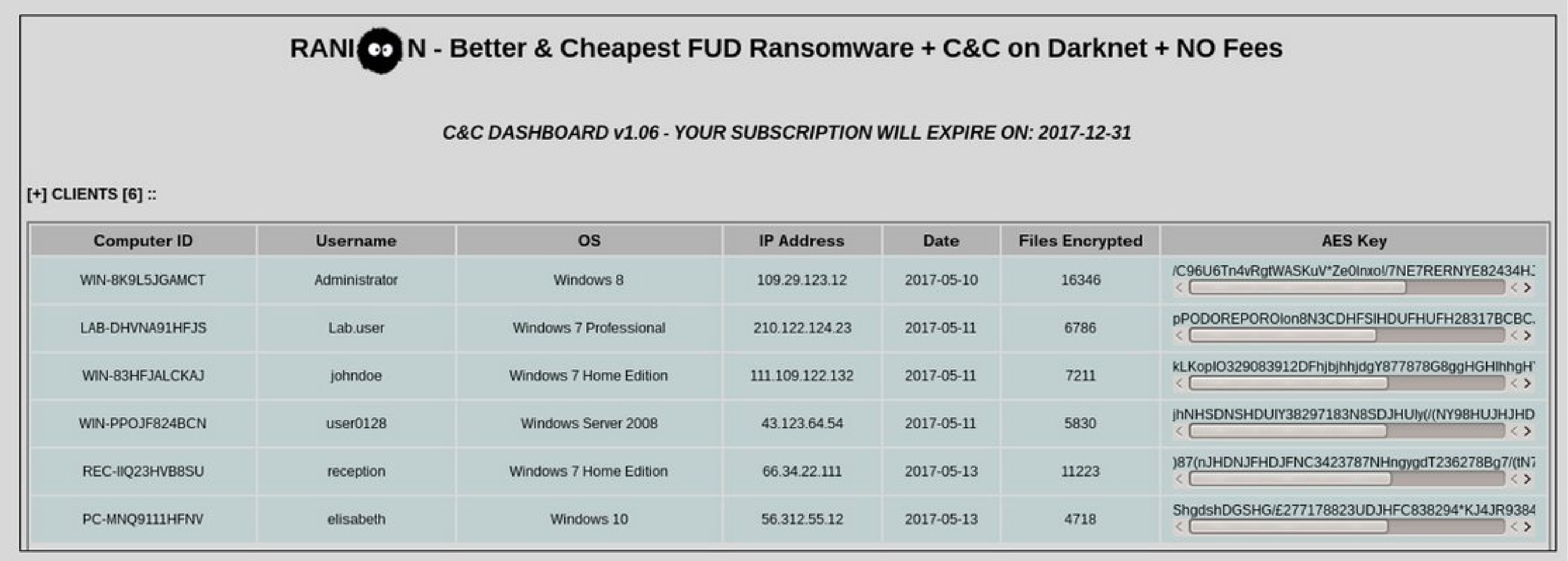
Below you can find private data of the companies which were hacked by DoppelPaymer. This companies decided to keep the leakage secret. And now their time to pay is over.

[redacted]

URL: [redacted]

Published: 2020-02-24 18:04:28

Do attackers range in sophistication?
Does this affect how a case is handled?



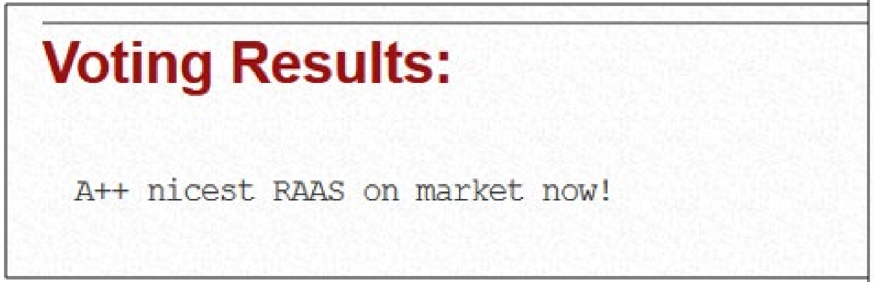
RANI●N - Better & Cheapest FUD Ransomware + C&C on Darknet + NO Fees

