



# Open for Extortion: Upcoming Ransomware Evolutions and Revolutions

**Feike Hacquebord**  
Senior Threat Researcher  
Trend Micro Research

**FIRST Symposium, Bilbao 2023**





# Central Research Question 1

What will happen with Ransomware Business models in

- the near future
- the far future



# Central Research Question 2

What will *trigger* Ransomware Business models to change?

# THIS HIDDEN SITE HAS BEEN SEIZED




The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware.



This action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol

# Impact sanctions?



tomorrow  
belongs to those who embrace it  
today


trending innovation home & office business finance education security

/ innovation





Home / Innovation / Security

## Ransomware has gone down because sanctions against Russia are making life harder for attackers

NSA director of cybersecurity Rob Joyce says US sanctions on Russia are making it harder for criminals based in the country to conduct campaigns.



Written by **Danny Palmer**, Senior Writer on May 10, 2022

Source: <https://www.zdnet.com/article/ransomware-has-gone-down-because-sanctions-against-russia-are-making-life-harder-for-attackers/>



# Crypto Winter or Ice Age

Source: CNN

<https://edition.cnn.com/business/live-news/ftx-sam-bankman-fried/index.html>

6:31 p.m. ET, December 13, 2022

## FTX founder Samuel Bankman-Fried faces a maximum of 115 years in prison if convicted on all counts against him

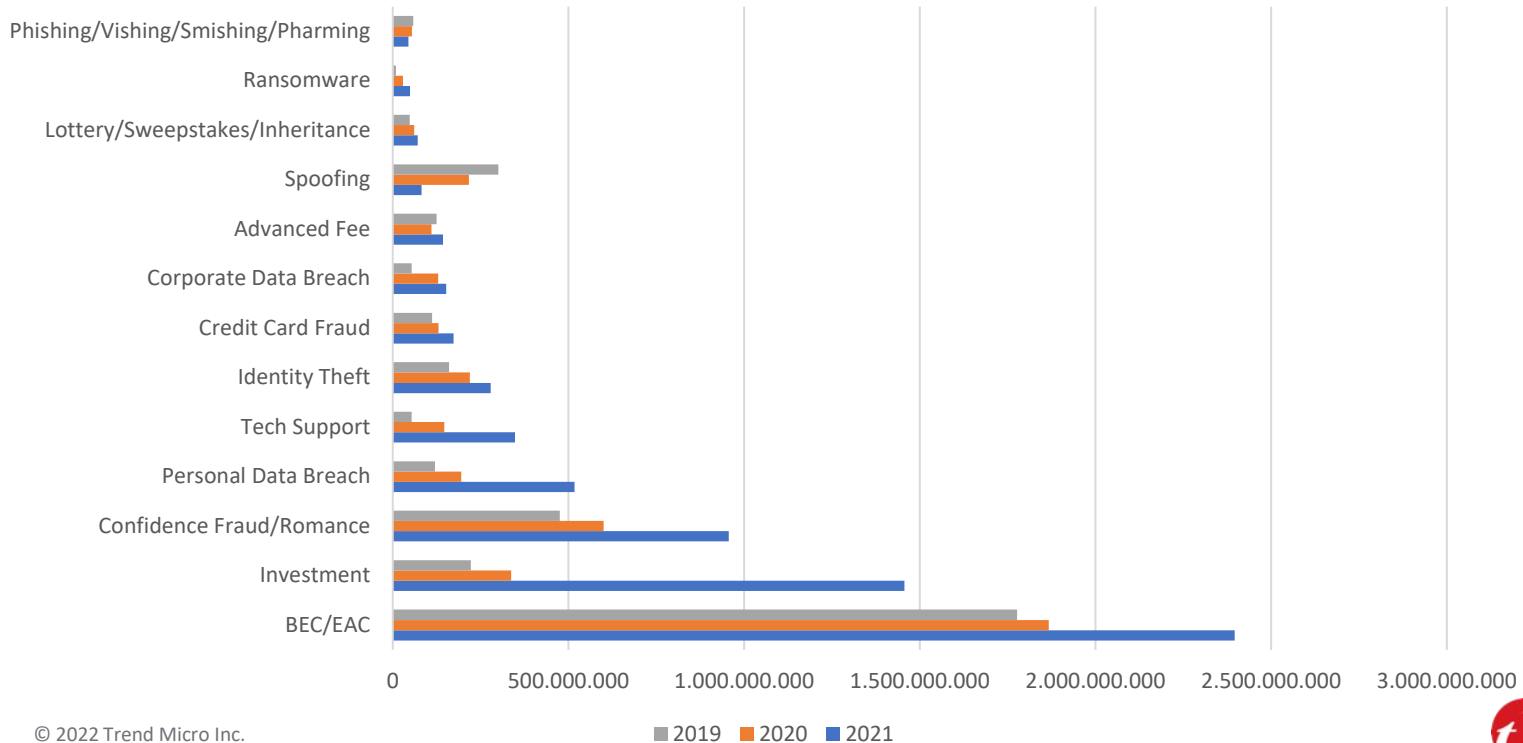
From Lauren del Valle and Kara Scannell



Sam Bankman-Fried is escorted out of the Magistrate Court building in Nassau, Bahamas December 13. (Dante Carrer/Reuters)

# Reported Victim Losses

Cybercrime. Victim Losses (source: FBI IC3)



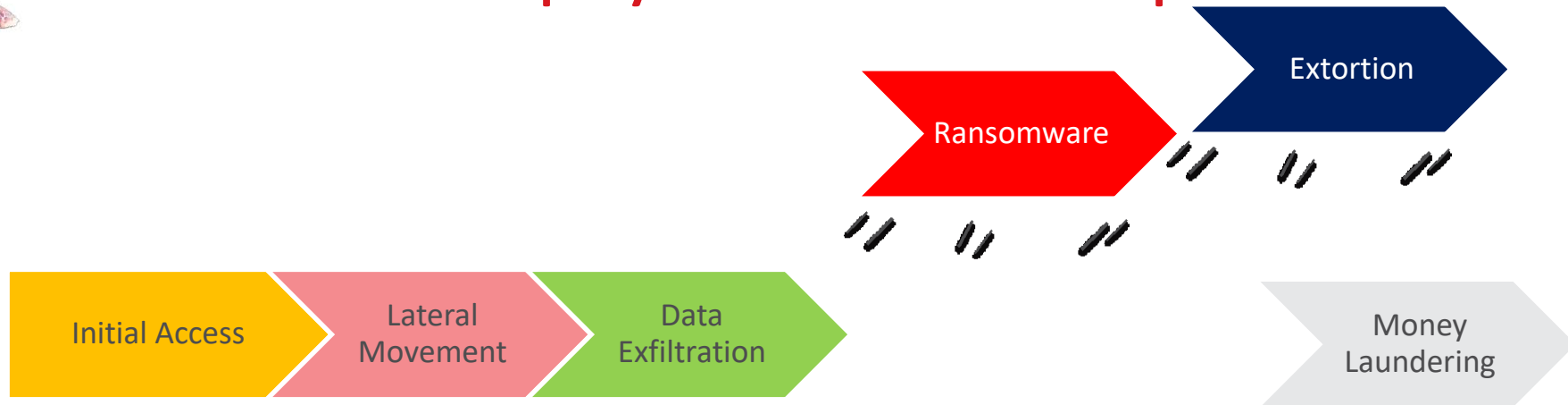




# Kill chain typical ransomware attack



# Ransomware payload can be replaced





# Extra Payload on top of ransomware





# Types of Ransomware Actors

Netwalker affiliate





# Types of Ransomware Actors

Netwalker affiliate

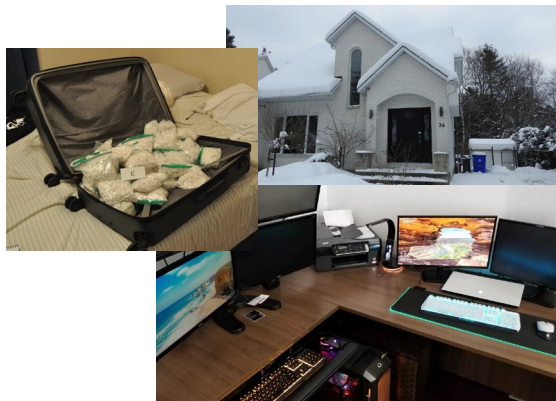


**HolyGhost**

We have been doing ransom for 8 years and did not publish or sell data which the user paid.  
So for 8 years, the people who is not related on us , never heard our group name.  
We help poor and starving people if we earn money.

