Trellix

# Ghosts of REvil:

## An Inside Look with the Hacker Behind the Kaseya Ransomware Attack



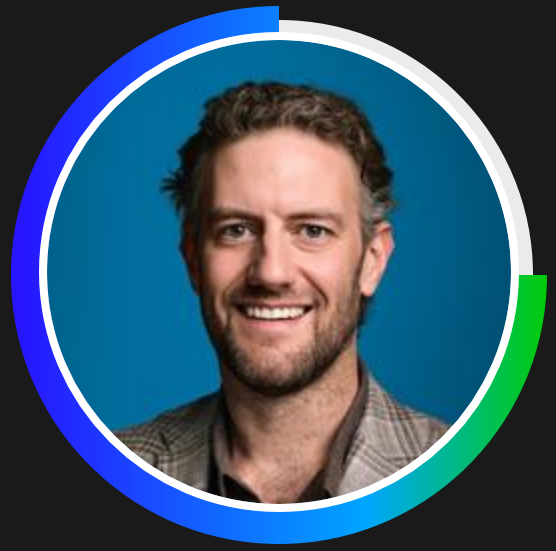
ANALYST1™

# Hosts for Today



**Jon DiMaggio**

Chief Security Strategist, Analyst1

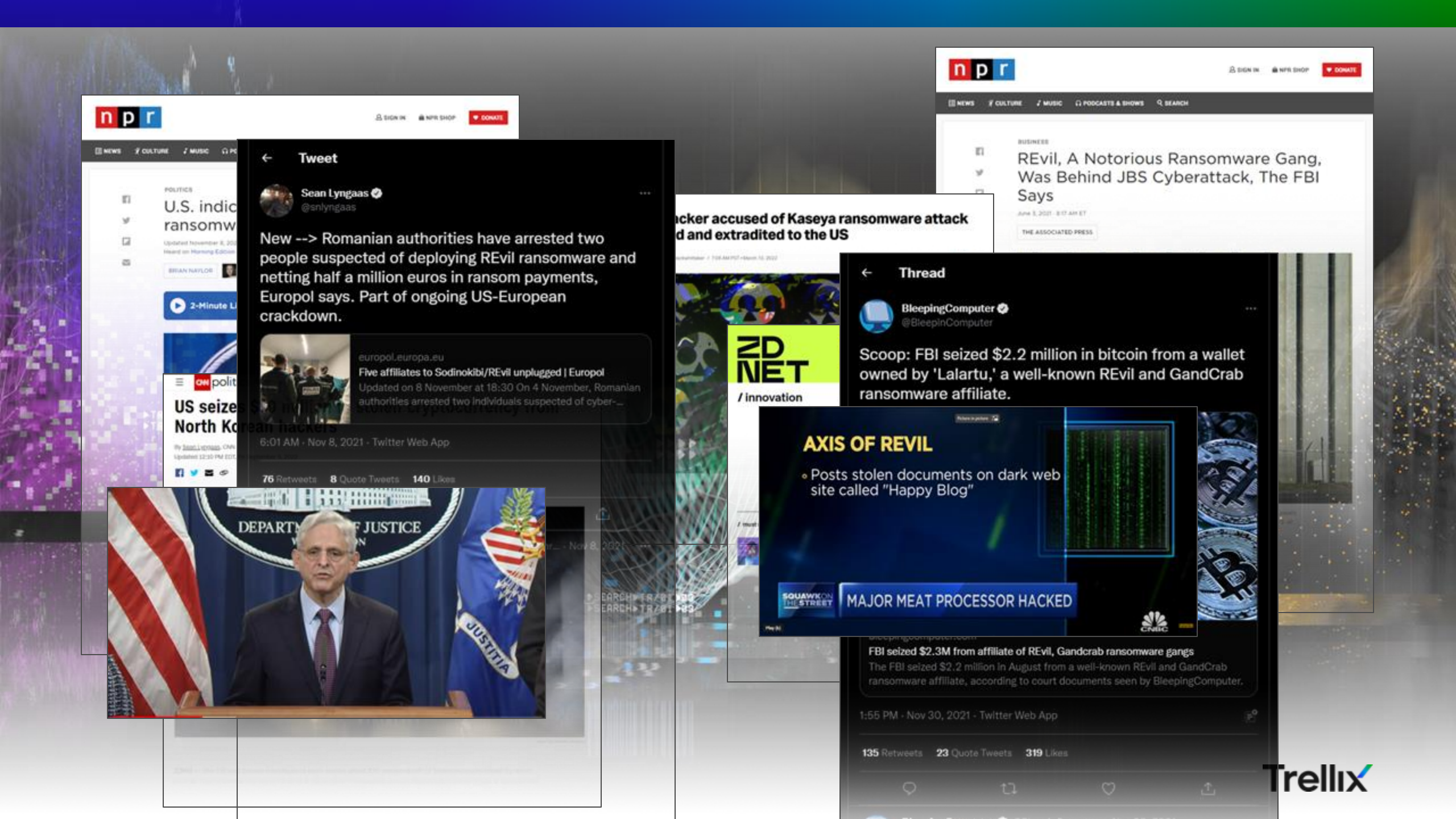


**John Fokker**

Head of Threat Intelligence, Trellix

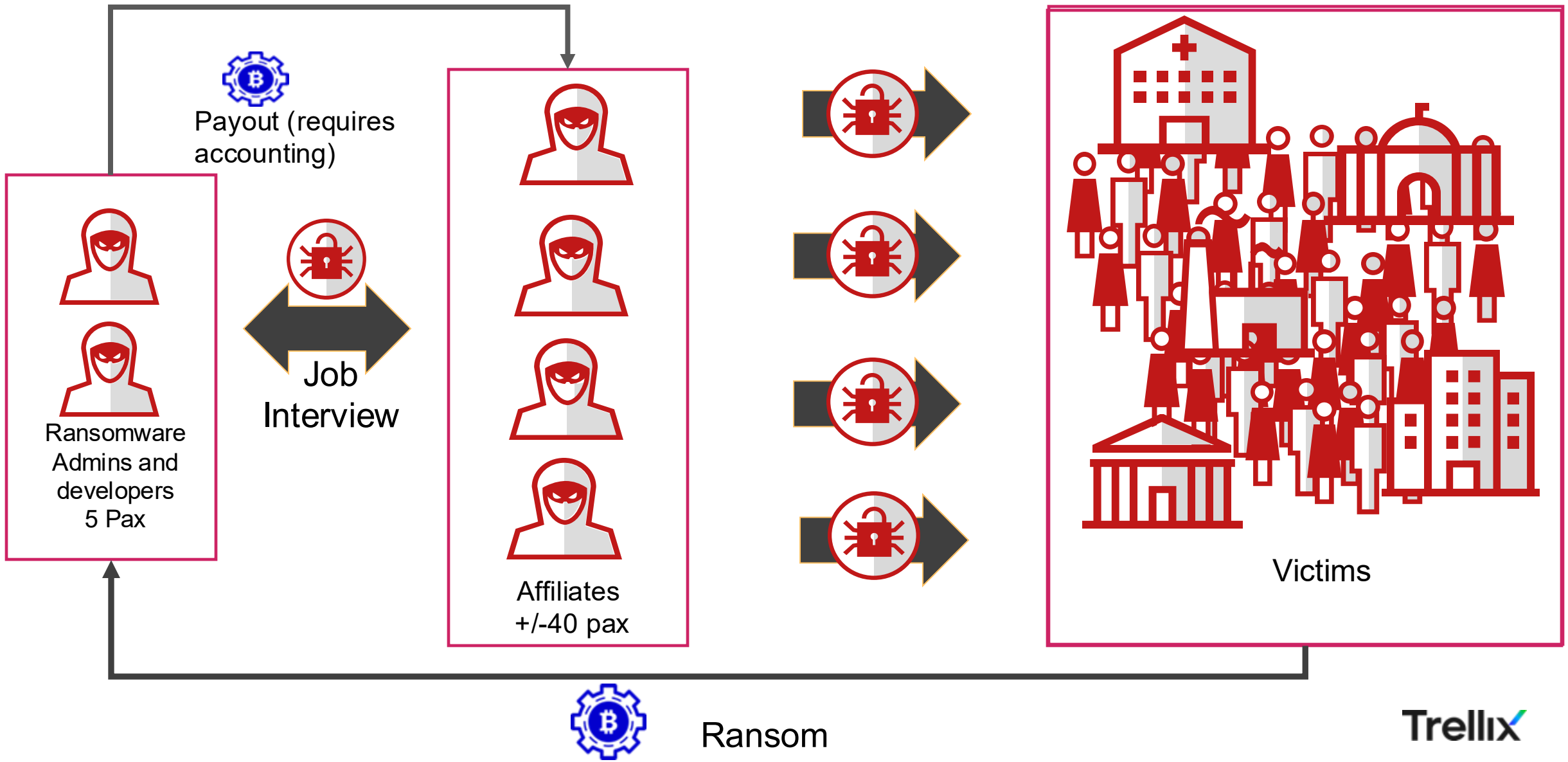
Trellix

ANALYST1


npr
REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says
Tweet
Sean Lyngaas
@snlyngaas
New --> Romanian authorities have arrested two people suspected of deploying REvil ransomware and netting half a million euros in ransom payments, Europol says. Part of ongoing US-European crackdown.
europol.europa.eu
Five affiliates to Sodinokibi/REvil unplugged | Europol
Updated on 8 November at 18:30 On 4 November, Romanian authorities arrested two individuals suspected of cyber-...
6:01 AM · Nov 8, 2021 · Twitter Web App
76 Retweets 8 Quote Tweets 140 Likes
ZDNET
/ innovation
Thread
BleepingComputer
@BleepinComputer
Scoop: FBI seized $2.2 million in bitcoin from a wallet owned by 'Lalartu,' a well-known REvil and GandCrab ransomware affiliate.
AXIS OF REVIL
Posts stolen documents on dark web site called "Happy Blog"
SQUAWK ON THE STREET
MAJOR MEAT PROCESSOR HACKED
CNBC
FBI seized $2.3M from affiliate of REvil, Gandcrab ransomware gangs
The FBI seized $2.2 million in August from a well-known REvil and GandCrab ransomware affiliate, according to court documents seen by BleepingComputer.
1:55 PM · Nov 30, 2021 · Twitter Web App
135 Retweets 23 Quote Tweets 319 Likes
JUSTICE
JUSTITIA

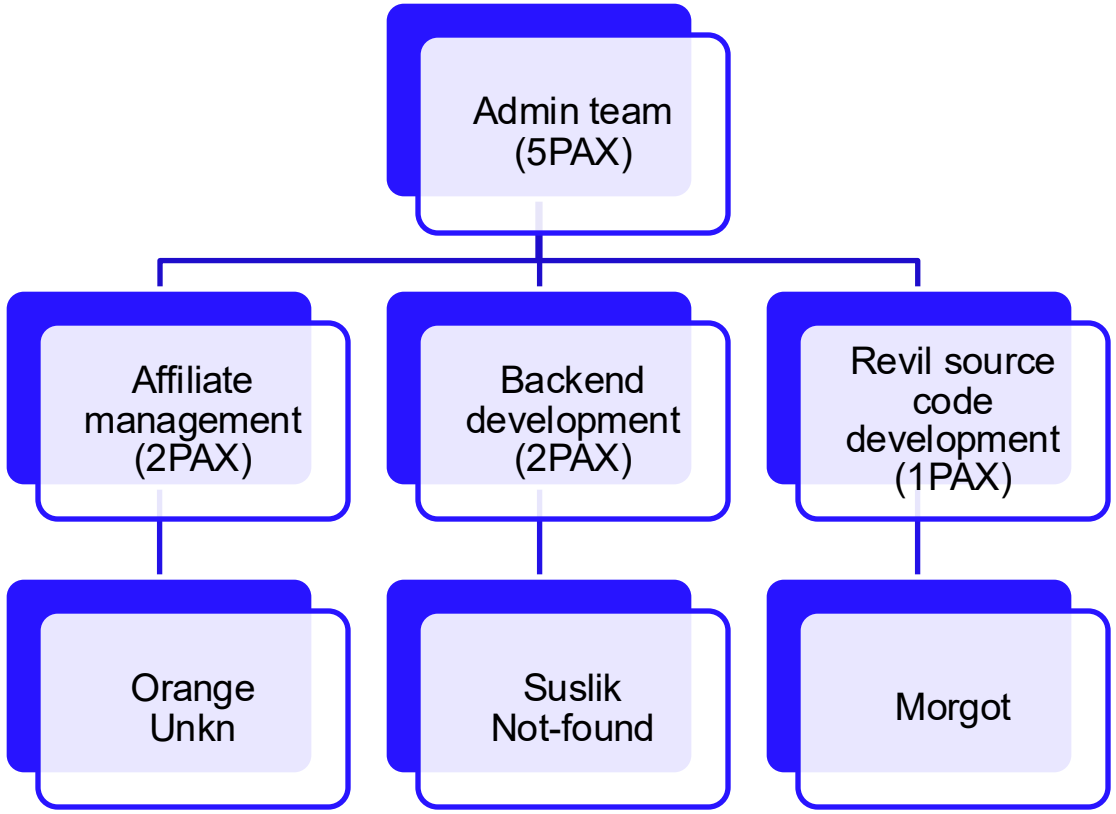
Trellix

# Revil Ransomware-as-a-Service (RaaS) Model




Trellix

# REVIL Core Operators




**Alternative Jabber accounts:**

**Orange**: Bitcoin, FunnyCrab

**Unkn**: 8800553535, Crab

**Suslik**: Eddie Bravo

**Morgot**: Rcode, Quake3

Trellix

ANALYST1

# REvil Key Success Factors

- Dedicated comms platform vs. Email negotiations
- Leak site to publish stolen data
- Stable Malware and Decryptors
- Increase of available affiliate spots strict selection
- Outsourcing or partnering with facilitating services (Malware obfuscation, Exploit Kits, Customer service Money laundering etc)
- Good administration of infections.




Trellix

# Accounting is Hard, but Affiliate Numbers Help…



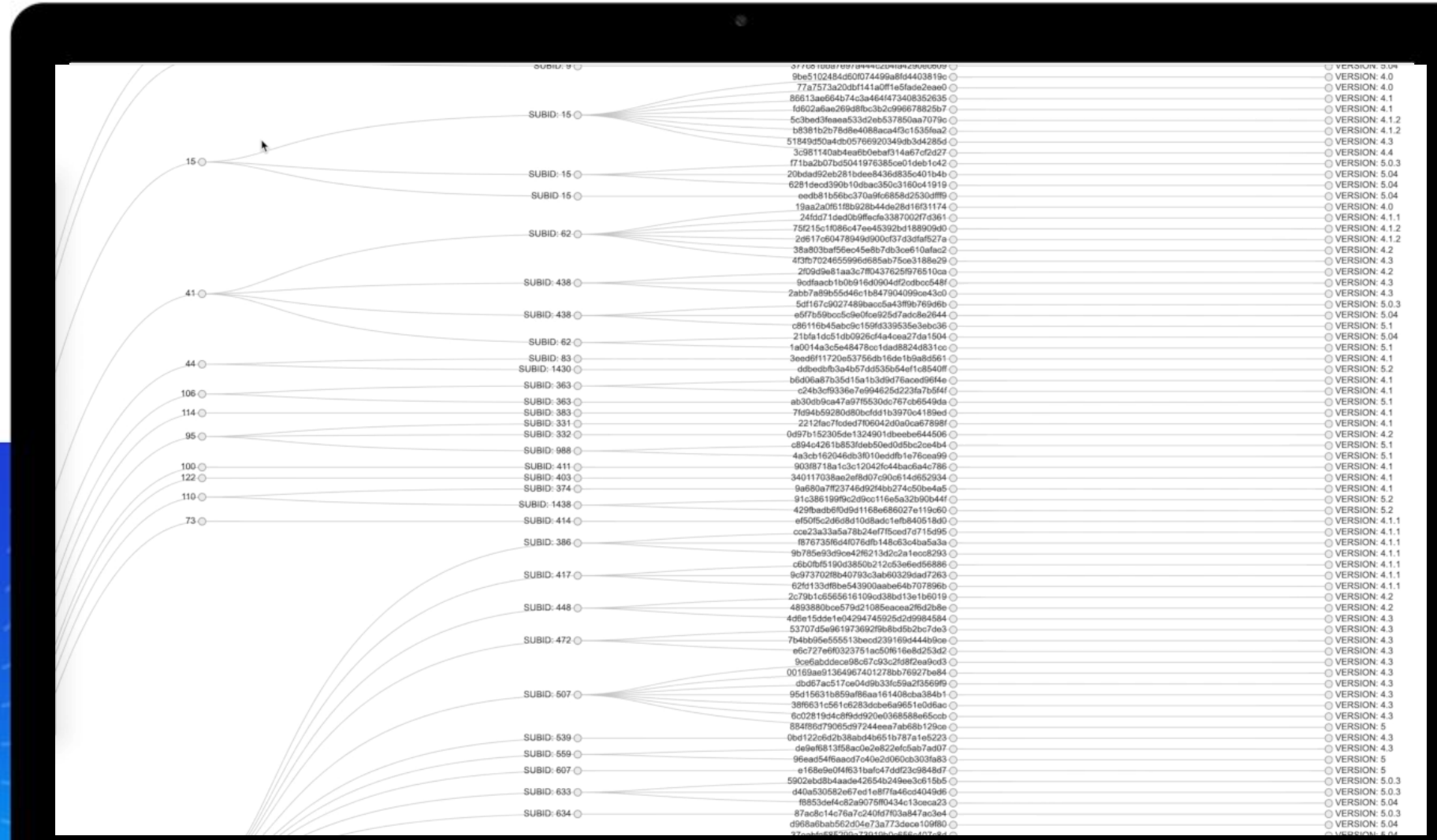

Trellix developed a custom Config extraction tool, for internal use and LE incident response.

Trellix

# Ransomware Accounting



| File Name | | Description |
|---|---|---|
| **pk** | | Public key of the attacker in Base64 |
| **pid** | | Affiliate number |
| **sub** | | Sub-account or campaign id |
| **dbg** | | Debug option |
| **fast** | | Option to encrypt the first 1 megabyte of each target file or all files |
| **wipe** | | Option to wipe specific files in the field ‘wfld’ |
| | **fld** | Folders whitelist |
| **wht** | **fls** | File whitelist |
| | **ext** | List of targeted extensions |
| **wfid** | | List of targeted folders |
| **prc** | | List of processes to kill |
| **dmn** | | List of C2 domains |
| **net** | | Option to specify the connexion to C2 |
| **nbody** | | Ransom not in base64 |
| **nname** | | Strings of malware name |
| **exp** | | Enable exploit CVE-2018-8453 |
| **img** | | Wallpaper ransom note in base64 |


15
41
44
106
114
95
100
122
110
73
SUBID: 15
SUBID: 15
SUBID 15
SUBID: 62
SUBID: 438
SUBID: 438
SUBID: 62
SUBID: 83
SUBID: 1430
SUBID: 363
SUBID: 363
SUBID: 383
SUBID: 331
SUBID: 332
SUBID: 988
SUBID: 411
SUBID: 403
SUBID: 374
SUBID: 1438
SUBID: 414
SUBID: 386
SUBID: 417
SUBID: 448
SUBID: 472
SUBID: 507
SUBID: 539
SUBID: 559
SUBID: 607
SUBID: 633
SUBID: 634
9be5102484d60f074499a8fd44403819c
77a7573a20dbf141a0ff1e5fade2eae0
86613ae664b74c3a464f473408352635
fd602a6ae269d8fbc3b2c996678825b7
5c3bed3feaea533d2eb537850aa7079c
b8381b2b78d8e4088aca4f3c1535fea2
51849d50a4db05766920349db3d4285d
3c981140ab4ea6b0ebaf314a67cf2d27
f71ba2b07bd5041976385ce01deb1c42
20bdad92eb281bdee8436d835c401b4b
6281decd390b10dbac350c3160c41919
eedb81b56bc370a9fc6858d2530dfff9
19aa2a0f61f8b928b44da28d16f31174
24fdd71ded0b9ffecfe3387002f7d361
75f215c1f086c47ee45392bd188909d0
2d617c60478949d900cf37d3faf527a
38a803baf56ec45e8b7db3ce610afac2
4f3fb702465599fd685ab75ce3188e29
2f09d9e81aa3c7f043762f5f97651 0ca
9cdfaacb1b0b916d0904df2cdbcc548f
2abb7a89b55d46c1b847904099ce43c0
5df167c9027489bacc5a43ff9b769d6b
e5f7b59bcc5c9e0fce925d7adc8e2644
c86116b45abc9c159fd339535e3ebc36
21bfa1dc51db0926cf4a4cea27da1504
1a0014a3c5e48478cc1dad8824d831cc
3eed6f11720e53756db16de1b9a8d561
ddbedbfb3a4b57dd535b54ef1c8540ff
b6d06a87b35d15a1b3d9d76aced96f4e
c24b3cf9336e7e994625d223fa7b5f4f
ab30db9ca47a97f5530dc767cb6549da
7fd94b59280d80bcfdd1b3970c4189ed
2212fac7fcded7f06042d0a0ca67898f
0d97b152305de1324901dbeebe644506
c894c4261b853fdeb50ed0d5bc2ce4b4
4a3cb162046db3f010eddfb1e76cea99
903f8718a1c3c12042fc44bac6a4c786
340117038ae2ef8d07c90c614d652934
9a680a7ff23746d92f4bb274c50be4a5
91c386199f9c2d9cc116e5a32b90b44f
429fbadb6f0d9d1168e686027e119c60
ef50f5c2d6d8d10d8adc1efb840518d0
cce23a33a5a78b24ef7f5ced7d715d95
f876735f6d4f076dfb148c63c4ba5a3a
9b785e93d9ce42f6213d2c2a1ecc8293
c6b0fbf5190d3850b212c53e6ed56886
9c973702f8b40793c3ab60329dad7263
62fd133df8be543900aabe64b707896b
2c79b1c6565616109cd38bd13e1b6019
4893880bce579d21085eacea2f6d2b8e
4d6e15dde1e04294745925d2d9984584
53707d5e9619736 92f9b8bd5b2bc7de3
7b4bb95e555513becd239169d444b9ce
e6c727e6f03237 51ac50f616e8d253d2
9ce6abddece98c67c93c2fd8f2ea9cd3
00169ae9136496740 1278bb76927be84
dbd67ac517ce04d9b33fc59a2f3569f9
95d15631b859af86aa161408cba384b1
38f6631c561c6283dcbe6a9651e0d6ac
6c02819d4c8f9dd920e0368588e65ccb
884f86d79065d97244eea7ab68b129ce
0bd122c6d2b38abd4b651b787a1e5223
de9ef6813f58ac0e2e822efc5ab7ad07
96ead54f6aacd7c40e2d060cb303fa83
e168e9e0f4f631bafc47ddf23c9848d7
5902ebd8b4aade42654b249ee3c615b5
d40a530582e67ed1e8f7fa46cd4049d6
f8853def4c82a9075ff0434c13ceca23
87ac8c14c76a7c240fd7f03a847ac3e4
d968a6bab562d04e73a773dece109f80
VERSION: 4.0
VERSION: 4.0
VERSION: 4.1
VERSION: 4.1
VERSION: 4.1.2
VERSION: 4.1.2
VERSION: 4.3
VERSION: 4.4
VERSION: 5.0.3
VERSION: 5.04
VERSION: 5.04
VERSION: 5.04
VERSION: 4.0
VERSION: 4.1.1
VERSION: 4.1.2
VERSION: 4.1.2
VERSION: 4.2
VERSION: 4.3
VERSION: 4.2
VERSION: 4.3
VERSION: 4.3
VERSION: 5.0.3
VERSION: 5.04
VERSION: 5.1
VERSION: 5.04
VERSION: 5.1
VERSION: 4.1
VERSION: 5.2
VERSION: 4.1
VERSION: 4.1
VERSION: 5.1
VERSION: 4.1
VERSION: 4.1
VERSION: 4.2
VERSION: 5.1
VERSION: 5.1
VERSION: 4.1
VERSION: 4.1
VERSION: 4.1
VERSION: 5.2
VERSION: 5.2
VERSION: 4.1.1
VERSION: 4.1.1
VERSION: 4.1.1
VERSION: 4.1.1
VERSION: 4.1.1
VERSION: 4.1.1
VERSION: 4.2
VERSION: 4.2
VERSION: 4.3
VERSION: 4.3
VERSION: 4.3
VERSION: 4.3
VERSION: 4.3
VERSION: 4.3
VERSION: 4.3
VERSION: 4.3
VERSION: 5
VERSION: 4.3
VERSION: 4.3
VERSION: 5
VERSION: 5
VERSION: 5.0.3
VERSION: 5.0.3
VERSION: 5.04
VERSION: 5.0.3
VERSION: 5.04

Trellix

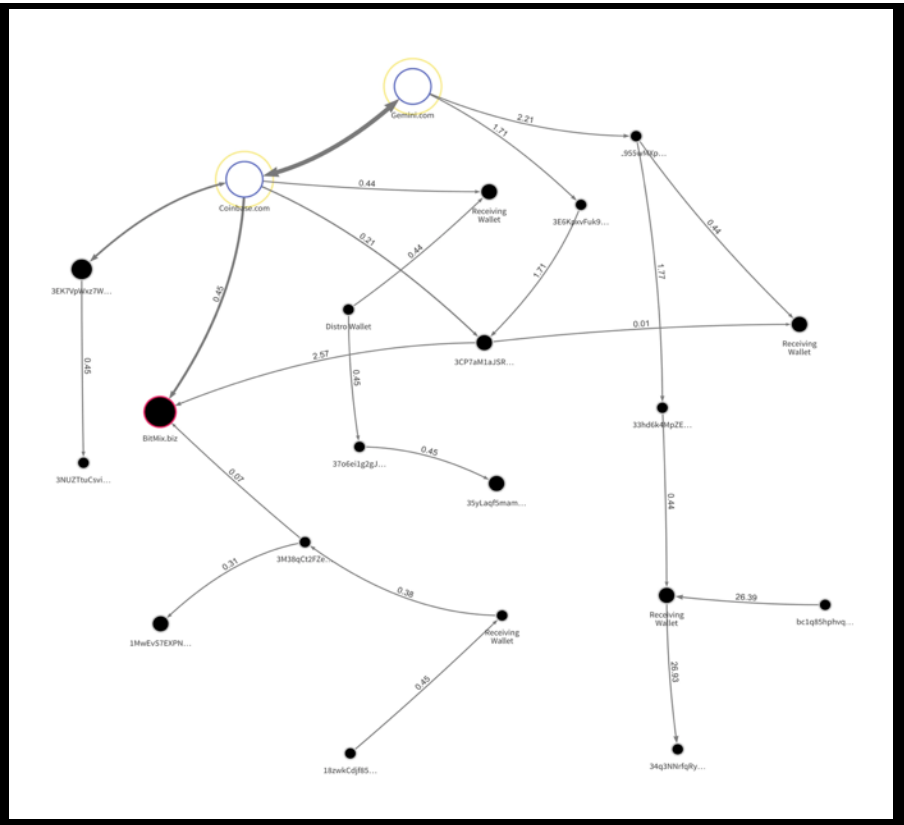
# But... Stay Humble

## The downfall of REvil



# Bragging

| Date | TXID | Bot | Status | Amount |
|---|---|---|---|---|
| 7 hours ago | 048c100a3bd9ed6a9a5d90791a78290d4a1367880415d2c069... | [redacted] | ✓ | 0.43707153<br>3988.98 USD |
| 11 hours ago | 16cd37ba2ab29973c202bbeab6dea3a9a1e9d0bf69a46952ec7... | [redacted] | ✓ | 26.38798971<br>240143.00 USD |
| 12 hours ago | 278dfb8f03f49f892bd2fbf17fd3dcf54fee33d32d580acb2c2856... | [redacted] | ✓ | 0.44554645<br>4084.89 USD |
| 12 hours ago | 26584ef98f78beac075f0f3d11bf88ee601b71cd9aabf9dcb4d0d... | [redacted] | ✓ | 0.44322399<br>4064.02 USD |
| 12 hours ago | 0b85c5b69e4b210b42a96eefec07f6f62559b9eaf0c0287659c4... | [redacted] | ✓ | 0.44238799<br>4053.80 USD |
| 12 hours ago | 74fcaa7c5b6f5ebdd83d2c962c16325c65e43292f68b4a429a46... | [redacted] | ✓ | 0.44189143<br>4050.42 USD |
| 12 hours ago | 91480ae15884f9b56f5fb83f26b016cefeb5302133504fcbb2145... | [redacted] | ✓ | 0.43909627<br>4018.53 USD |
| 2 days ago | d569cef16b5e7f142dcae523a51d3a08074790053a630ff6d606... | [redacted] | ✓ | 1.71205268<br>15102.40 USD |
| 2 days ago | 5d97529a3a09a0a888156877357c63e4a3a0c72c1205a92998e... | [redacted] | ✓ | 0.45300601<br>3984.26 USD |
| 2 days ago | fce34caa6506d5f02166d8006814f7f7ca11dd3d1fde41b0b1f78... | [redacted] | ✓ | 0.45414266<br>4009.63 USD |




**Lalartu made 300K USD in one weekend**

Trellix

# “Mo Money Mo Problems”

**Notorious B.I.G. 1997**

**Even for Cyber Criminals…**

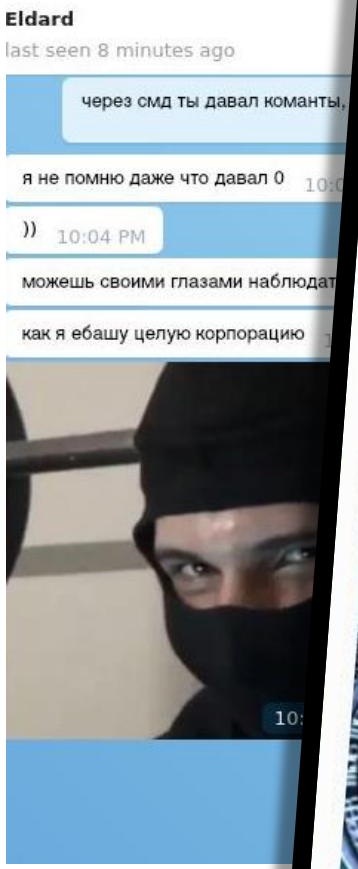


Trellix


INFORMANT

# Snitches get stitches… or not?

Lalartu exp

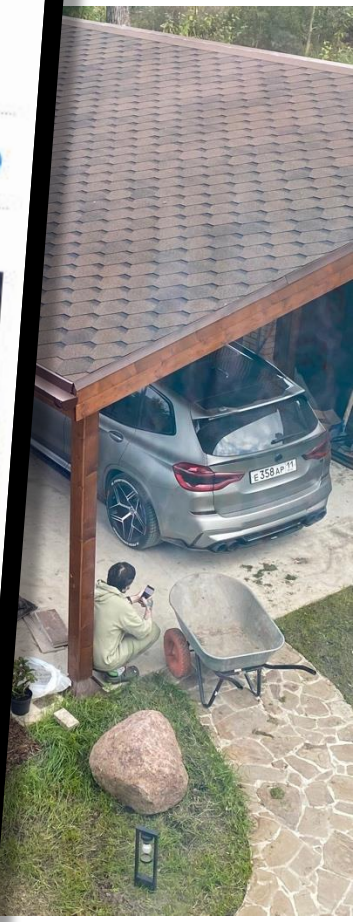



**FBI seized $2.3M from affiliate of REvil, Gandcrab ransomware gangs**

By Lawrence Abrams

November 30, 2021 04:46 PM 0



Trellix

FILTERS | Bot regist | Ran | From: 13 Dec, 2019 To: 13 I

| Info | Sub account | Price | Last visit | Bot reg ↓ |
|---|---|---|---|---|
| F3018F6AC886AAD2<br>US 71.78 | waxXxXx | $6,500 | -- | a few seconds ago |
| EDEB12EC08725E2E<br>US 216.59. | waxXxXx | $6,500 | -- | a few seconds ago |
| 3C5B0ED23ECFA541<br>US 68. | waxXxXx | $6,500 | -- | a minute ago |
| 7146E02E22BD6C77<br>US 108. | waxXxXx | $6,500 | -- | a minute ago |
| 00F1CA8AFA582968<br>US 98.6 | waxXxXx | $6,500 | -- | a minute ago |
| 5A3D863116190E37<br>US 70.58 | waxXxXx | $6,500 | -- | 5 minutes ago |

## 8D34D09DEC106C2E CHA

### Base Information

1.6
Bot Version

United States 104.6
GEO

Friday, 13 December 18:24 (9 minutes ago)
Registration date

njevsm16
Extension

0
Visits

lalartu (33) / waxXxXx (2231)
User / SubAccount

Windows 10 Enterprise / 64bit
OS / Bit

en-US / no
Language / Ru?

**A53001555AEDCE85**
I uploaded. the universal decrypto...
support

**5007957F86022CBA**
meant http://decryptor.top/42B1...
support

**BC913DFFA8A1438E**
Say him to find $100 more from hi...
support

**42B1CB1EB8B22EBC**
Ok, thank you for information.
support

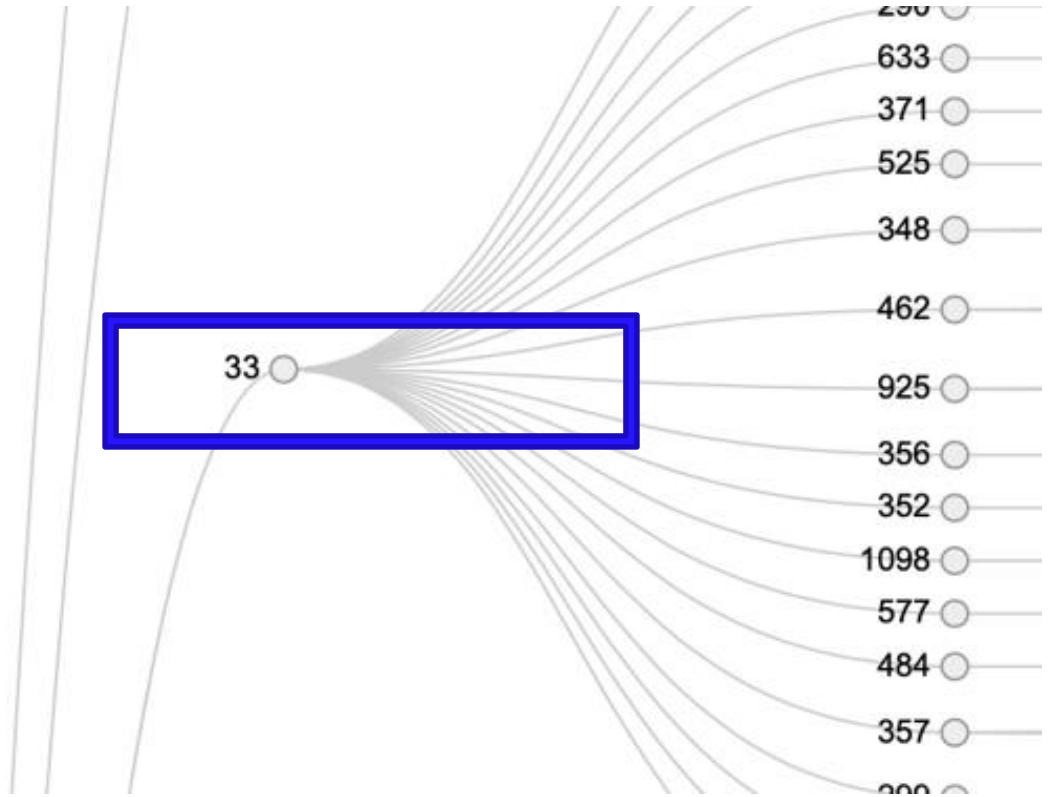
**49690BC634A9041A**
Thank you.
Data recovery: SLCUT

**5F99630E849394F8**
Thank you.
Data recovery: SLCUT

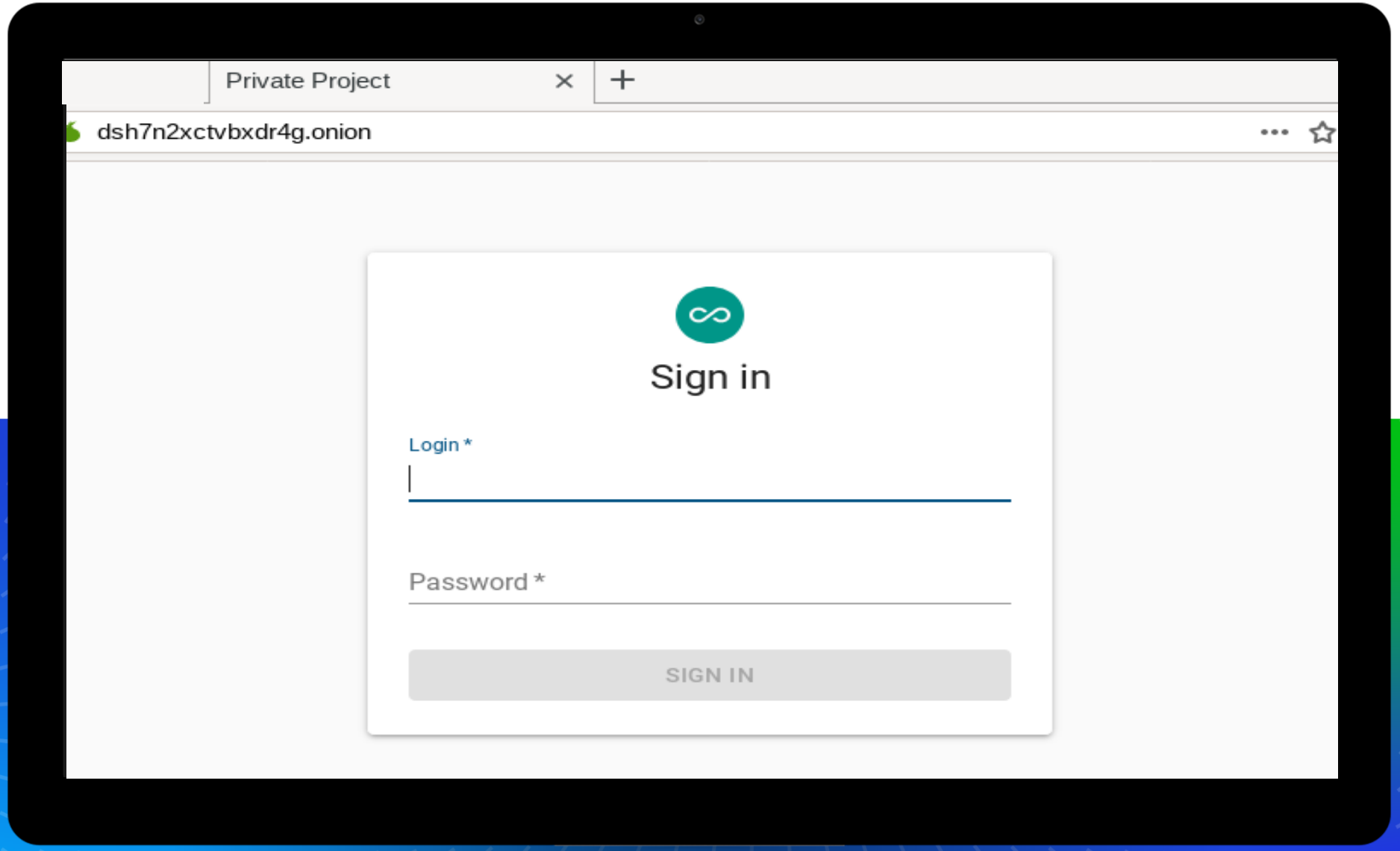
**66CC254A[illegible]7E7A60**
it is your decision. I will pass the ...
Victim

# Accounting is a double-edged sword…



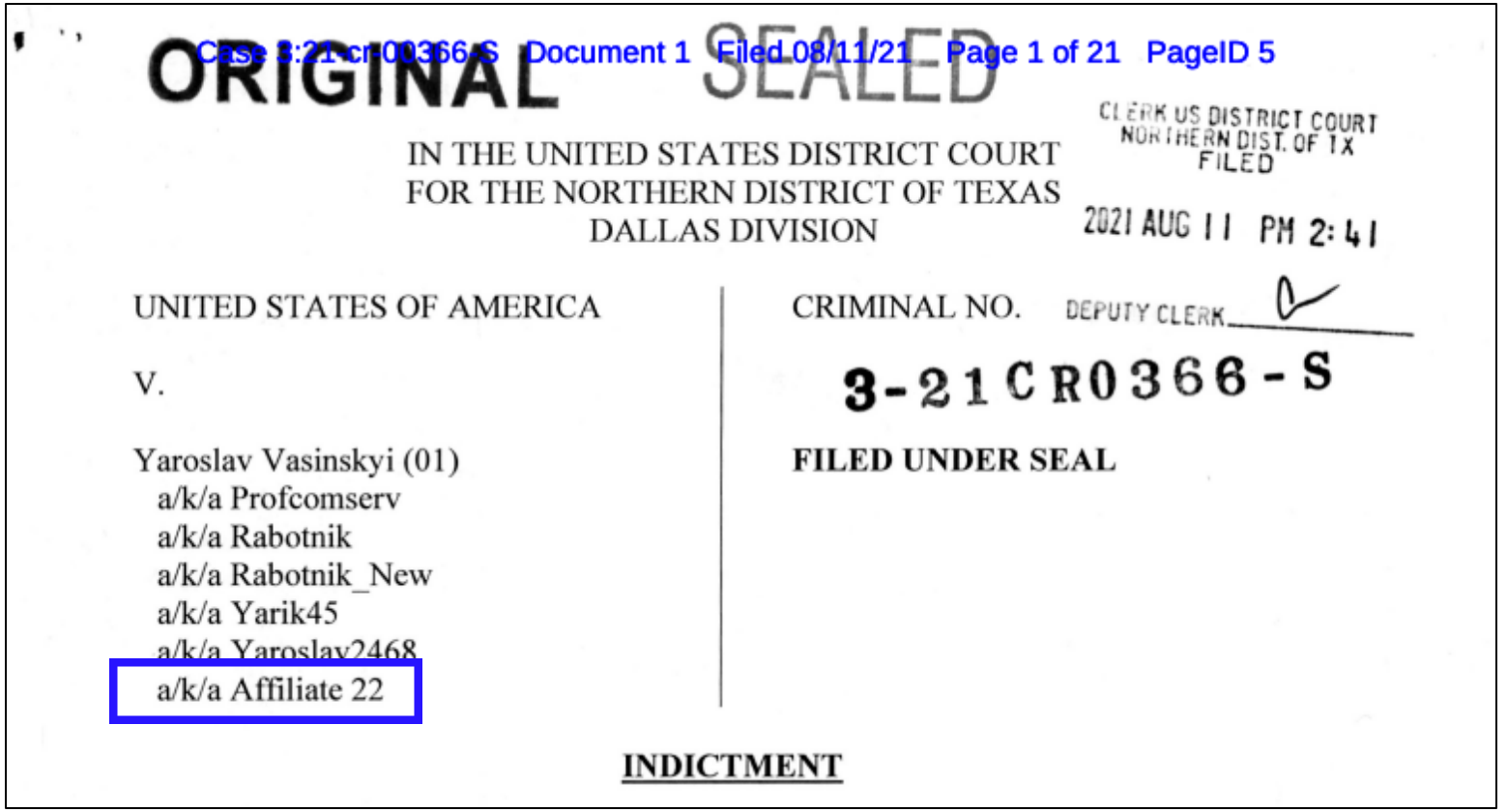




Trellix


Private Project
dsh7n2xctvbxdr4g.onion
Sign in
Login *
Password *
SIGN IN

Trellix

**Full Circle:** the ID nr 22 included on the indictment



Case 3:21-cr-00366-S Document 1 Filed 08/11/21 Page 1 of 21 PageID 5

ORIGINAL SEALED

CLERK US DISTRICT COURT
NORTHERN DIST. OF TX
FILED

2021 AUG 11 PM 2:41

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

DEPUTY CLERK

UNITED STATES OF AMERICA

V.

Yaroslav Vasinskyi (01)
a/k/a Profcomserv
a/k/a Rabotnik
a/k/a Rabotnik_New
a/k/a Yarik45
a/k/a Yaroslav2468
a/k/a Affiliate 22

CRIMINAL NO. 3-21CR0366-S

**FILED UNDER SEAL**

**INDICTMENT**

Trellix

# Breaking His Silence

**Person in Custody: VASINSKYI, YAROSLAV**

C

**CorrLinks <info@corrlinks.com>**

**To:** Jon DiMaggio

Friday, February 7, 2025 at 16:52

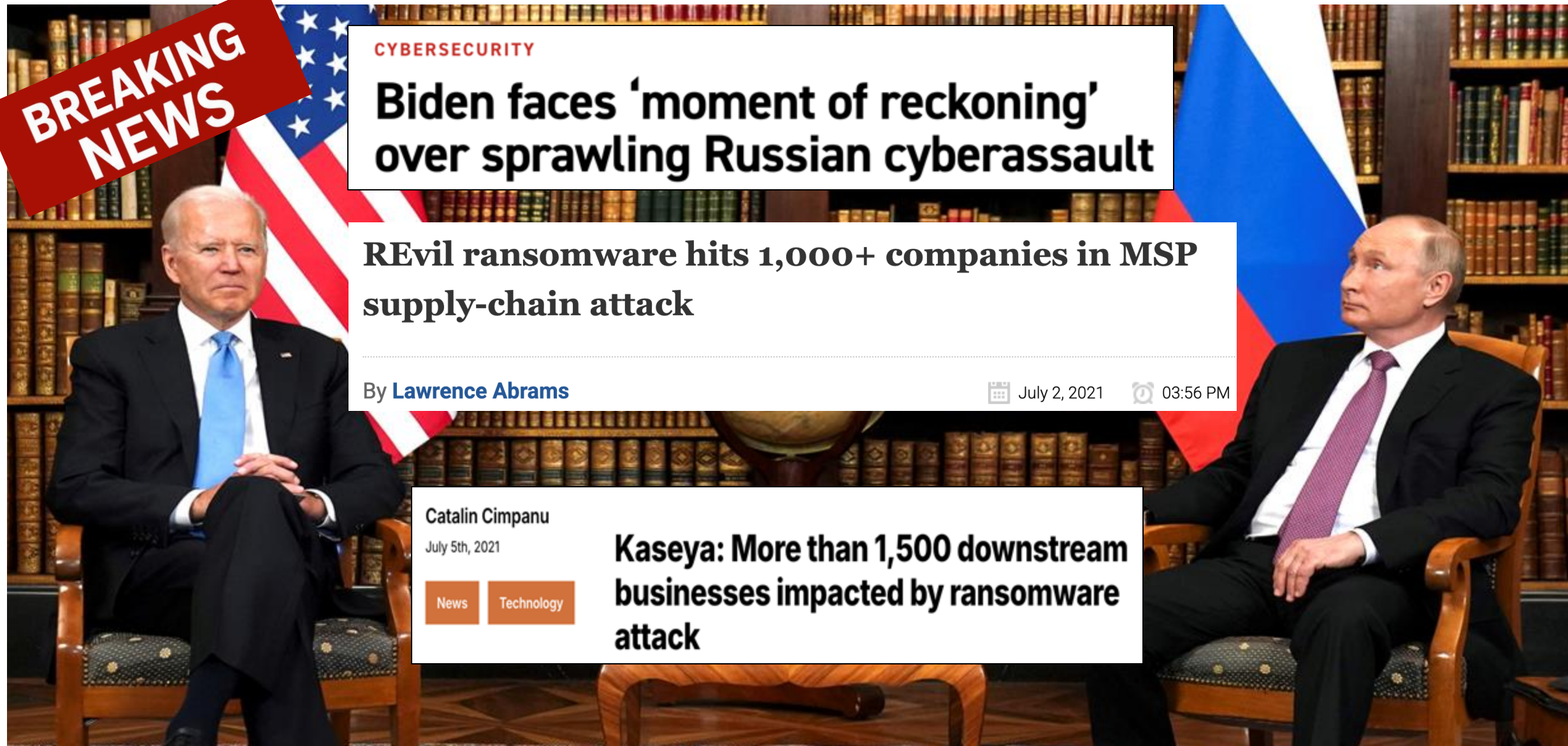
**External Sender** - From: ("CorrLinks" <info@corrlinks.com>)

This message came from outside your organization.

Learn More

This is a system generated message informing you that the above-named person is a federal person in custody who seeks to add you to his/her contact list for exchanging electronic messages.  There is no message from the person in custody at this time.

# What We Know About the Attack



# Attack Roles & Responsibilities










ANALYST1

Trellix

# “The Meeting”

## QTOX Meeting – 2 Days Before Attack

Unprecedented high-level coordination meeting – "they never made a chat like that that before"

| UNKN | "Trump" | "0_neday" | "1_zeroday" | "Rabotnik" |
|---|---|---|---|---|
| (Tearn Leader) | (Head of Support) | (Coder) | (Exploit Provider) | (Vasinskyi) |

**Division of Labor:** REvil provides clean manual build → Vasinskyi prepares attack → "Old friends" execute



1. **Antivirus Evasion**
   REvil command manually cleaned the executable file (exe) from antivirus detection systems
2. **File Disguise**
   Re-encoded the executable into a certificate format to avoid detection
3. **MSP Delivery**
   Certificate was delivered to the Managed Service Provider through the compromised Kaseya platform
4. **Endpoint Distribution**
   Certificate copied from MSP to endpoint devices with random bytes added to make the file's MD5 hash unique, reducing antivirus detection
5. **Payload Activation**
   Certificate decoded back into executable format on the endpoint device and ransomware deployed
6. **Evidence Cleanup**
   Logs and operation history were systematically cleaned to remove traces
7. **Final Deletion**
   Operation was completely deleted from the MSP database to eliminate forensic evidence

ANALYST1

# The Hand-off




**“Yes, the REvil team had partners who were associated with (Russian) government authorities. “**

**“I wrote to my "old friends"— here are the instructions, log in here, run the command, or find someone who will run it. I'm not going to do it”**

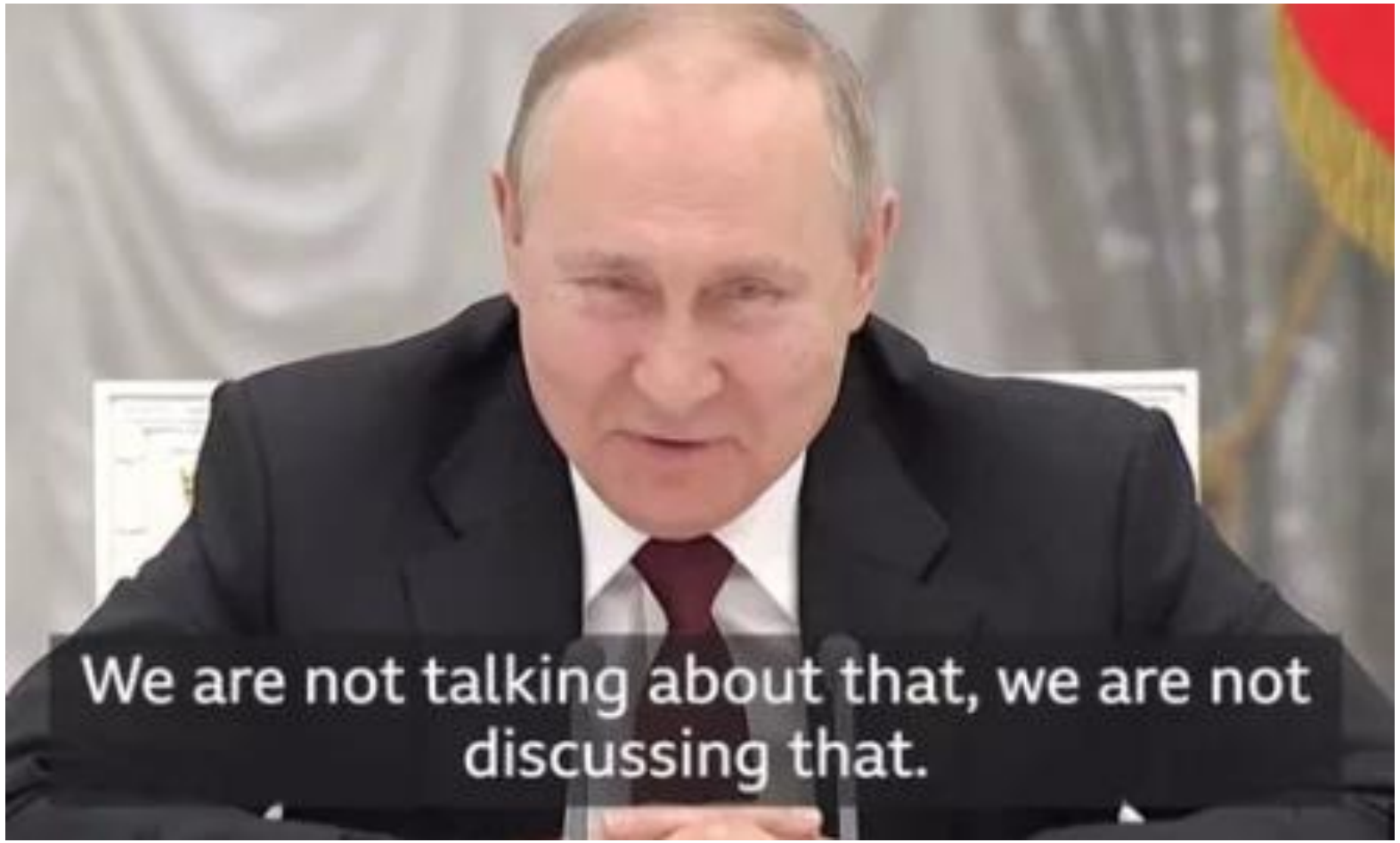
Trellix

# Attack Motivation

**Motive:** Disruption, crippling downstream systems, collecting intelligence, and gaining access to critic al infrastructure

# Visinkyi's Silence




ANALYST1

Trellix

# The Russian Connection

Trellix

ANALYST1

# Working for Russian Intelligence

"Before REvil... I had gotten to know people with ties to government authorities. During my work with the ransomware group, those connections deepened."

“I got requests from intelligence agencies (usually before elections), though I only realized this after the job was done.”



# The Job You Can't Quit







ANALYST1

Trellix

# Detained and Questioned in Ukraine







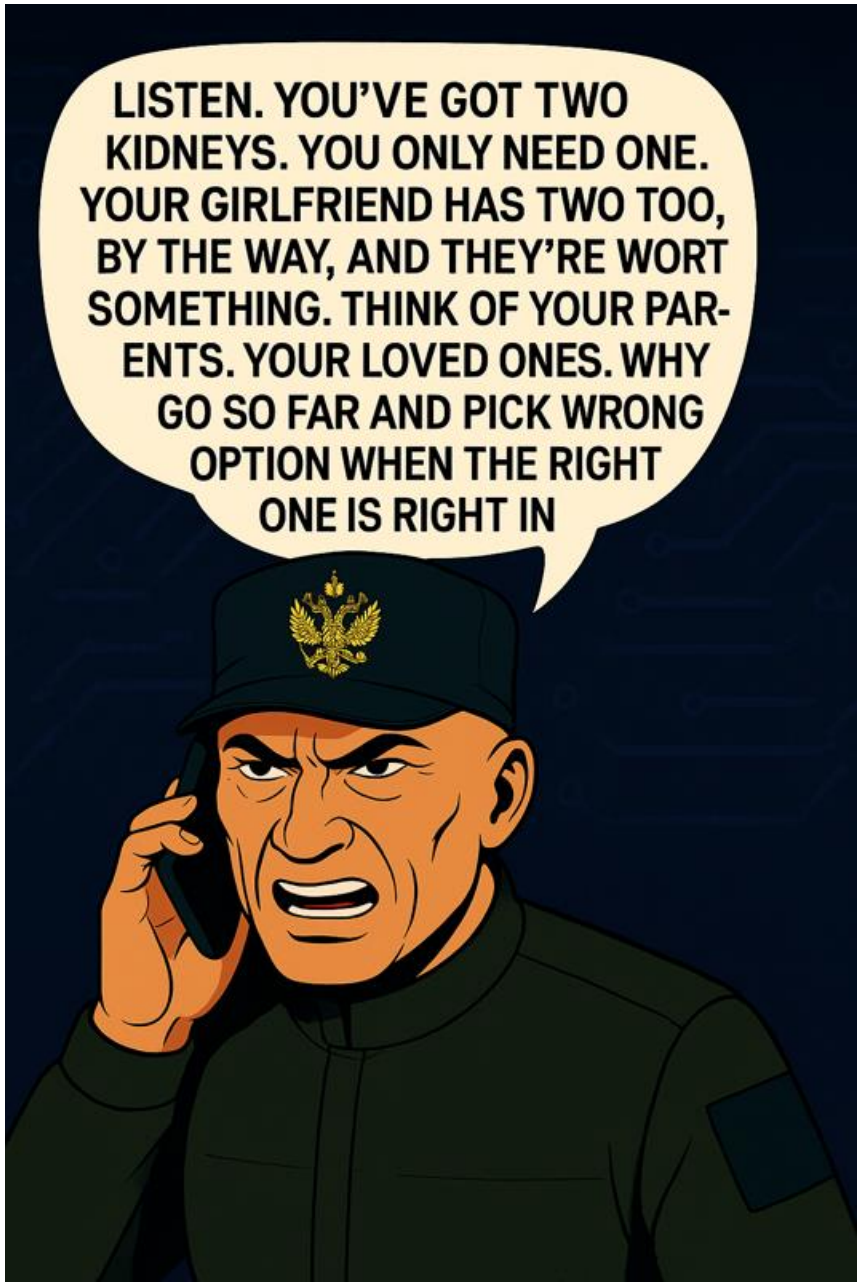
ANALYST1

Trellix










ANALYST1

Trellix

# Warning Email

2 days before the attack



# WHY DIDN'T HE TALK

Trellix

ANALYST1

# Arrest & Extradition






Trellix

# The Trophy & The Ghost



Vasinskyi's arrest and conviction was a big win for the DoJ

But there is still more work to do

**Are they even looking for REvil leadership? Appears not.**

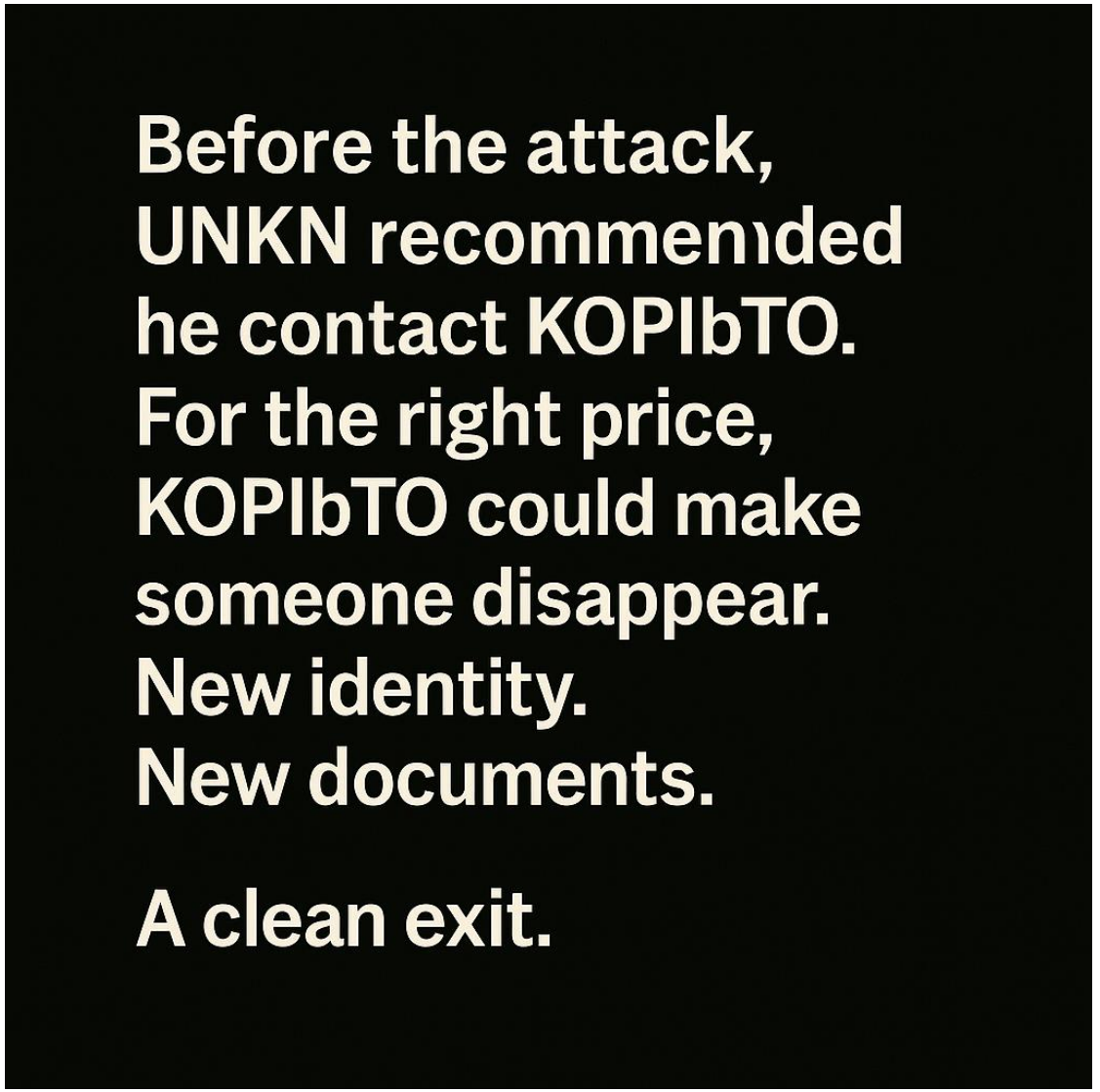
# HAVE YOU SEEN THIS MAN?!




UNKWN was only ever online during specific time zones, either UTC–6 or UTC+8. (If it's –6, it's likely Latin America; if +8, it could be Russia or Asia.) He also frequently took long-haul flights of about 6–8 hours. After his disappearance, a theory emerged. Trying to figure out what happened, such as flight dates, approximate departure and arrival times, I gathered information over the course of several months to try to match it with a real identity.

–Vasinskyi

# The Vanishing Act




Trellix

# Why Disappear?

UNKN didn’t just disappear; HE HAD TO. The $70 million ransom demand, posted publicly by REvil after the Kaseya attack, may have gone too far. Based on everything Vasinskyi told me, it clashed with the deeper purpose of the operation. This wasn’t supposed to be about extortion. It was about disruption: crippling downstream systems, collecting intelligence, and gaining access to critical infrastructure. Putting a price tag on that risked undermining all of it.

**People like this shouldn't get to disappear into the dark without consequence.**

Trellix

# The Silence After the Storm – What Comes Next

**Revil should not be forgotten. Criminals don’t disappear, they evolve**

**Law enforcement momentum changed priorities:** Initial global push didn’t evolve into lasting pressure.

**Ransomware is evolving underground**: Smaller, splintered crews now operate quietly, drawing from the same playbook.

**Without consequences, the model persists**: REvil’s legacy lives on—not as a name, but as a method.

**The real story didn’t end—it just stopped being told**.

Trellix

ANALYST1

# Q&A - Let's Talk About It

Trellix

ANALYST1