C&C DASHBOARD v1.06 - YOUR SUBSCRIPTION WILL EXPIRE ON: 2017-12-31

[+] CLIENTS [6] ::

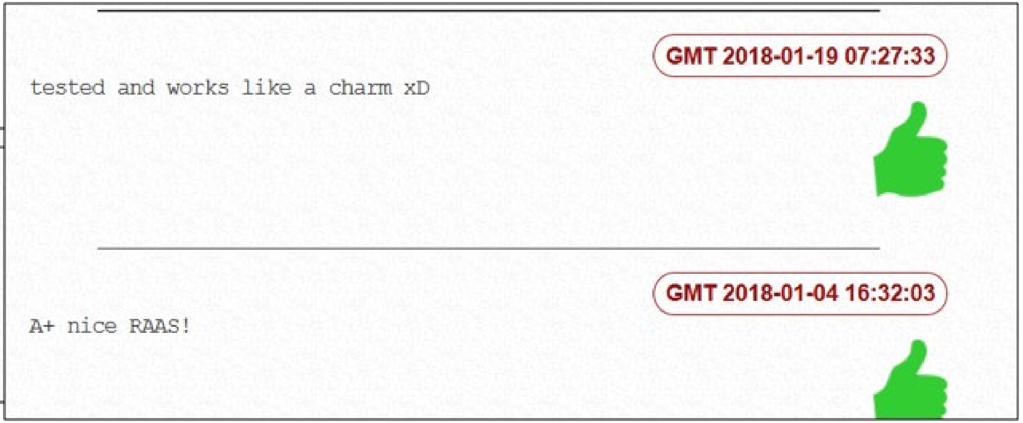
Computer ID	Username	OS	IP Address	Date	Files Encrypted	AES Key
WIN-8K9L5JGAMCT	Administrator	Windows 8	109.29.123.12	2017-05-10	16346	/C96U6Tn4vRgtWASKuV*Ze0lnxol/7NE7RERNYE82434H.
LAB-DHVNA91HFJS	Lab.user	Windows 7 Professional	210.122.124.23	2017-05-11	6786	pPODOREPOROlon8N3CDHFSIHDUFHUFH28317BCBC.
WIN-83HFJALCKAJ	johndoe	Windows 7 Home Edition	111.109.122.132	2017-05-11	7211	kLKoplO329083912DFhjbjhhjdgY877878G8ggHGHlhhgH'
WIN-PPOJF824BCN	user0128	Windows Server 2008	43.123.64.54	2017-05-11	5830	jhNHSDNSHDUIY38297183N8SDJHUly(/(NY98HUJHJHD
REC-IIQ23HVB8SU	reception	Windows 7 Home Edition	66.34.22.111	2017-05-13	11223	)87(nJHDNJFHDJFNC3423787NHngygdT236278Bg7/(tN7
PC-MNQ9111HFNV	elisabeth	Windows 10	56.312.55.12	2017-05-13	4718	ShgdshDGSHG/£277178823UDJHFC838294*KJ4JR9384

- RaaS platforms vary in terms of what they offer
- Some offer a range of packages from “basic” to “platinum”
- Pricier subscriptions ensure access to additional features, like customer support, a malware downloader, and longer access to the server



Voting Results:

A++ nicest RAAS on market now!



GMT 2018-01-19 07:27:33

tested and works like a charm xD

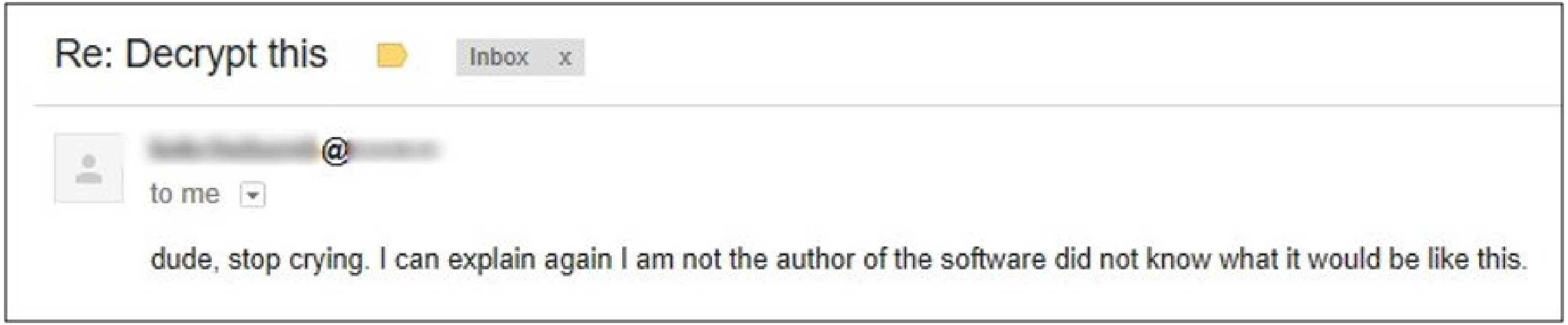
👍

GMT 2018-01-04 16:32:03

A+ nice RAAS!

👍

- The result: a new wave of **amateur** ransomware attackers
- Little to **no technical knowledge**
- Infection vectors are messy and cause **damage** to data
- When keys fail or the tool doesn't work, they cannot or will not **troubleshoot**



Re: Decrypt this

[redacted]@[redacted]

to me

dude, stop crying. I can explain again I am not the author of the software did not know what it would be like this.

- The bad or poorly operated RaaS:
  - Platform does not screen their subscribers
  - Subscribers may have **little to no technical knowledge**
  - Subscribers tend to be hostile, **disorganized**
  - Malware samples are **not updated or improved** overtime
  - Developer provides **little to no customer support**
- The good or closely monitored RaaS:
  - Developers tightly control their pool of subscribers
  - Subscribers are **rigorously vetted** and must have prior hacking/ransom experience
  - Malware samples and decryption tools are **updated every few days** or weeks
  - Developers provide **robust customer support**

Where does the call from a client come first? Where should it go?

Company's incident response plan should include consideration of:

- Cyber insurance and first notice of loss
- Ransomware response

Ransomware service provider / IT forensics firm should be pre-agreed with insurer

- Eliminate need for insurer consent at time of incident?
- Permits first notice of incident to service provider rather than insurer?

What costs are covered? How are claims handled?

Company must have understanding of its own cyber policy's terms and conditions

- Extortion payment
- Service provider fees
- Business interruption costs
- Data recovery costs
- Legal costs
- Crisis management and public relations costs
- Notice and consent

Claims are best handled with preparation and forethought before an incident and then collaboration at the time of the incident

- If possible, discuss claims handling at time of policy binding
- Internal preparation by company's incident response team and possibly board
- Transparent flow of information and communication during (not after) incident

Ransomware-as-a-Service: An Evolving Business Model

Chad Hemenway
Advisen

Oliver Brew
CyberCube Analytics

Lizzie Cookson
Kivu Consulting, Inc.

Tony Kriesel
Hiscox London Market

Alejandro Sauter
CyberCube Analytics

Advisen
Transforming • Insurance℠

Thank you to our panelists!

Oliver Brew
Head of Client Services
CyberCube Analytics

Lizzie Cookson
Associate Director, Cyber Investigations
Kivu Consulting, Inc.

Tony Kriesel
Senior Claims Underwriter
Hiscox London Market

Alejandro Sauter
Cyber Risk Analyst
CyberCube Analytics

Ransomware-as-a-Service: An Evolving Business Model

Visit **www.advisenltd.com** at the end of this webinar to download:

- Copy of these slides
- Recording of today's webinar

For more on Advisen, visit www.advisenltd.com or email us advisenevents@advisen.com

On the Job:
EPLI and the Coronavirus Pandemic
LIVE WEBINAR | MAY 19 @ 11 AM ET
Advisen
REGISTER NOW

Leading the way to **smarter**
and more **efficient**
risk and insurance **communities**.

Advisen delivers:
the ***right information*** into
the ***right hands*** at
the ***right time***
to ***power performance***.