# Types of Ransomware Actors

## Netwalker affiliate



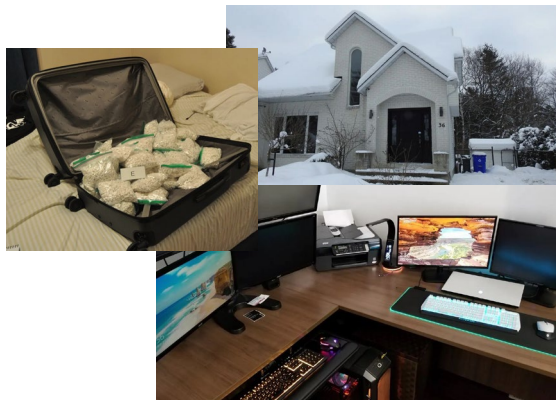
**HolyGhost**

We have been doing ransom for 8 years and did not publish or sell data which the user paid.  
So for 8 years, the people who is not related on us , never heard our group name.  
We help poor and starving people if we earn money.

Source: CBCNews <https://www.cbc.ca/newsinteractives/features/takedown-homegrown-ransomware-hacker>

# Types of Ransomware Actors

## Netwalker affiliate



**HolyGhost**

We have been doing ransom for 8 years and did not publish or sell data which the user paid.  
So for 8 years, the people who is not related on us , never heard our group name.  
We help poor and starving people if we earn money.

Source: CBCNews <https://www.cbc.ca/newsinteractives/features/takedown-homegrown-ransomware-hacker>



# Types of Ransomware Actors

Big Game Hunters

Nation state actors

Traditional Cybercriminals





# Triggers leading to Ransomware Evolution

- Arrests
- Sanctions
- Improved Actors' OpSec
- Automation of ransomware attacks
- Cloud adoption



# Triggers leading to Ransomware Revolution

- Cryptocurrency Regulations
- Geopolitical events
- More profitable cybercrime



# Impact of Arrests

- Impact of arrests has been limited so far
- Some arrests of affiliates
- Investigations seem to take forever
- Some new arrests to be expected
  
- But with all the focus on ransomware: *is that all there is?*

# Evolution Trigger: Sanctions

Date	Organization	Reason of OFAC designation
Dec. 29, 2016	Individual	Developer of Zeus malware
Dec. 29, 2016	Individual	Major data breaches
Nov. 28, 2018	Two individuals	SamSam ransomware
Sept. 13, 2019	Lazarus Group	WannaCry 2.0 ransomware, cryptocurrency hacks
Sept. 13, 2019	Bluenoroff	Attacks against financial institutions
Sept. 13, 2019	Andariel	ATM hacks, banking attacks
Dec. 5, 2019	Evil Corp	Development of Dridex malware
Dec. 5, 2019	17 individuals	Related to Evil Corp
Dec. 5, 2019	Six cooperations	Related to Evil Corp
Mar. 20, 2020	Two individuals	Assisted Lazarus Group with money laundering
Sept. 21, 2021	Suex OTC	Virtual currency exchange – Money laundering
Nov. 8, 2021	Chatex	Virtual currency exchange – Money laundering
Nov. 8, 2021	Three businesses	Related to Chatex
Apr. 5, 2022	Hydra market	Marketplace
May 6, 2022	Blender.io	Cryptocurrency mixer
Aug. 8, 2022	Tornado Cash	Cryptocurrency mixer



# How 2022's Biggest Cryptocurrency Sanctions Designations Affected Crypto Crime

JANUARY 9, 2023 | BY CHAINALYSIS TEAM



Source: <https://blog.chainalysis.com/reports/how-2022-crypto-sanction-designations-affected-crypto-crime/>



# Impact of Sanctions

- Sanctions are usually used as a political tool
- Impact will be limited [anybody remembers take down of Liberty Reserve – 2013?]
- Sanctions probably only increase costs for cyber criminals somewhat



# Remarks on OpSec

While RaaS actors are giving interviews to the journalists and brag about their crimes, their RaaS had been compromised for months....

-> RaaS are not immune to breaches

# Tor hidden servers exposing clear web IP

Nefilim

HolyGhost

AtomSilo

Ragnar

Onyx

Snatch

RansomExx

Arvin Club

Lorenz

Rook

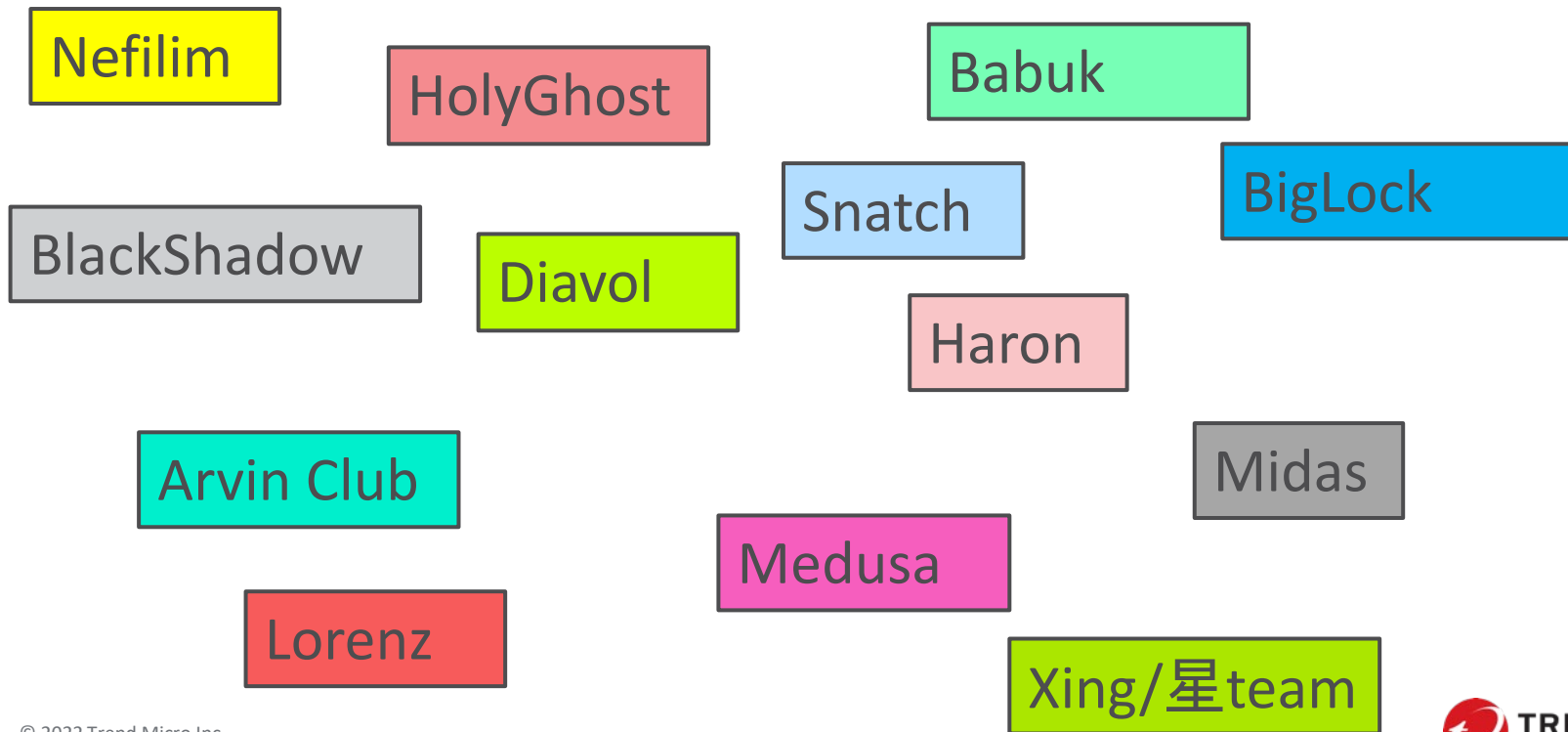
Marketo

Xing/星team





# RaaS with Server Status exposed





# Same SSH key.... for Nefilim

```
hxt254aygrsziejn.onion:22
```

```
78.128.x.y:22
```



# Serious breaches RaaS

- |                 |                                  |
|-----------------|----------------------------------|
| <b>REvil</b>    | - undisclosed LE agency          |
| <b>Hive</b>     | - FBI                            |
| <b>LockBit</b>  | - ProDaft                        |
| <b>Conti</b>    | - UA researcher, ProDaft, others |
| <b>Karakurt</b> | - Infitum                        |
| <b>PYSA</b>     | - ProDaft                        |
| <b>[.....]</b>  | - [.....]                        |

# Takedown No arrests

**THIS HIDDEN SITE HAS BEEN SEIZED**

## Hive

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against Hive Ransomware.

DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION

UNITED STATES  
CALIFORNIA STATE POLICE

EUROPOL

POLIZEI  
BADEN-WÜRTTEMBERG  
POLIZEIPRÄSIDIUM REUTLINGEN

FEDERAL CRIMINAL POLICE OFFICE  
BKA

Jonathan Greig  
January 26, 2023

Cybercrime Government  
Malware News

### 'We hacked the hackers:' DOJ, FBI take down Hive ransomware after spending months inside gang systems

Source: <https://therecord.media/we-hacked-the-hackers-doj-fbi-take-down-hive-ransomware-after-spending-months-inside-gang-systems/>



# More automation

2017

Cerber already  
used Blockchain  
for C&C

## Malware Coordination using the Blockchain: An Analysis of the Cerber Ransomware

Stijn Pletinckx\*, Cyril Trap\* and Christian Doerr  
TU Delft

Cyber Security Group  
2628CD Delft, The Netherlands

{S.R.G.Pletinckx@student., C.H.Trap@student., c.doerr}@tudelft.nl

**Abstract**—In order for malicious software to receive configuration information or commands, malware needs to be able to locate and connect to its owner. As hard-coded addresses are easy to block and thus render the malware installation inoperable, malware writers have turned to dynamically generated addresses. Domain generation algorithms (DGA) generate a list of candidate domain names, each valid for only a short time, at which the malware installation searches for its command & control (C&C) server. As DGAs generate a large list of potential domains – out of which one or a few is actually in use –, they leave a characteristic trace of many failed DNS lookups (NXDomain) in the network, and in result most DGAs can be efficiently detected.

In this paper we describe an entirely new principle of domain generation, actively deployed in the Cerber ransomware, which finds and coordinates with its owner based on transaction information in the bitcoin blockchain. This allows the malware author to dynamically update the location of the server in real-time, and as the malware directly goes to the right location no longer generates a sequence of NXDomain responses. We describe the concept of coordination via the blockchain, and report results on a year-long observation of the assets used in the Cerber campaign.

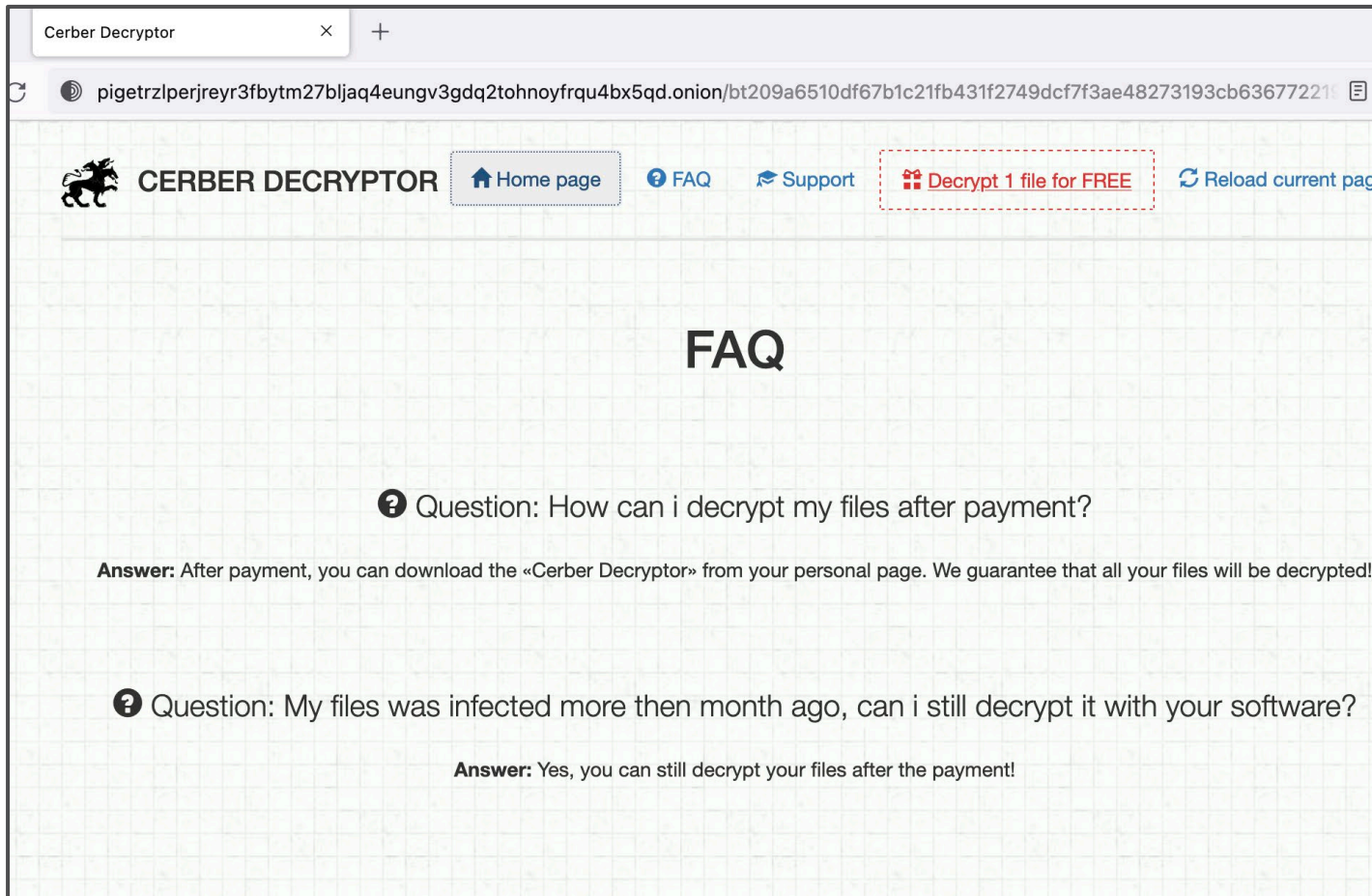
**Index Terms**—threat intelligence, blockchain, ransomware, C&C, domain-generation algorithm, campaign analysis

\*Both contributed equally to this work.

blacklisted or seized by law enforcement, although some m effort is required for this. Malware authors have hence evol to the dynamic generation of domain names, which are ea active for only a short amount of time, a principle referred as “domain fluxing”. For each time interval, a DGA produ a long list of candidate domain names at which the Ce server may be found, of which in practice only one or a t is actually registered. Each client will independently run DGA and in random order attempt to connect to the candida until the C&C server has been found. In order to complet break the control channel, the defender would thus have register all domain names valid for this time interval, wh is prohibitively expensive. In order to generate a predicta list, DGAs use the current time as random number se however some recent DGAs have evolved to include so public information such as the current trending topics fr Twitter [1] to make a prediction impossible.

This approach of coordinating malware however leave very characteristic trace in network traffic. As the candid lists are large and randomly probed, an infected client will geerate dozens or hundreds of lookups to non-existing domain

# Less interaction



The screenshot shows a web browser window with the title "Cerber Decryptor". The address bar contains a long URL. The website header includes a logo of a black horse, the text "CERBER DECRYPTOR", and navigation links: "Home page", "FAQ", "Support", "Decrypt 1 file for FREE" (highlighted with a red dashed border), and "Reload current page". The main content area is titled "FAQ" and contains two questions and answers.

**FAQ**

**?** Question: How can i decrypt my files after payment?

**Answer:** After payment, you can download the «Cerber Decryptor» from your personal page. We guarantee that all your files will be decrypted!

**?** Question: My files was infected more then month ago, can i still decrypt it with your software?

**Answer:** Yes, you can still decrypt your files after the payment!



# Cloud Adoption





# Impact of Cloud Adoption


- Cloud adoption will raise the bar for ransomware

BUT:

- Misconfigurations
- Theft of admin keys
- Vulnerabilities in Cloud (like no proper tenant separation)




# Critical Cloud vulnerabilities




Platform Use Cases Partners Research Resources About

BLOG RESEARCH POD

## Security Advisory: Insufficient Tenant Separation in Azure Synapse Service

 **Avi Shua** Published: May 09, 2022 Reading time: 7 Minutes


Source: <https://orca.security/resources/blog/synapse-critical-azure-synapse-analytics-service-vulnerability/>






Product Learn Company Blog Sign in Contact us

## AttachMe: critical OCI vulnerability allows unauthorized access to customer cloud storage volumes

Before it was patched, #AttachMe could have allowed attackers to access and modify any other users' OCI storage volumes without authorization, thereby violating cloud isolation. Upon disclosure, the vulnerability was fixed within hours by Oracle. No customer action was required.

 **Elad Gabay** September 20, 2022 8 min read

Source: <https://www.wiz.io/blog/chaosdb-explained-azures-cosmos-db-vulnerability-walkthrough/>



# Expected evolutions in ransomware

- Better OpSec
- More automation
- Less interaction with victims
- Move to targeting Cloud and Linux servers



# Triggers leading to Ransomware Revolution

- Cryptocurrency Regulations
- Geopolitical events
- More profitable cybercrime

# Cryptocurrency Regulations



Image: Trend Micro



# Crypto Winter or Ice Age

Source: CNN

<https://edition.cnn.com/business/live-news/ftx-sam-bankman-fried/index.html>

6:31 p.m. ET, December 13, 2022

## FTX founder Samuel Bankman-Fried faces a maximum of 115 years in prison if convicted on all counts against him

From Lauren del Valle and Kara Scannell



Sam Bankman-Fried is escorted out of the Magistrate Court building in Nassau, Bahamas December 13. (Dante Carrer/Reuters)



# Crypto Regulation

## Reasons for crypto regulation

- Protect investors and consumers
- Avoid ripple effects on financial markets
- Capital flight
  
- Money laundering



# FATF recommended Crypto regulations

## Recommendation #15

- VASPs\*) need to be regulated for anti-money laundering
- VASPs need to be licensed

## Recommendation #16 (Crypto Travel Rule)

- Info on payer and payee for transactions to be shared among CASPs\*\*)

\*) VASP: Virtual Asset Service Provider

\*\*\*) CASP: Crypto Asset Service Provider



# Crypto regulations – EU version

- MiCA legislation in EU
  - Stricter security rules on CASPs \*)
  - CASPs need authorization to operate in EU
- Crypto Travel Rule
  - Info on payer and payee for transactions
  - no threshold for payment





# Issues with regulations – worldwide

- low implementation of FATF recommendations
- different implementations between countries
  - threshold of travel rule differs
    - 0 in EU, 3000 USD in US
  - transfers to non-compliant CASPs: allowed / disallowed?
  - how about “unhosted” wallets?
- some countries are likely not to follow the FATF recommendations anytime soon



# Crypto regulations: impact on ransomware

- Potentially a huge impact
- But limited for the time being
- EU regulations expected to have the biggest impact (not before 2025).



# Geopolitical Events



# Geopolitical events

- Some RaaS might fall apart
- Some affiliates start to work for governments
- Initial access used for espionage / wiper attacks
- Usage of Ransomware as smokescreen



# Geopolitical events

October 14, 2022 • 8 min read

New “Prestige” ransomware impacts organizations in Ukraine and Poland

Microsoft Security Threat Intelligence

Microsoft MSTIC about Sandworm

THREAT ANALYSIS

## BRONZE STARLIGHT Ransomware Operations Use HUI Loader

THURSDAY, JUNE 23, 2022  
BY: COUNTER THREAT UNIT RESEARCH TEAM

SecureWorks: CN espionage smokescreen

THREAT ANALYSIS GROUP

## