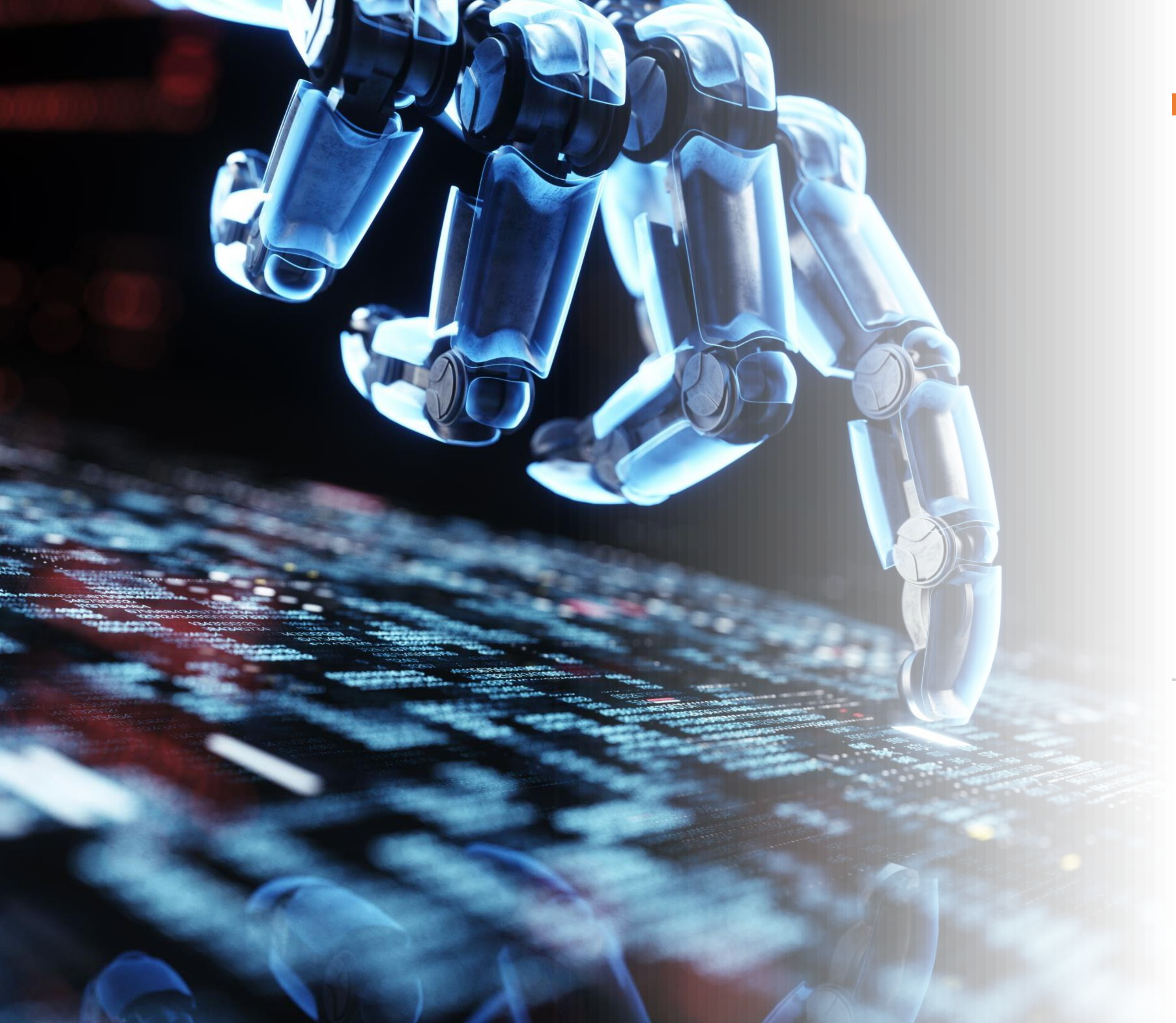
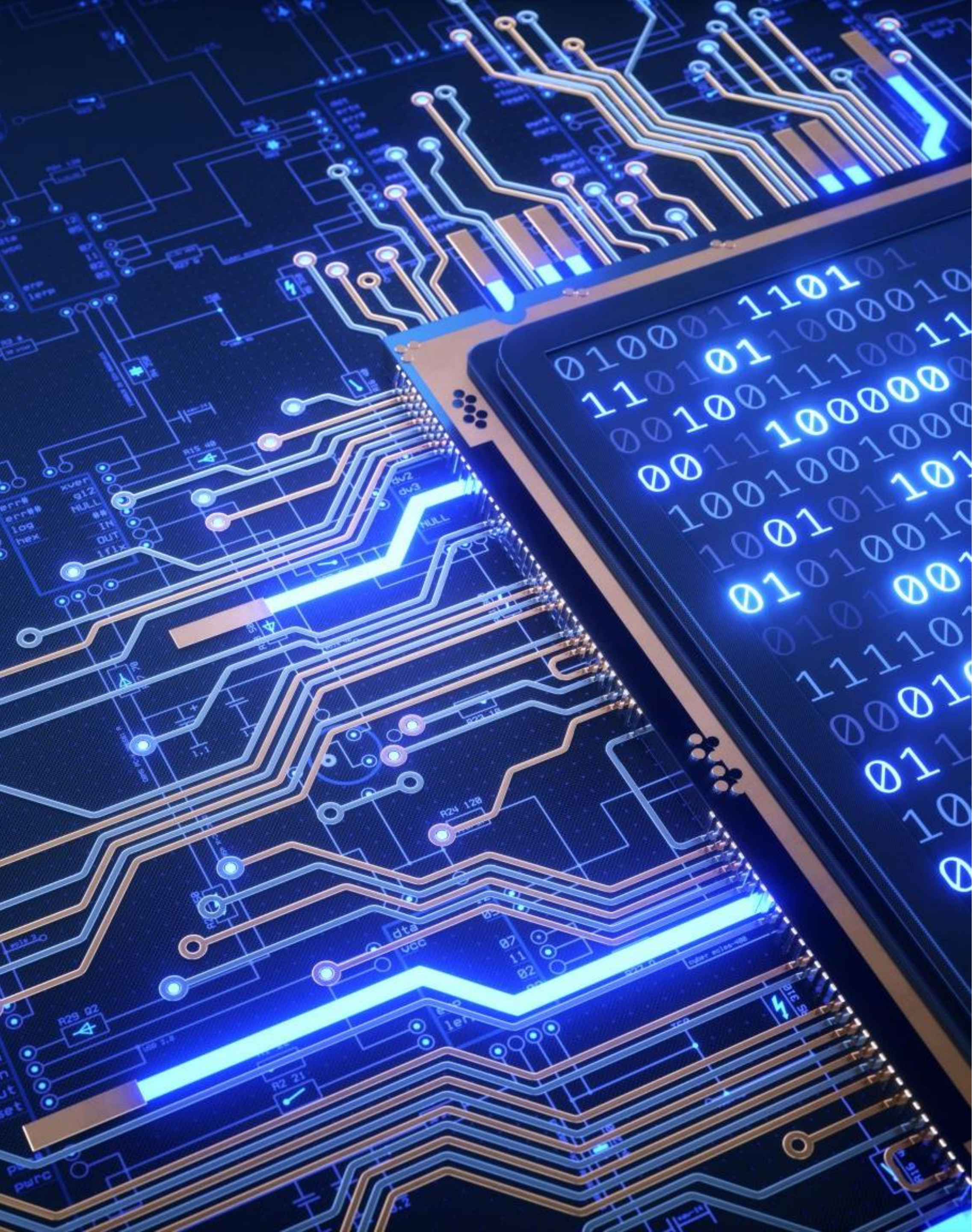


Practical Cybercrime Intelligence

CyberThreat23



About Me

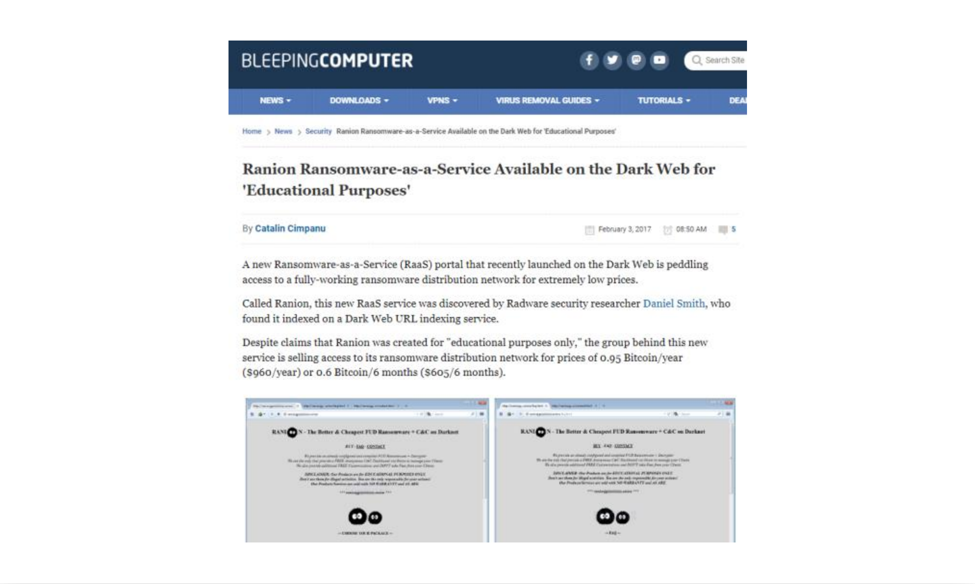
- Will Thomas
- Co-author of SANS FOR589: Cybercrime Intelligence
- Co-founder of Curated Intelligence
- CTI Researcher at Equinix
- Aka @BushidoToken online

Practical Lessons from a Cybercrime Investigation

- Navigating the darknet
- Identifying Infrastructure
- Mapping Capabilities
- Researching the Adversary
- Revealing its Victims
- Malware Analysis
- Blockchain Analysis
- Campaign Profiling

OSINT on Ranion

- Appeared around February 2017
- Ransomware-as-a-Service
- Self-Service Kit and Pay-as-you-go
- Spreads via phishing emails with ZIP attachments containing the EXE
- Ransomware code is based on HiddenTear (an open-source ransomware with code on GitHub)
- Code is Packed (obfuscated) with ConfuserEx


BLEEPINGCOMPUTER
Search Site
NEWS
DOWNLOADS
VPNS
VIRUS REMOVAL GUIDES
TUTORIALS
Home > News > Security Ranion Ransomware-as-a-Service Available on the Dark Web for 'Educational Purposes'
RANION - The Better & Cheapest FUD Ransomware + C&C on Darknet
RANION - The Better & Cheapest FUD Ransomware + C&C on Darknet

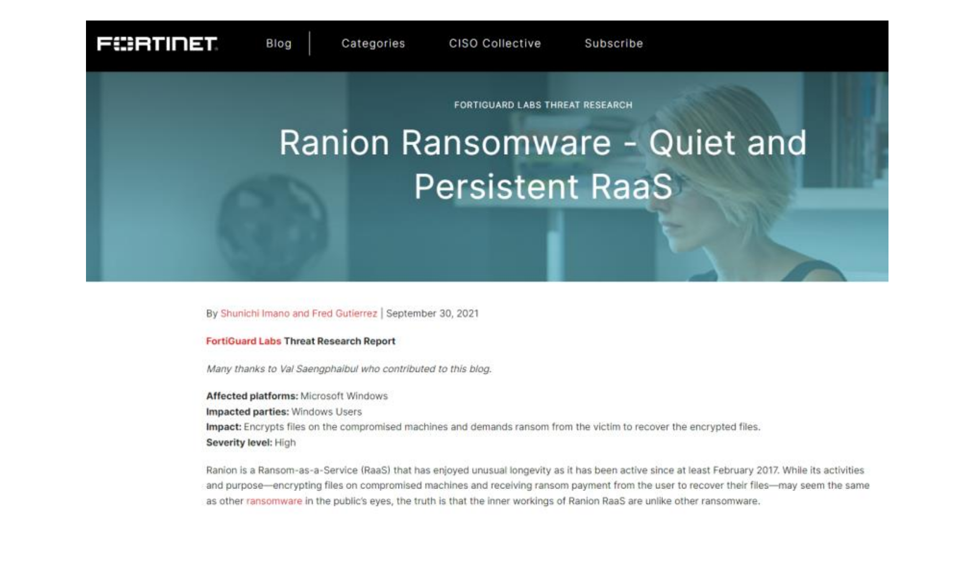
Ranion Ransomware-as-a-Service Available on the Dark Web for 'Educational Purposes'

By Catalin Cimpanu   February 3, 2017   08:50 AM   5

A new Ransomware-as-a-Service (RaaS) portal that recently launched on the Dark Web is peddling access to a fully-working ransomware distribution network for extremely low prices.

Called Ranion, this new RaaS service was discovered by Radware security researcher Daniel Smith, who found it indexed on a Dark Web URL indexing service.

Despite claims that Ranion was created for "educational purposes only," the group behind this new service is selling access to its ransomware distribution network for prices of 0.95 Bitcoin/year ($960/year) or 0.6 Bitcoin/6 months ($605/6 months).



Ranion Ransomware - Quiet and Persistent RaaS

By Shunichi Imano and Fred Gutierrez | September 30, 2021

FortiGuard Labs Threat Research Report

Many thanks to Val Saengphaibul who contributed to this blog.

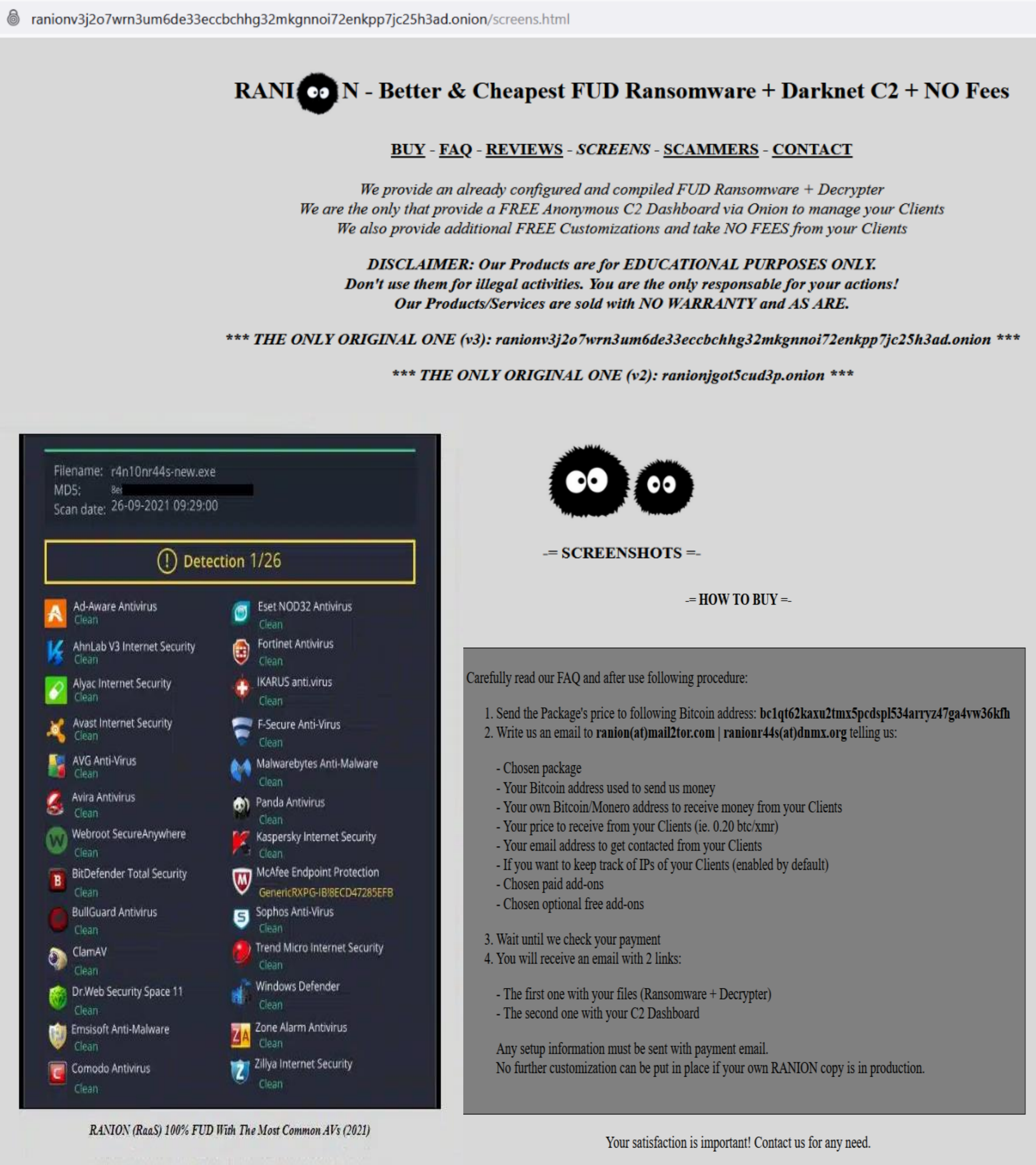
Affected platforms: Microsoft Windows
Impacted parties: Windows Users
Impact: Encrypts files on the compromised machines and demands ransom from the victim to recover the encrypted files.
Severity level: High

Ranion is a Ransom-as-a-Service (RaaS) that has enjoyed unusual longevity as it has been active since at least February 2017. While its activities and purpose—encrypting files on compromised machines and receiving ransom payment from the user to recover their files—may seem the same as other ransomware in the public's eyes, the truth is that the inner workings of Ranion RaaS are unlike other ransomware.

Infrastructure

Ranion’s Tor Site

- **Original Tor Site:**
  - ranionjgot5cud3p[.]onion
- **New Tor v3 Site:**
  - ranionv3j2o7wrn3um6de33eccbchhg32mkgnnoi72enkpp7jc25h3ad[.]onion
- **Bitcoin Address:**
  - bc1qt62kaxu2tmx5pcdspl534arryz47ga4vw36kfh
- **Emails:**
  - ranion(at)mail2tor.com
  - ranionr44s(at)dnmx.org
- **Filename:**
  - r4n1onr44s-new.exe



ranionv3j2o7wrn3um6de33eccbchhg32mkgnnoi72enkpp7jc25h3ad.onion/screens.html

RANI N - Better & Cheapest FUD Ransomware + Darknet C2 + NO Fees

We provide an already configured and compiled FUD Ransomware + Decrypter
We are the only that provide a FREE Anonymous C2 Dashboard via Onion to manage your Clients
We also provide additional FREE Customizations and take NO FEES from your Clients

DISCLAIMER: Our Products are for EDUCATIONAL PURPOSES ONLY.
Don't use them for illegal activities. You are the only responsable for your actions!
Our Products/Services are sold with NO WARRANTY and AS ARE.

****** THE ONLY ORIGINAL ONE (v3): ranionv3j2o7wrn3um6de33eccbchhg32mkgnnoi72enkpp7jc25h3ad.onion ******

****** THE ONLY ORIGINAL ONE (v2): ranionjgot5cud3p.onion ******

Filename: r4n10nr44s-new.exe
MD5: [redacted]
Scan date: 26-09-2021 09:29:00

Detection 1/26

Ad-Aware Antivirus	Clean	Eset NOD32 Antivirus	Clean
AhnLab V3 Internet Security	Clean	Fortinet Antivirus	Clean
Alyac Internet Security	Clean	IKARUS anti.virus	Clean
Avast Internet Security	Clean	F-Secure Anti-Virus	Clean
AVG Anti-Virus	Clean	Malwarebytes Anti-Malware	Clean
Avira Antivirus	Clean	Panda Antivirus	Clean
Webroot SecureAnywhere	Clean	Kaspersky Internet Security	Clean
BitDefender Total Security	Clean	McAfee Endpoint Protection	GenericRXPG-IB!8ECD47285EFB
BullGuard Antivirus	Clean	Sophos Anti-Virus	Clean
ClamAV	Clean	Trend Micro Internet Security	Clean
Dr.Web Security Space 11	Clean	Windows Defender	Clean
Emsisoft Anti-Malware	Clean	Zone Alarm Antivirus	Clean
Comodo Antivirus	Clean	Zillya Internet Security	Clean

RANION (RaaS) 100% FUD With The Most Common AVs (2021)

-= SCREENSHOTS =-

-= HOW TO BUY =-

Carefully read our FAQ and after use following procedure:

1. Send the Package's price to following Bitcoin address: **bc1qt62kaxu2tmx5pcdspl534arryz47ga4vw36kfh**
2. Write us an email to **ranion(at)mail2tor.com | ranionr44s(at)dnmx.org** telling us:

   - Chosen package
   - Your Bitcoin address used to send us money
   - Your own Bitcoin/Monero address to receive money from your Clients
   - Your price to receive from your Clients (ie. 0.20 btc/xmr)
   - Your email address to get contacted from your Clients
   - If you want to keep track of IPs of your Clients (enabled by default)
   - Chosen paid add-ons
   - Chosen optional free add-ons

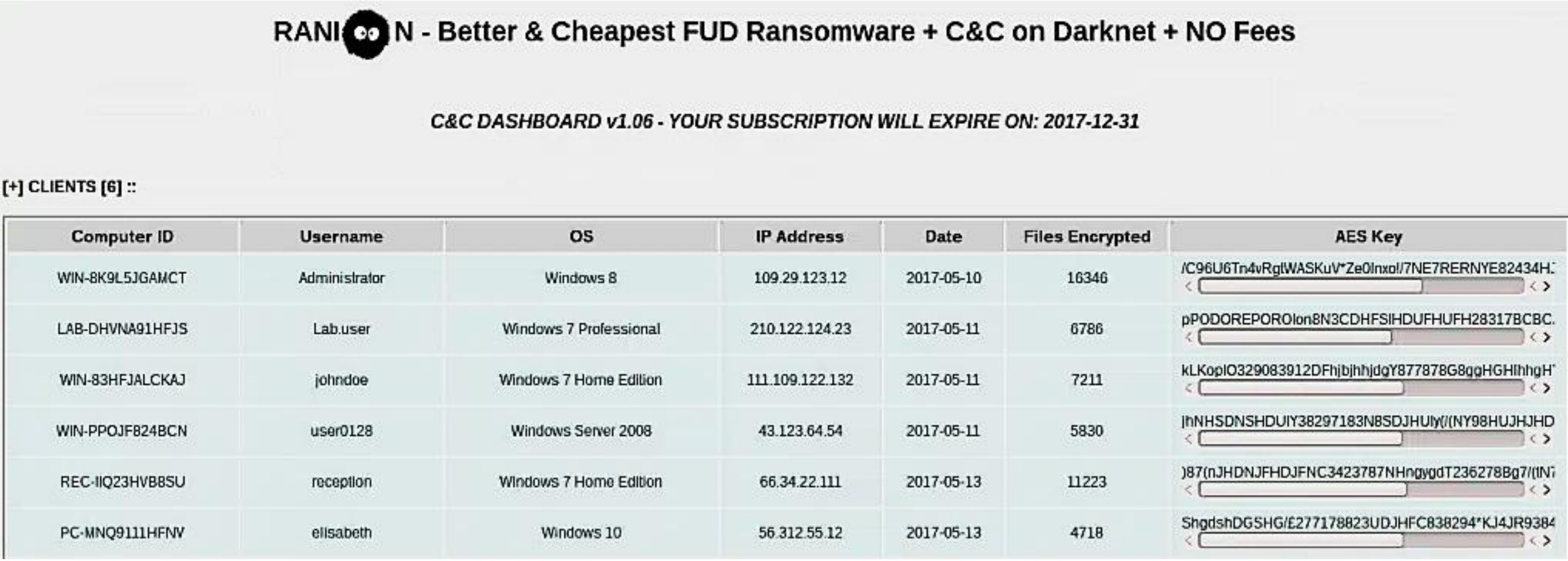
3. Wait until we check your payment
4. You will receive an email with 2 links:

   - The first one with your files (Ransomware + Decrypter)
   - The second one with your C2 Dashboard

   Any setup information must be sent with payment email.
   No further customization can be put in place if your own RANION copy is in production.

Your satisfaction is important! Contact us for any need.

Ranion Ransomware-as-a-Service



RANION - Better & Cheapest FUD Ransomware + C&C on Darknet + NO Fees

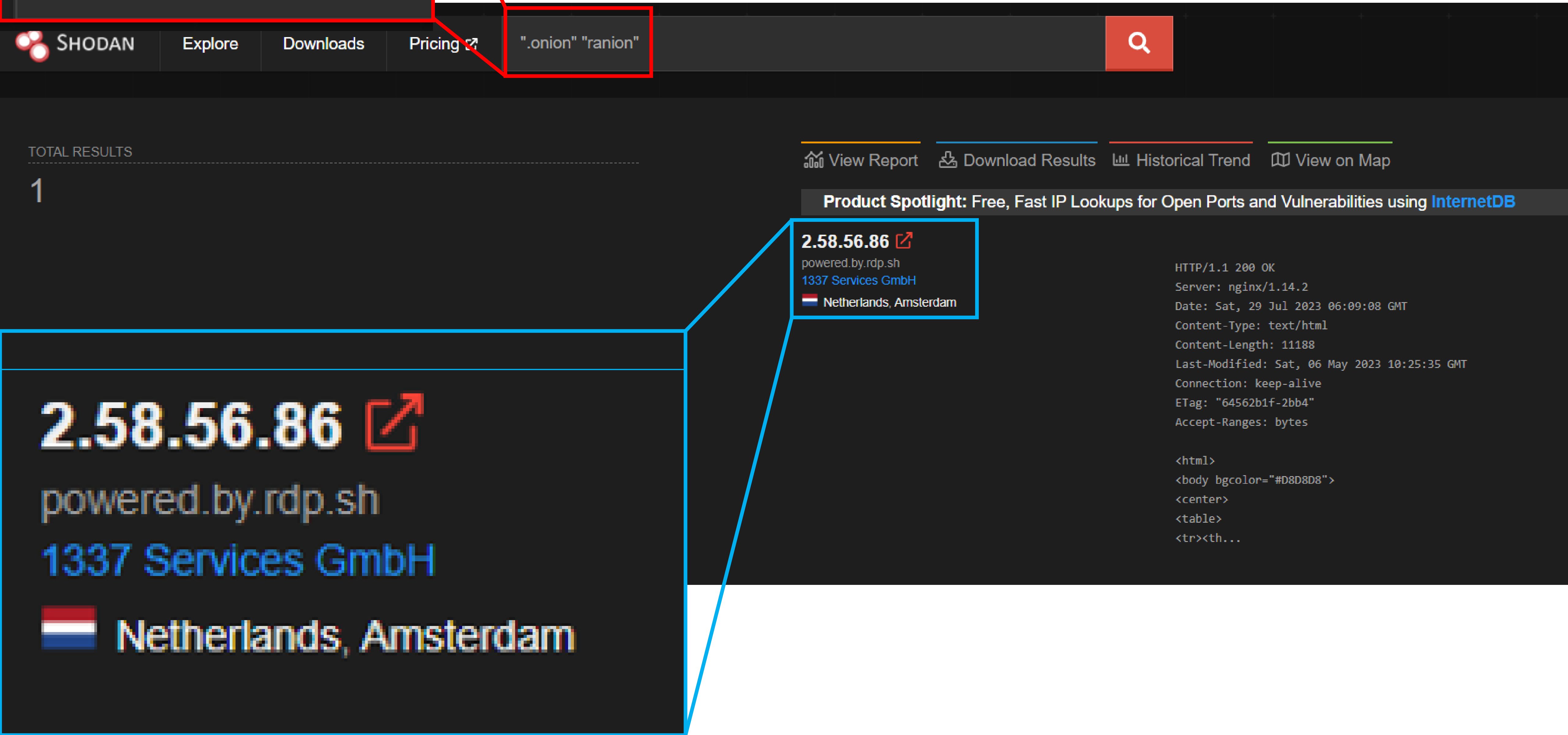
C&C DASHBOARD v1.06 - YOUR SUBSCRIPTION WILL EXPIRE ON: 2017-12-31

[+] 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	/C96U6Tn4vRglWASKuV*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/(tN
PC-MNQ9111HFNV	elisabeth	Windows 10	56.312.55.12	2017-05-13	4718	ShgdshDGSHG/£277178823UDJHFC838294*KJ4JR9384

A New Tor Site found via Shodan

".onion" "ranion"



TOTAL RESULTS

1

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

2.58.56.86

powered.by.rdp.sh

1337 Services GmbH

Netherlands, Amsterdam

```
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Sat, 29 Jul 2023 06:09:08 GMT
Content-Type: text/html
Content-Length: 11188
Last-Modified: Sat, 06 May 2023 10:25:35 GMT
Connection: keep-alive
ETag: "64562b1f-2bb4"
Accept-Ranges: bytes

<html>
<body bgcolor="#D8D8D8">
<center>
<table>
<tr><th...
```

2.58.56.86

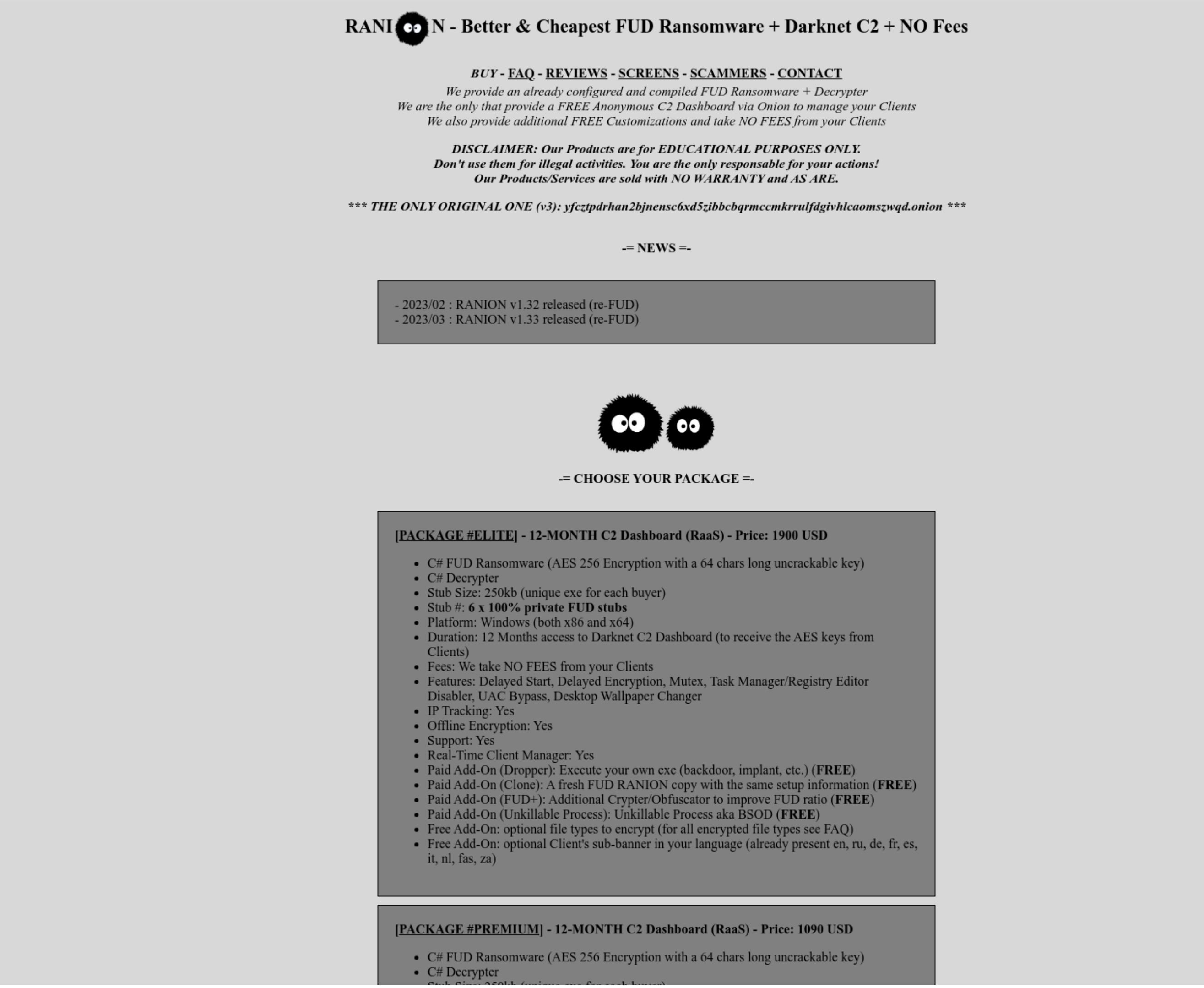
powered.by.rdp.sh

1337 Services GmbH

Netherlands, Amsterdam

Scammer's Tor Site

yfcztpdrhan2bjnensc6xd5zibbcbqrmccmkrrulfdgivhlcaomszwqd.onion



RANI🌑N - Better & Cheapest FUD Ransomware + Darknet C2 + NO Fees

BUY **-** **FAQ** **-** **REVIEWS** **-** **SCREENS** **-** **SCAMMERS** **-** **CONTACT**

We provide an already configured and compiled FUD Ransomware + Decrypter
We are the only that provide a FREE Anonymous C2 Dashboard via Onion to manage your Clients
We also provide additional FREE Customizations and take NO FEES from your Clients

DISCLAIMER: Our Products are for EDUCATIONAL PURPOSES ONLY.
Don't use them for illegal activities. You are the only responsable for your actions!
Our Products/Services are sold with NO WARRANTY and AS ARE.

****** THE ONLY ORIGINAL ONE (v3): yfcztpdrhan2bjnensc6xd5zibbcbqrmccmkrrulfdgivhlcaomszwqd.onion ******

-= NEWS =-

- 2023/02 : RANION v1.32 released (re-FUD)
- 2023/03 : RANION v1.33 released (re-FUD)

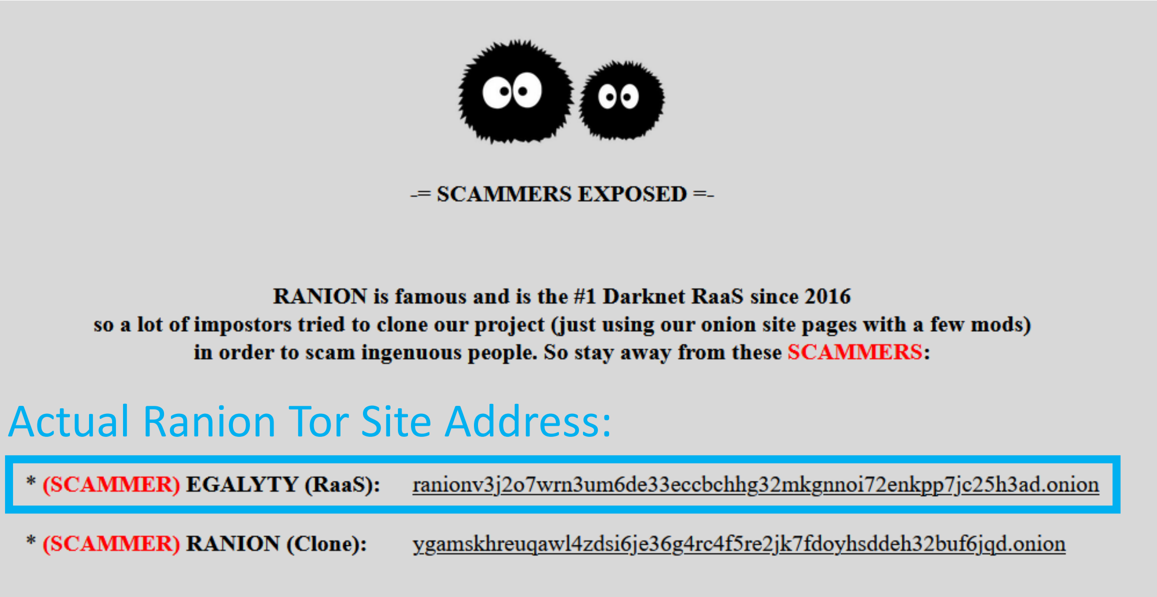
-= CHOOSE YOUR PACKAGE =-

[PACKAGE #ELITE] - 12-MONTH C2 Dashboard (RaaS) - Price: 1900 USD

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- Stub #: **6 x 100% private FUD stubs**
- Platform: Windows (both x86 and x64)
- Duration: 12 Months access to Darknet C2 Dashboard (to receive the AES keys from Clients)
- Fees: We take NO FEES from your Clients
- Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer
- IP Tracking: Yes
- Offline Encryption: Yes
- Support: Yes
- Real-Time Client Manager: Yes
- Paid Add-On (Dropper): Execute your own exe (backdoor, implant, etc.) (**FREE**)
- Paid Add-On (Clone): A fresh FUD RANION copy with the same setup information (**FREE**)
- Paid Add-On (FUD+): Additional Crypter/Obfuscator to improve FUD ratio (**FREE**)
- Paid Add-On (Unkillable Process): Unkillable Process aka BSOD (**FREE**)
- Free Add-On: optional file types to encrypt (for all encrypted file types see FAQ)
- Free Add-On: optional Client's sub-banner in your language (already present en, ru, de, fr, es, it, nl, fas, za)

[PACKAGE #PREMIUM] - 12-MONTH C2 Dashboard (RaaS) - Price: 1090 USD

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter



-= SCAMMERS EXPOSED =-

RANION is famous and is the #1 Darknet RaaS since 2016
so a lot of impostors tried to clone our project (just using our onion site pages with a few mods)
in order to scam ingenuous people. So stay away from these SCAMMERS:

Actual Ranion Tor Site Address:

* **(SCAMMER) EGALYTY (RaaS):** ranionv3j2o7wrn3um6de33eccbchhg32mkgnnoi72enkpp7jc25h3ad.onion

* **(SCAMMER) RANION (Clone):** ygamskhreuqawl4zdsi6je36g4rc4f5re2jk7fdoyhsddeh32buf6jqd.onion

Bitcoin Address:

- bc1qezstceqtjg9qsu7uprapcevxlhrs9rttc2h0lm

Email:

- Incognit0@dnmx.org

Capabilities

MITRE ATT&CK TTPs

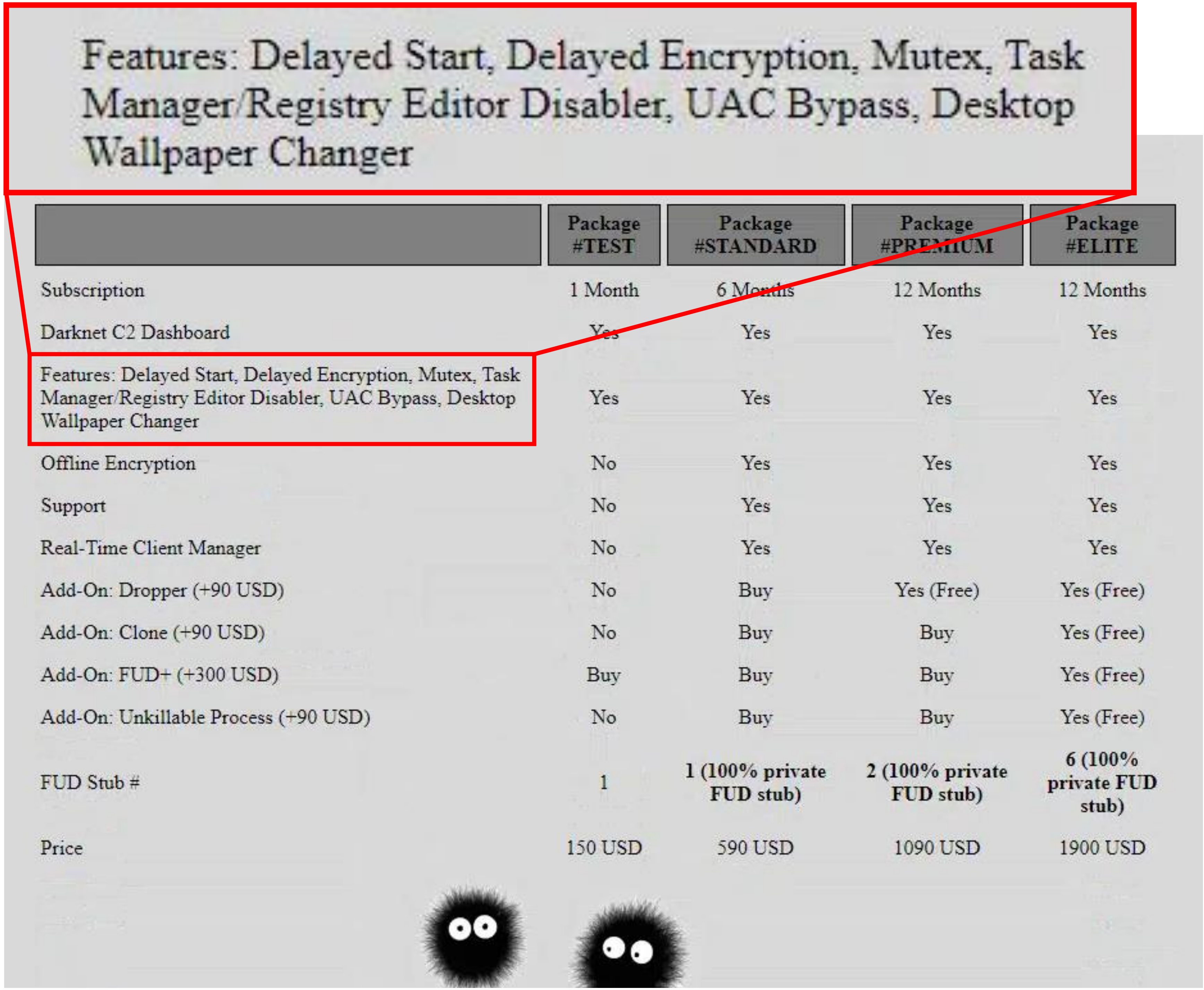
1. “Delayed Start”
   T1497.003 - Time Based Evasion

2. “Delayed Encryption”
   T1486 - Data Encrypted for Impact

3. “Task Manager/Registry Editor Disabled”
   T1112 - Modify Registry

4. “UAC Bypass”
   T1548.002 - Bypass User Account Control (UAC)

5. “Desktop Wallpaper Changer”
   T1491.001 - Internal Defacement



Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer

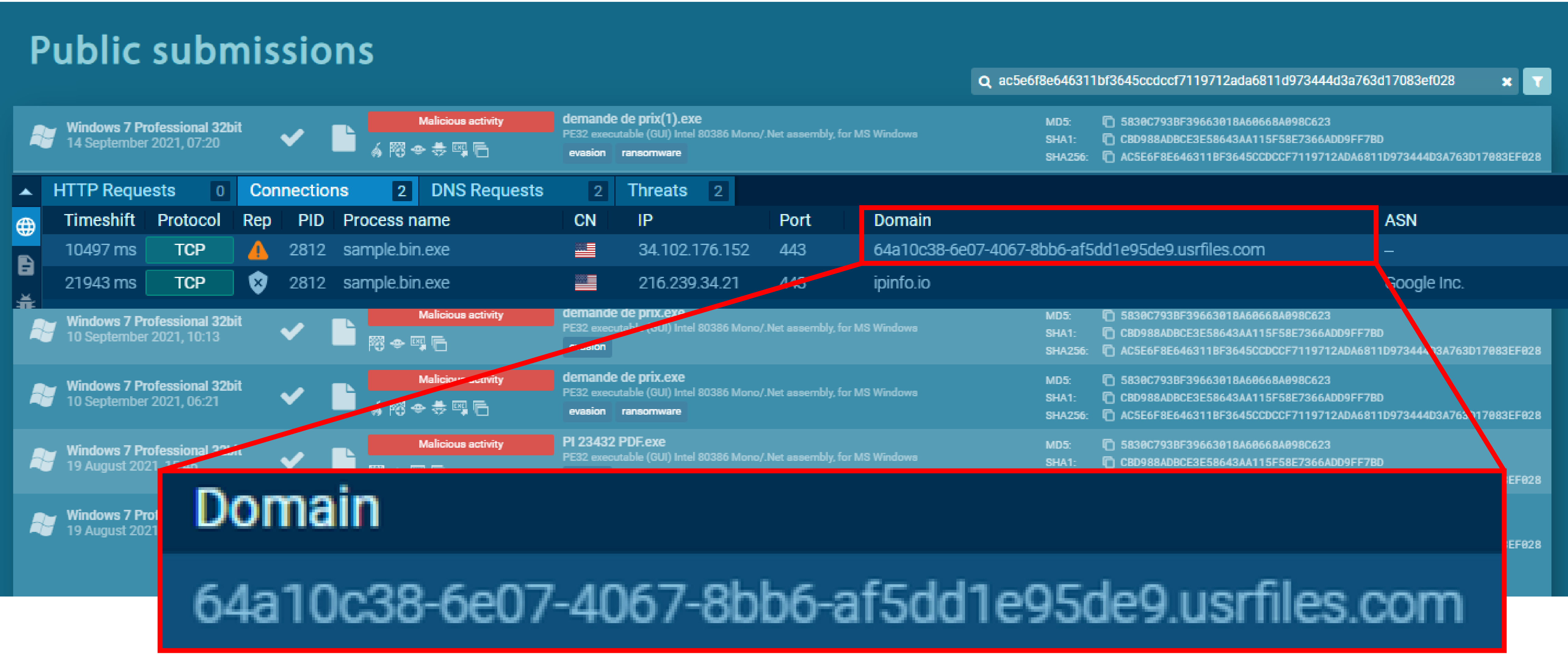
	Package #TEST	Package #STANDARD	Package #PREMIUM	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C2 Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Add-On: Dropper (+90 USD)	No	Buy	Yes (Free)	Yes (Free)
Add-On: Clone (+90 USD)	No	Buy	Buy	Yes (Free)
Add-On: FUD+ (+300 USD)	Buy	Buy	Buy	Yes (Free)
Add-On: Unkillable Process (+90 USD)	No	Buy	Buy	Yes (Free)
FUD Stub #	1	1 (100% private FUD stub)	2 (100% private FUD stub)	6 (100% private FUD stub)
Price	150 USD	590 USD	1090 USD	1900 USD

Ranion Binaries VirusTotal

Creation Time	MD5 File Hash	Size
2017-04-25 15:54:19 UTC	1ff22451d7c700ae6bdc765e06f21619	231.50 KB (237056 bytes)
2018-01-26 15:19:26 UTC	eca948ea4dec7a9237605658e516baa6	274.50 KB (281088 bytes)
2018-07-28 19:40:09 UTC	4a9891a32895ac456bfdf7e05eb176c1	275.50 KB (282112 bytes)
2018-11-15 08:55:38 UTC	61e69b6ecf176fc74179fffab0fc4292	276.50 KB (283136 bytes)
2021-08-16 08:08:05 UTC	5830c793bf39663018a60668a098c623	260.50 KB (266752 bytes)

Similarities	Value
Common File Name	custom-2017.exe
Other Style File Name	“r44s_YYYY-MM-DD NNNN.exe”
Import Hash (Imphash)	f34d5f2d4577ed6d9ceec516c1f5a744
VirusTotal Magic Check	PE32 exe for MS Windows, Intel 80386 32-bit Mono/.Net assembly
File Version Info	Adobe Acrobat Reader (Copyright 2015 Adobe Systems Incorporated.)

Pivoting to Sandbox Detonations



Public submissions

ac5e6f8e646311bf3645ccdccf7119712ada6811d973444d3a763d17083ef028

Windows 7 Professional 32bit
14 September 2021, 07:20
Malicious activity
demande de prix(1).exe
PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
evasion ransomware
MD5: 5830C793BF39663018A60668A098C623
SHA1: CBD988ADBCE3E58643AA115F58E7366ADD9FF7BD
SHA256: AC5E6F8E646311BF3645CCDCCF7119712ADA6811D973444D3A763D17083EF028

HTTP Requests 0 | Connections 2 | DNS Requests 2 | Threats 2

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN
10497 ms	TCP	⚠	2812	sample.bin.exe	🇺🇸	34.102.176.152	443	64a10c38-6e07-4067-8bb6-af5dd1e95de9.usrfiles.com	–
21943 ms	TCP	🛡	2812	sample.bin.exe	🇺🇸	216.239.34.21	443	ipinfo.io	Google Inc.

Windows 7 Professional 32bit
10 September 2021, 10:13
Malicious activity
demande de prix.exe
PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
evasion
MD5: 5830C793BF39663018A60668A098C623
SHA1: CBD988ADBCE3E58643AA115F58E7366ADD9FF7BD
SHA256: AC5E6F8E646311BF3645CCDCCF7119712ADA6811D973444D3A763D17083EF028

Windows 7 Professional 32bit
10 September 2021, 06:21
Malicious activity
demande de prix.exe
PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
evasion ransomware
MD5: 5830C793BF39663018A60668A098C623
SHA1: CBD988ADBCE3E58643AA115F58E7366ADD9FF7BD
SHA256: AC5E6F8E646311BF3645CCDCCF7119712ADA6811D973444D3A763D17083EF028

Windows 7 Professional 32bit
19 August 2021
Malicious activity
PI 23432 PDF.exe
PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5: 5830C793BF39663018A60668A098C623
SHA1: CBD988ADBCE3E58643AA115F58E7366ADD9FF7BD

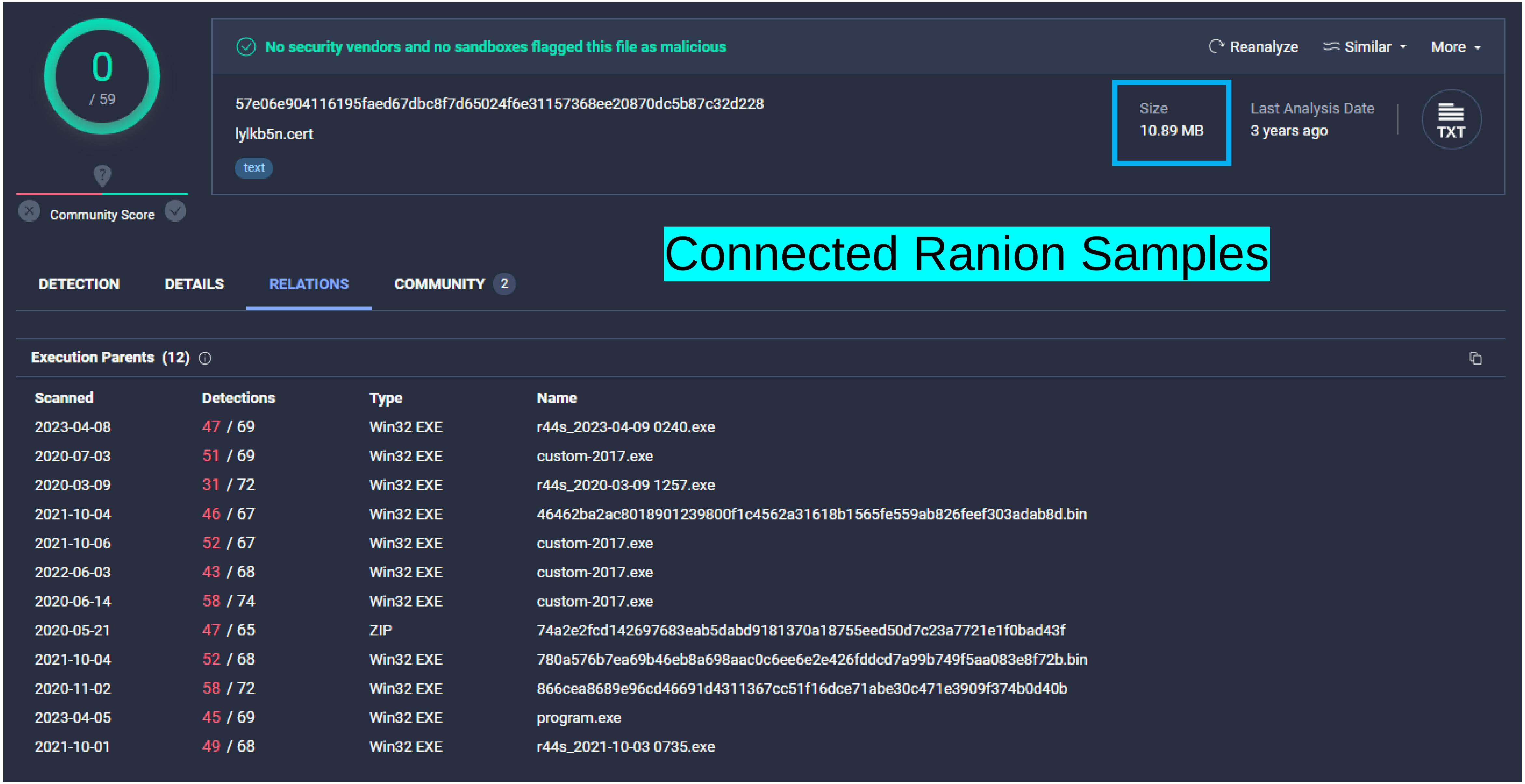
Windows 7 Prof
19 August 2021

Domain

64a10c38-6e07-4067-8bb6-af5dd1e95de9.usrfiles.com

VirusTotal

The .cert file is actually 0/59 FUD!



No security vendors and no sandboxes flagged this file as malicious

57e06e904116195faed67dbc8f7d65024f6e31157368ee20870dc5b87c32d228

lylkb5n.cert

text

Size
10.89 MB

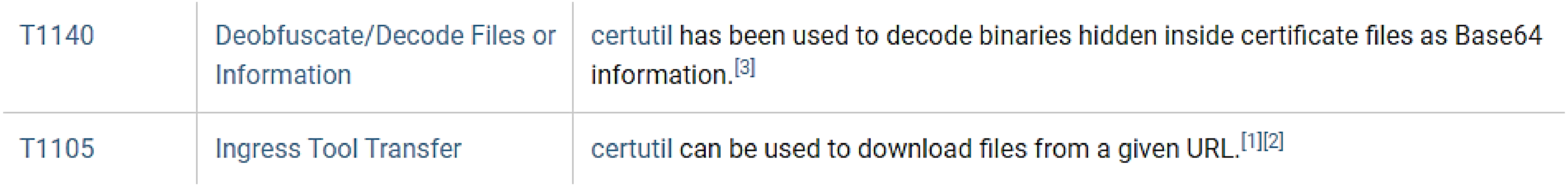
Last Analysis Date
3 years ago

Connected Ranion Samples

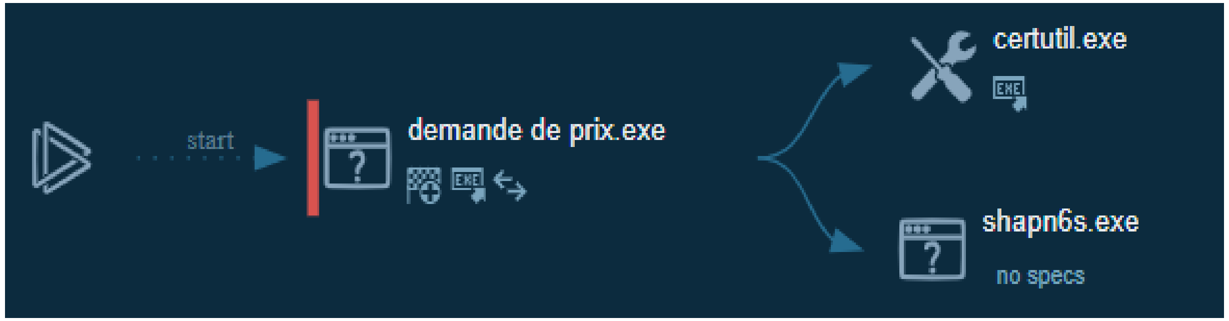
Execution Parents (12)

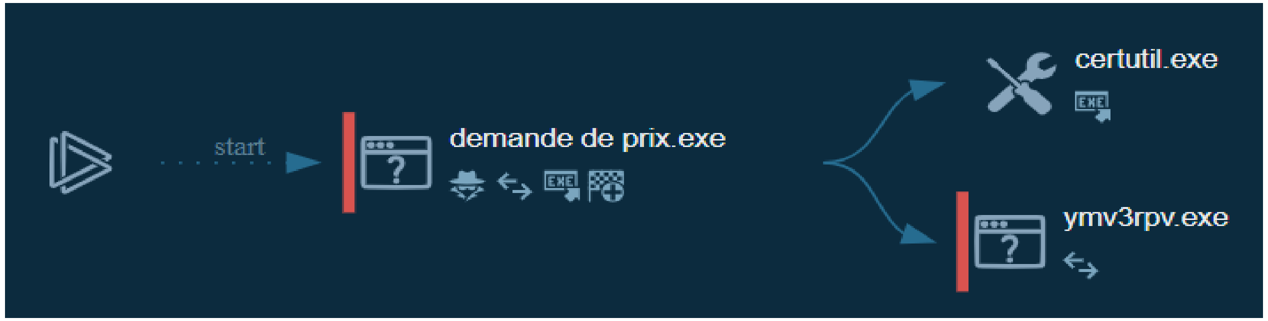
Scanned	Detections	Type	Name
2023-04-08	47 / 69	Win32 EXE	r44s_2023-04-09 0240.exe
2020-07-03	51 / 69	Win32 EXE	custom-2017.exe
2020-03-09	31 / 72	Win32 EXE	r44s_2020-03-09 1257.exe
2021-10-04	46 / 67	Win32 EXE	46462ba2ac8018901239800f1c4562a31618b1565fe559ab826feef303adab8d.bin
2021-10-06	52 / 67	Win32 EXE	custom-2017.exe
2022-06-03	43 / 68	Win32 EXE	custom-2017.exe
2020-06-14	58 / 74	Win32 EXE	custom-2017.exe
2020-05-21	47 / 65	ZIP	74a2e2fcd142697683eab5dabd9181370a18755eed50d7c23a7721e1f0bad43f
2021-10-04	52 / 68	Win32 EXE	780a576b7ea69b46eb8a698aac0c6ee6e2e426fddcd7a99b749f5aa083e8f72b.bin
2020-11-02	58 / 72	Win32 EXE	866cea8689e96cd46691d4311367cc51f16dce71abe30c471e3909f374b0d40b
2023-04-05	45 / 69	Win32 EXE	program.exe
2021-10-01	49 / 68	Win32 EXE	r44s_2021-10-03 0735.exe

CertUtil for Ranion payload decoding



T1140	Deobfuscate/Decode Files or Information	certutil has been used to decode binaries hidden inside certificate files as Base64 information.[3]
T1105	Ingress Tool Transfer	certutil can be used to download files from a given URL.[1][2]

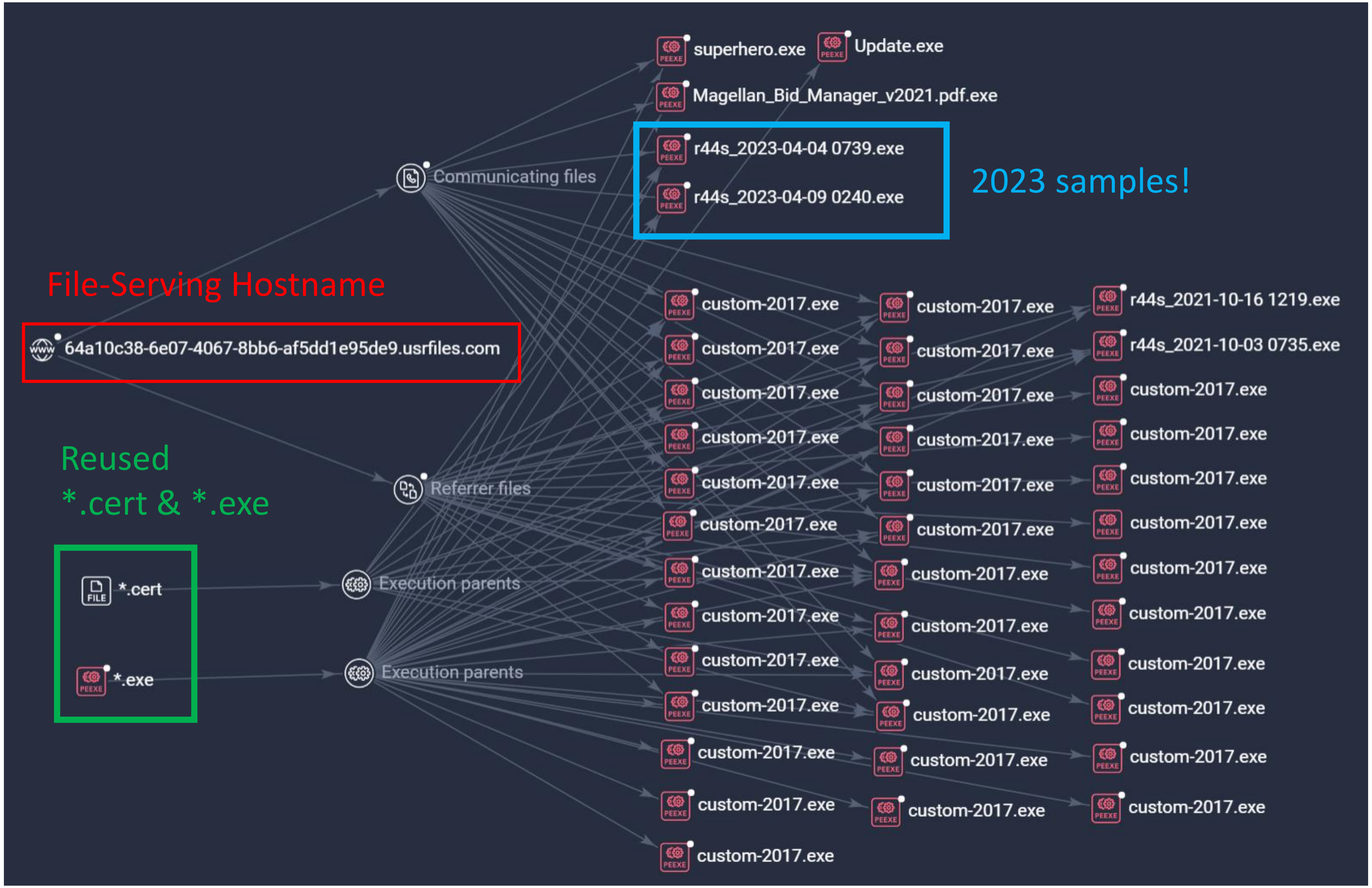




- "certutil.exe" –decod C:\Users\admin\AppData\Roaming\shapn6s.cert
- "C:\Users\admin\AppData\Roaming\shapn6s.exe"
- "C:\Users\admin\AppData\Roaming\shapn6s.exe" -HTTPTunnelPort 10080
- “C:\Users\Public\r44s_2021-09-10 1013.exe

Pivoting in VirusTotal

A lot more IOCs!

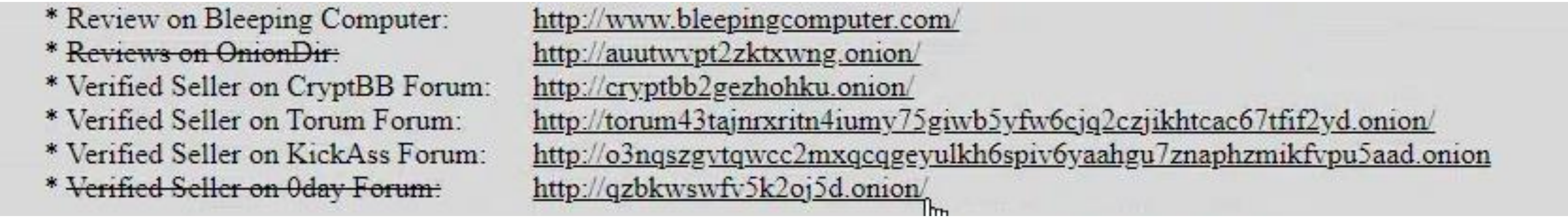

File-Serving Hostname

Reused
*.cert & *.exe

2023 samples!

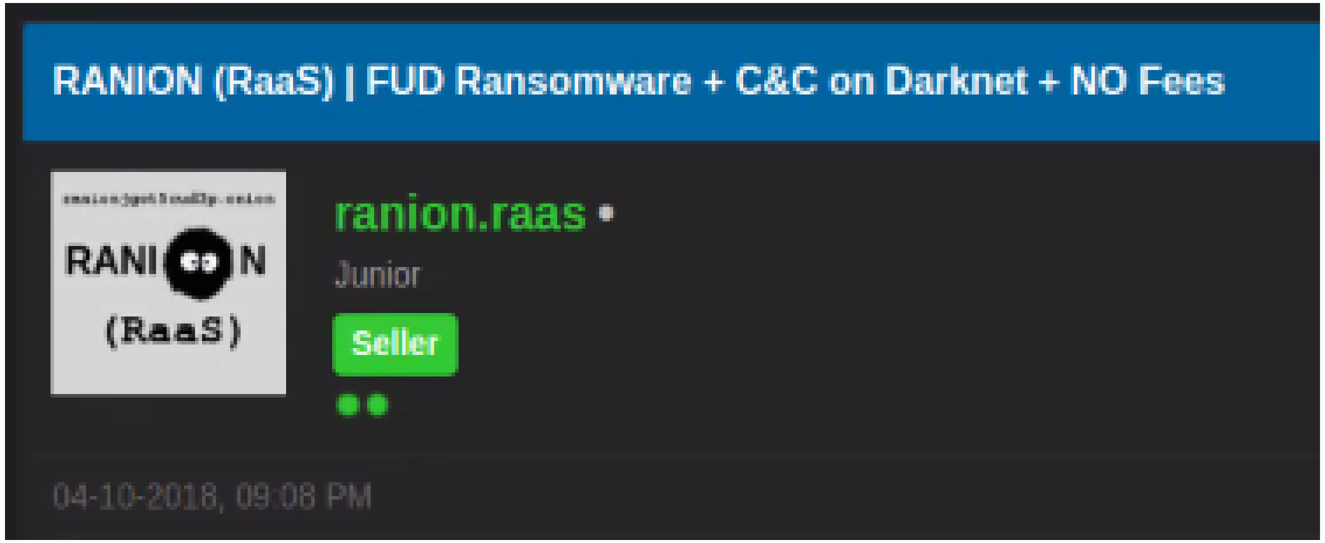
Adversary

Ranion on the Cybercrime Forums



* Review on Bleeping Computer:	http://www.bleepingcomputer.com/
* ~~Reviews on OnionDir:~~	http://auutwvpt2zktxwng.onion/
* Verified Seller on CryptBB Forum:	http://cryptbb2gezhohku.onion/
* Verified Seller on Torum Forum:	http://torum43tajnrxritn4iumy75giwb5yfw6cjq2czjikhtcac67tfif2yd.onion/
* Verified Seller on KickAss Forum:	http://o3nqszgvtqwcc2mxqcqgeyulkh6spiv6yaahgu7znaphzmikfvpu5aad.onion
* ~~Verified Seller on 0day Forum:~~	http://qzbkwswfv5k2oj5d.onion/

Ranion on CryptBB



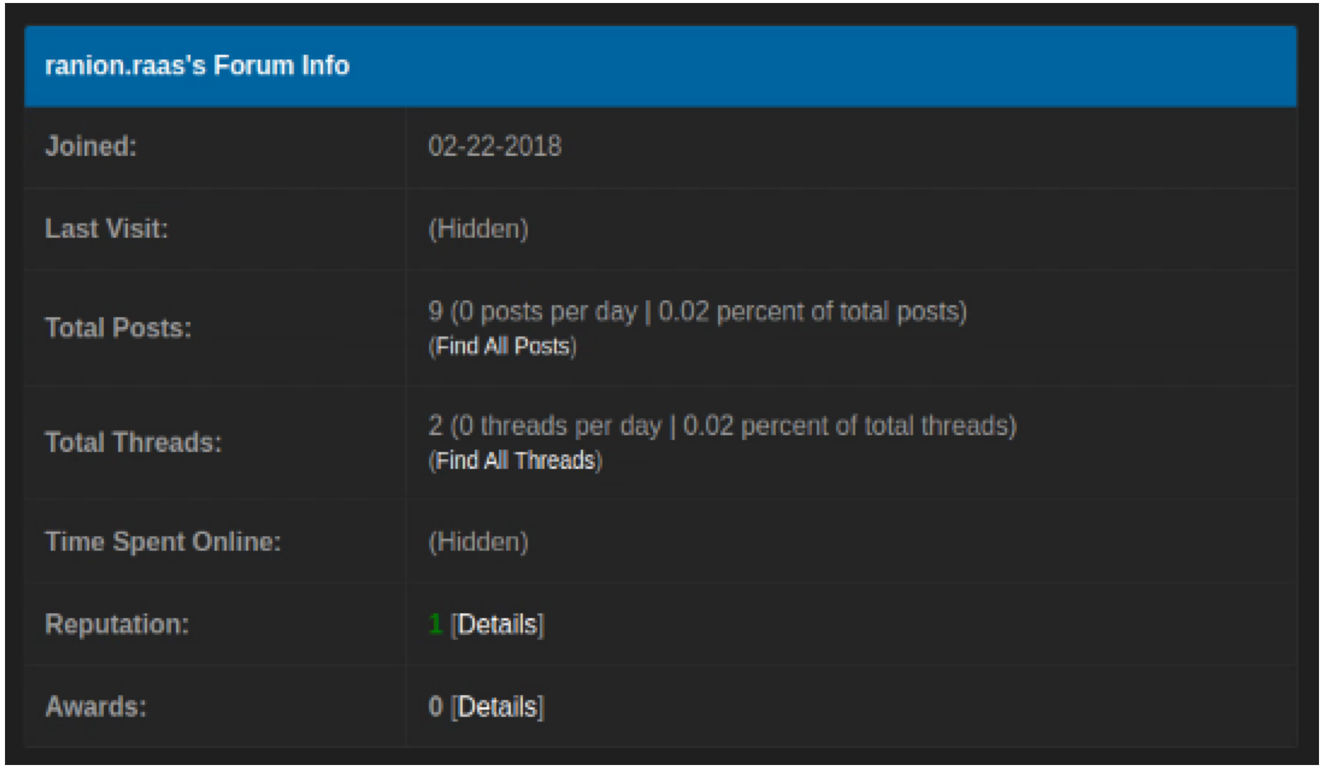
RANION (RaaS) | FUD Ransomware + C&C on Darknet + NO Fees

ranion.raas

Junior

Seller

04-10-2018, 09:08 PM



ranion.raas's Forum Info

Joined:	02-22-2018
Last Visit:	(Hidden)
Total Posts:	9 (0 posts per day | 0.02 percent of total posts) (Find All Posts)
Total Threads:	2 (0 threads per day | 0.02 percent of total threads) (Find All Threads)
Time Spent Online:	(Hidden)
Reputation:	1 [Details]
Awards:	0 [Details]

Username: “ranion.raas”
Account Type: Seller
Account Rating: Junior (New)

Joined: 22 February 2018

Total Post: 9
Total Threads: 2

Positive Reputation: +1
Last Visit: Hidden
Time Spent Online: Hidden

This is the last surviving profile, as the other forums have gone offline

Ranion operator on the Forums

- “ranionjgot5cud3p.onion” is shared in the Ranion operator’s original post
- Only advertised on English-speaking crimeware forums, somewhat unusual
- Thread: “RANION (RaaS) | FUD Ransomware + C&C On Darknet + NO Fees”

Forum	Date	Activity
Zeroday	24-May-2017	“ransion.raas” shared the first advert of Ranion
KickAss	01-Feb-2018	“ransionraas” advertised Ranion on KickAss
CryptBB	10-Apr-2018	“ranion.raas” advertised Ranion on CryptBB
Torum	07-Mar-2020	“ranion.raas” advertised Ranion on Torum
CryptBB	26-Oct-2021	“ranion.raas” explains that Ranion works with any .NET crypter

Ranion scams appear on the Forums

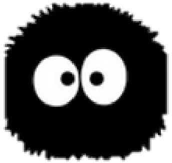
- Fake version of Ranion was spread around in August 2021
- Ranion operators warned about the scammers in September 2021

Forum	Date	Activity
Tape	16-Aug-2021	“Ranion” advertised fake Ranion on Tape
Club2Crd	16-Aug-2021	“Ranion” advertised fake Ranion on Club2Crd
World Forum	17-Aug-2021	“Ranion” advertised fake Ranion on World Forum
Torigon	23-Aug-2021	“Ranion.RaaS” advertised fake Ranion on Torigon
Best Carding World	29-Aug-2021	“Ranion” advertised fake Ranion on Best Carding World
CryptBB	12-Sept-2021	“ranion.raas” warns about the scammers and added a section to the actual Tor site about fake Tor sites

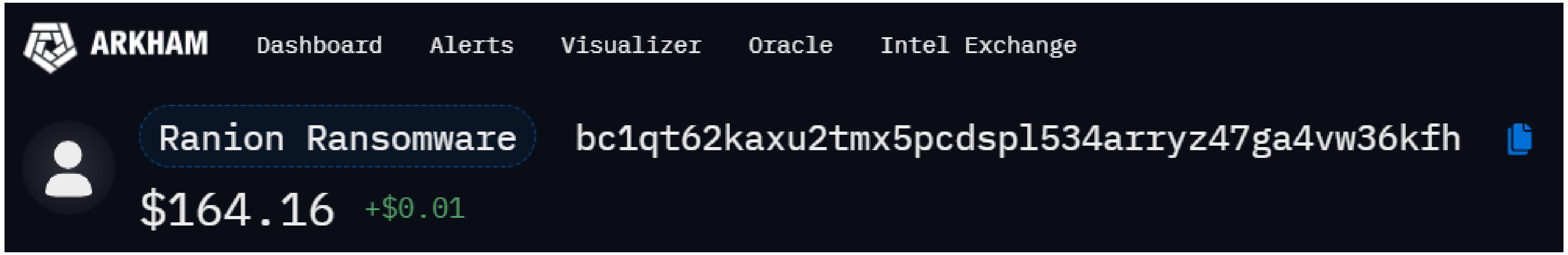
Ranion customers on the Forums

Forum	Date	Activity
KickAss	20-Jul-2018	“slasher1” informed “ranionraas” they bought Ranion
CryptBB	28-Jun-2018	“Tiren72” replied to “ranion.raas” they recommend Ranion
Torum	13-June-2019	“kingofspades” recommended **“.exe can be stitched to PDFs”** on a thread about Ranion ransomware
CryptBB	07-Mar-2020	“Funshine” replied to “ranion.raas” they recommend Ranion
CryptBB	18-May-2022	“Sn1PeR” paid and sent an email and never received a reply from Ranion
CryptBB	01-Jun-2022	“bentleybitup” wrote that Ranion is not worth any money as it is a copy of **HiddenTear** and recommends using leaked **Babuk** or **Conti**

How much is Ranion making?

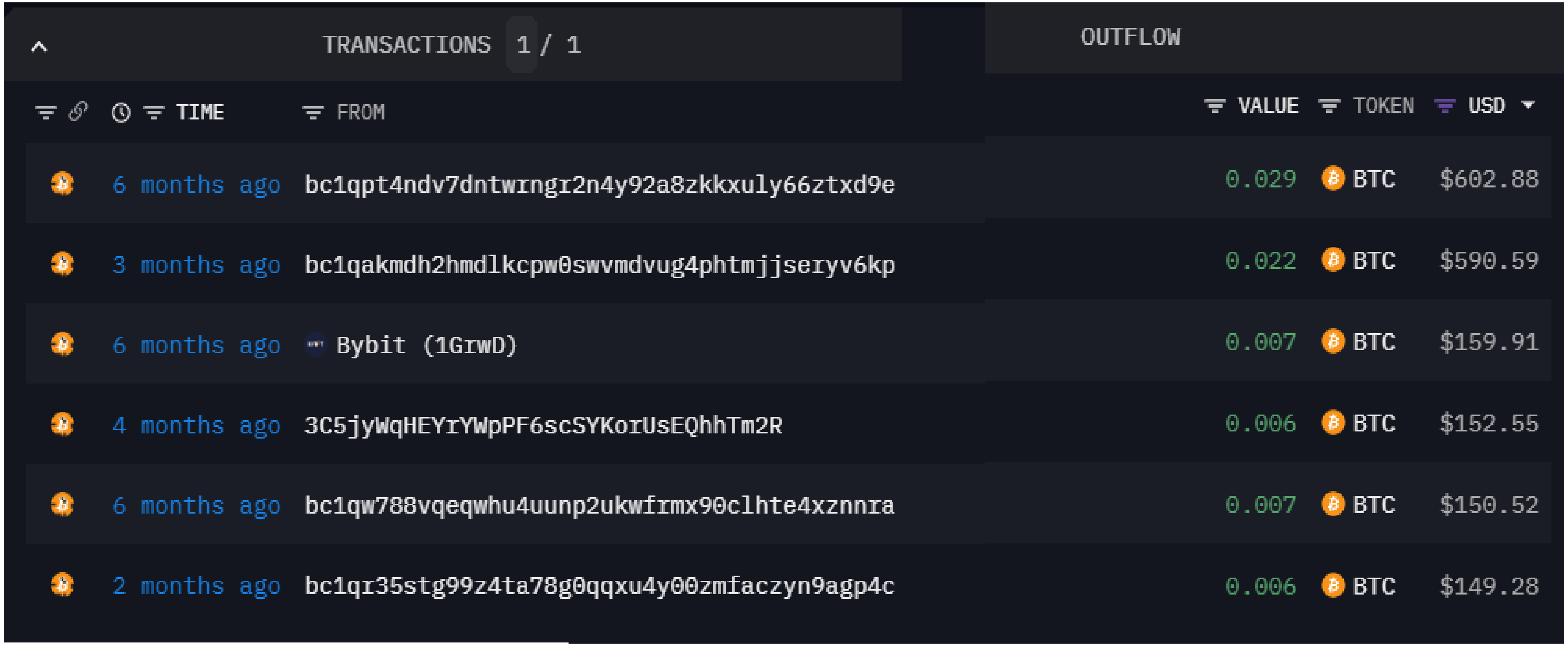


BTC Address from the Tor Site:



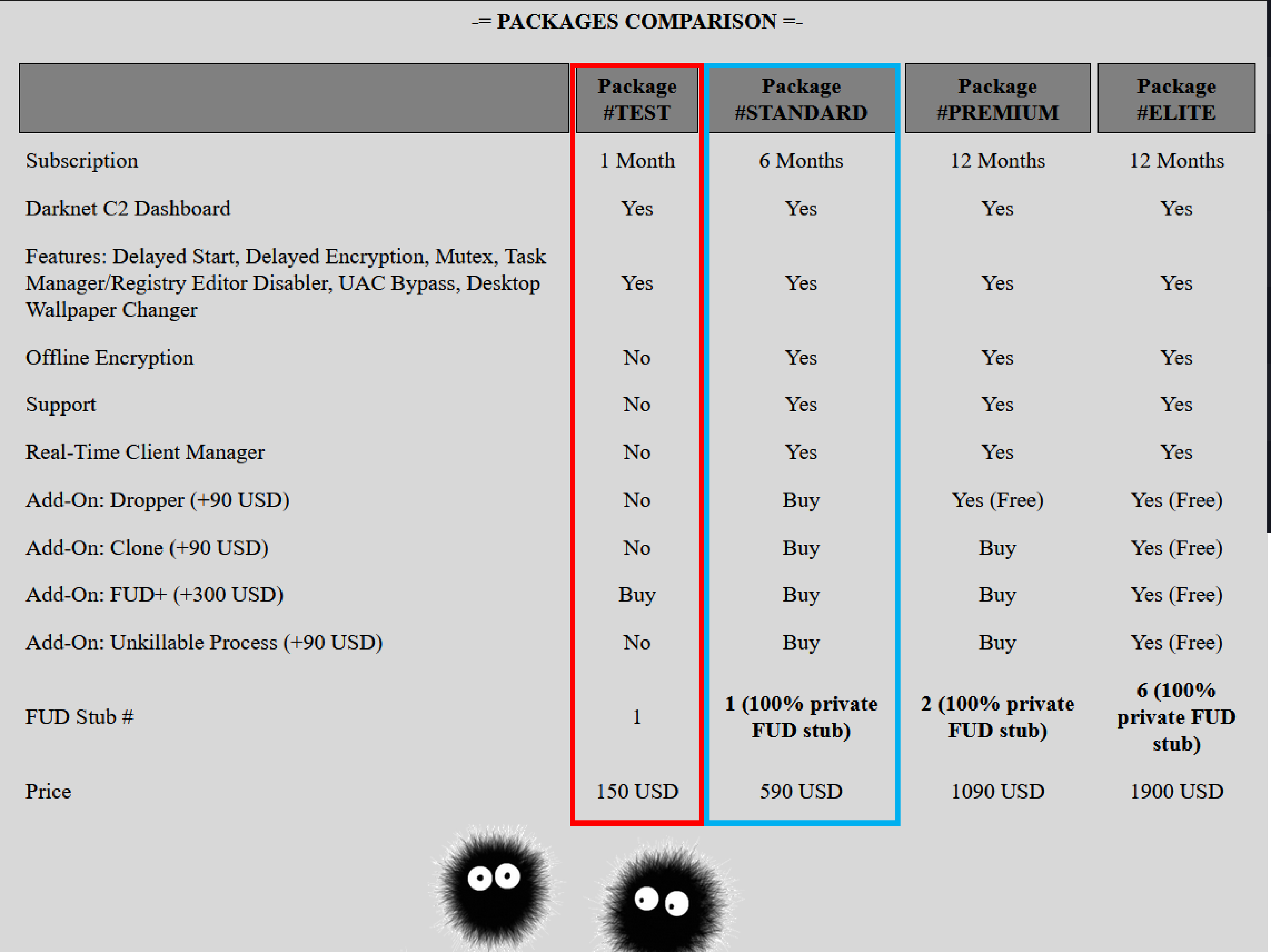
Ranion Ransomware bc1qt62kaxu2tmx5pcdspl534arryz47ga4vw36kfh

$164.16 +$0.01



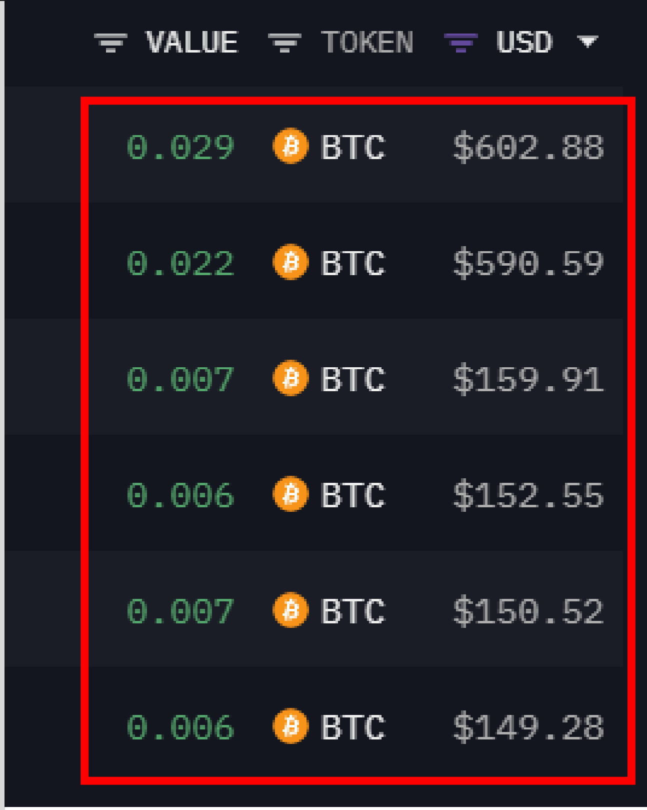
TIME	FROM	VALUE	TOKEN	USD
6 months ago	bc1qpt4ndv7dntwrngr2n4y92a8zkkxuly66ztxd9e	0.029	BTC	$602.88
3 months ago	bc1qakmdh2hmdlkcpw0swvmdvug4phtmjjseryv6kp	0.022	BTC	$590.59
6 months ago	Bybit (1GrwD)	0.007	BTC	$159.91
4 months ago	3C5jyWqHEYrYWpPF6scSYKorUsEQhhTm2R	0.006	BTC	$152.55
6 months ago	bc1qw788vqeqwhu4uunp2ukwfrmx90clhte4xznnra	0.007	BTC	$150.52
2 months ago	bc1qr35stg99z4ta78g0qqxu4y00zmfaczyn9agp4c	0.006	BTC	$149.28

~$1.8k
19 Jan – 19 May 2023



-= PACKAGES COMPARISON =-

	Package #TEST	Package #STANDARD	Package #PREMIUM	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C2 Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Add-On: Dropper (+90 USD)	No	Buy	Yes (Free)	Yes (Free)
Add-On: Clone (+90 USD)	No	Buy	Buy	Yes (Free)
Add-On: FUD+ (+300 USD)	Buy	Buy	Buy	Yes (Free)
Add-On: Unkillable Process (+90 USD)	No	Buy	Buy	Yes (Free)
FUD Stub #	1	**1 (100% private FUD stub)**	**2 (100% private FUD stub)**	**6 (100% private FUD stub)**
Price	150 USD	590 USD	1090 USD	1900 USD



VALUE	TOKEN	USD
0.029	BTC	$602.88
0.022	BTC	$590.59
0.007	BTC	$159.91
0.006	BTC	$152.55
0.007	BTC	$150.52
0.006	BTC	$149.28

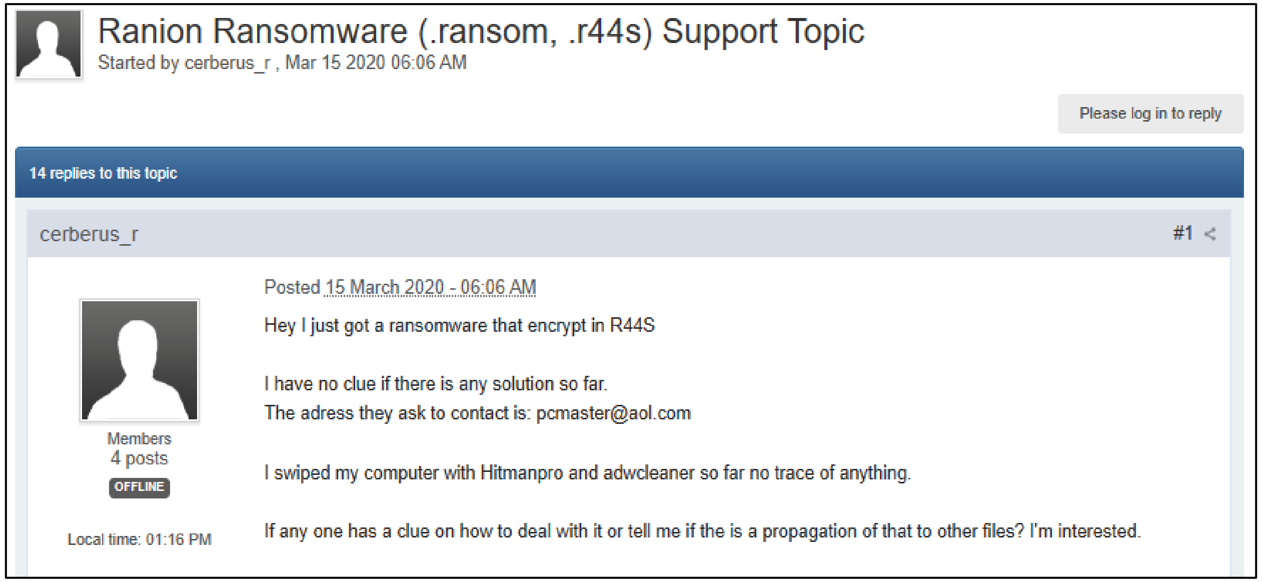
Ranion Affiliates:

4x Test Package

2x Standard Package

Victims

Ranion victims on BleepingComputer Forums



Ranion Ransomware (.ransom, .r44s) Support Topic

Started by cerberus_r , Mar 15 2020 06:06 AM

14 replies to this topic

cerberus_r #1

Posted 15 March 2020 - 06:06 AM

Hey I just got a ransomware that encrypt in R44S

I have no clue if there is any solution so far.
The adress they ask to contact is: pcmaster@aol.com

I swiped my computer with Hitmanpro and adwcleaner so far no trace of anything.

If any one has a clue on how to deal with it or tell me if the is a propagation of that to other files? I'm interested.

Victim 1 Details:

pcmaster@aol.com

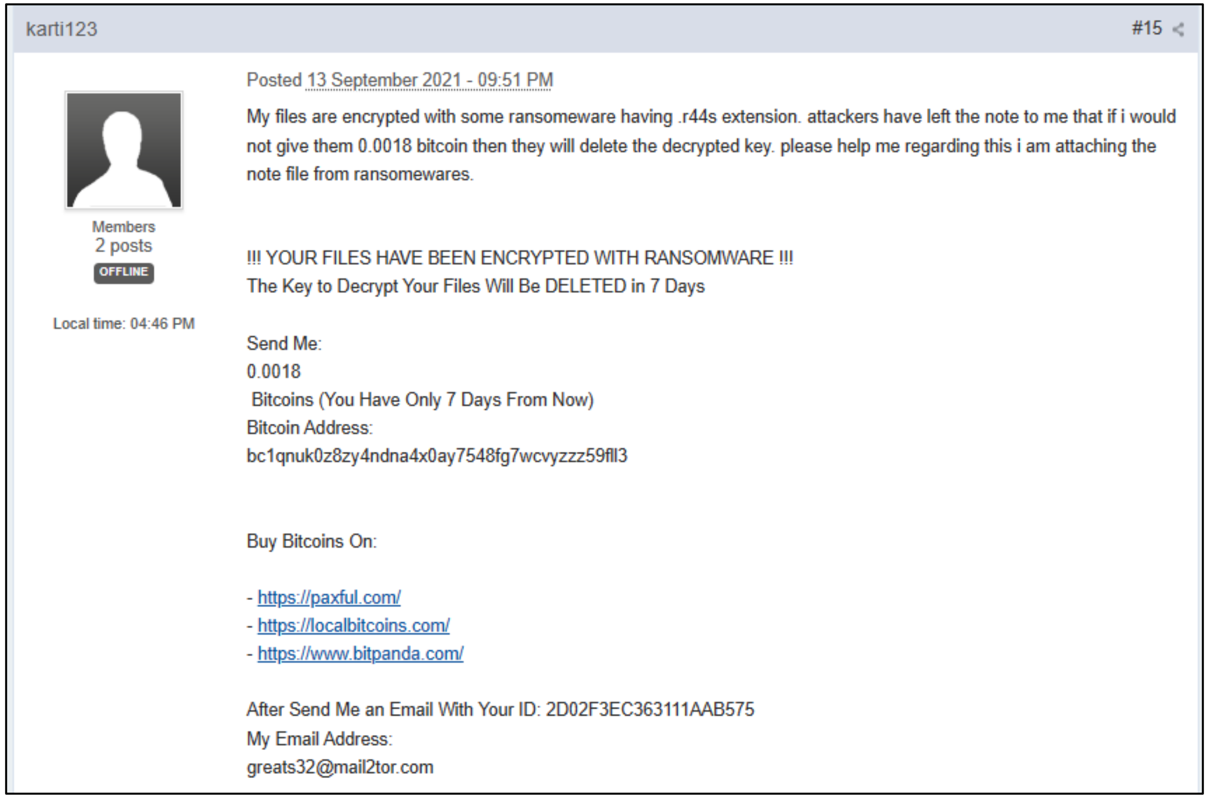
".r44s" extension

Victim 2 Details:

greats@mail2tor.com

".r44s" extension

bc1qnuk0z8zy4ndna4x0ay7548fg7wcvyzzz59fll3



karti123 #15

Posted 13 September 2021 - 09:51 PM

My files are encrypted with some ransomeware having .r44s extension. attackers have left the note to me that if i would not give them 0.0018 bitcoin then they will delete the decrypted key. please help me regarding this i am attaching the note file from ransomewares.

!!! YOUR FILES HAVE BEEN ENCRYPTED WITH RANSOMWARE !!!
The Key to Decrypt Your Files Will Be DELETED in 7 Days

Send Me:
0.0018
Bitcoins (You Have Only 7 Days From Now)
Bitcoin Address:
bc1qnuk0z8zy4ndna4x0ay7548fg7wcvyzzz59fll3

Buy Bitcoins On:

- https://paxful.com/
- https://localbitcoins.com/
- https://www.bitpanda.com/

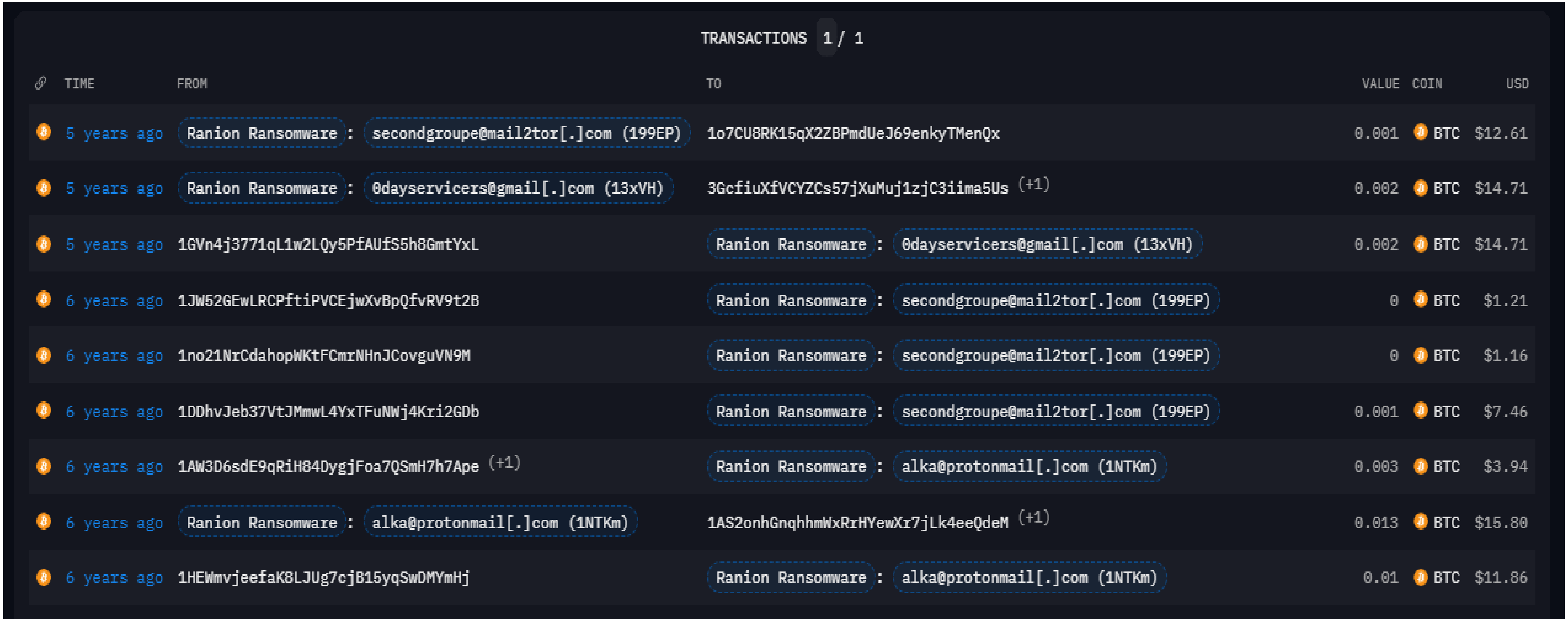
After Send Me an Email With Your ID: 2D02F3EC363111AAB575
My Email Address:
greats32@mail2tor.com

Victim BTC Addresses via OSINT

Ransom Note	Email Address	BTC Address
1	ssdt3@protonmail[.]com	1HDGQjPhe2pakxKJanQv7NuNQRSKQW4C
2	ToEasyyy4u@protonmail[.]com	1FnERg6NMCZeB9jgUtJT6G9uqfwQ3uJYpj
3	secondgroupe@mail2tor[.]com	199EPfkH6t1iXZNp5H8QYwHwHELLWxARRh
4	alka@protonmail[.]com	1NTKmeeLp52y9oZVfVZEdUCJBK9xhTcZNW
5	0dayservicers@gmail[.]com	13xVHparL62HuG8mRm42CBTZT6MtnrSytC
6	chimera@secmail[.]pro	1Pyy5WHoqQeGk9zKn9f72uL4hbF5mhf7ec
7	ransunlock@protonmail[.]com	1LSstcRAu1xGueBJRuyUgHi18PEPHxztvR
8	pc.master@aol[.]com	1X3eCf1JriycNiWwpNHyQamZS1pApE8XX
9	contactfordecrypt@secmail[.]pro	N/A
10	greats32@mail2tor.com	bc1qnuk0z8zy4ndna4x0ay7548fg7wcvyzzz59fll3

Victim Blockchain Analysis

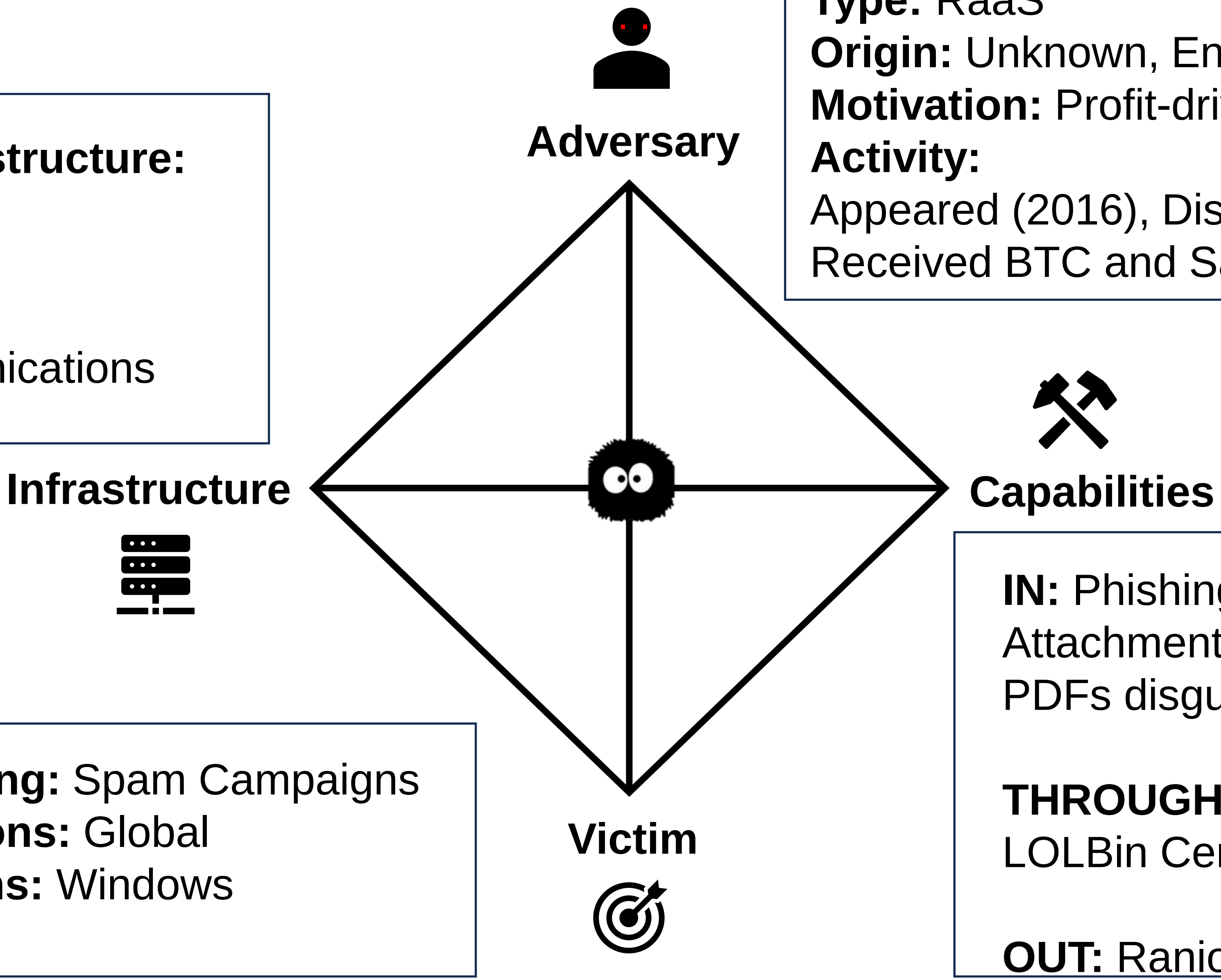
Total Amount these RaaS Affiliates Made: $83.46



TRANSACTIONS 1 / 1

TIME	FROM	TO	VALUE	COIN	USD
5 years ago	Ranion Ransomware : secondgroupe@mail2tor[.]com (199EP)	1o7CU8RK15qX2ZBPmdUeJ69enkyTMenQx	0.001	BTC	$12.61
5 years ago	Ranion Ransomware : 0dayservicers@gmail[.]com (13xVH)	3GcfiuXfVCYZCs57jXuMuj1zjC3iima5Us (+1)	0.002	BTC	$14.71
5 years ago	1GVn4j3771qL1w2LQy5PfAUfS5h8GmtYxL	Ranion Ransomware : 0dayservicers@gmail[.]com (13xVH)	0.002	BTC	$14.71
6 years ago	1JW52GEwLRCPftiPVCEjwXvBpQfvRV9t2B	Ranion Ransomware : secondgroupe@mail2tor[.]com (199EP)	0	BTC	$1.21
6 years ago	1no21NrCdahopWKtFCmrNHnJCovguVN9M	Ranion Ransomware : secondgroupe@mail2tor[.]com (199EP)	0	BTC	$1.16
6 years ago	1DDhvJeb37VtJMmwL4YxTFuNWj4Kri2GDb	Ranion Ransomware : secondgroupe@mail2tor[.]com (199EP)	0.001	BTC	$7.46
6 years ago	1AW3D6sdE9qRiH84DygjFoa7QSmH7h7Ape (+1)	Ranion Ransomware : alka@protonmail[.]com (1NTKm)	0.003	BTC	$3.94
6 years ago	Ranion Ransomware : alka@protonmail[.]com (1NTKm)	1AS2onhGnqhhmWxRrHYewXr7jLk4eeQdeM (+1)	0.013	BTC	$15.80
6 years ago	1HEWmvjeefaK8LJUg7cjB15yqSwDMYmHj	Ranion Ransomware : alka@protonmail[.]com (1NTKm)	0.01	BTC	$11.86

Ranion Operator Diamond Model



Type: RaaS
Origin: Unknown, English-speaking
Motivation: Profit-driven
Activity:
Appeared (2016), Disappeared (2022),
Received BTC and Samples (2023)

Support Infrastructure:
usrfiles[.]com
Tor Services
BTC Wallet(s)
Email Communications

IN: Phishing Email
Attachments
PDFs disguised as EXEs

THROUGH: Windows
LOLBin CertUtil.exe

OUT: Ranion Ransomware

Targeting: Spam Campaigns
Locations: Global
Systems: Windows

Practical Cybercrime Intelligence

Methodical Investigations

- Discovery – Identifying Ranion
- Interaction – Visiting The Site
- Extraction – Gathering Information
- Research – Additional Context
- Pivoting – Widen The Scope
- Profiling – Summarize Your Results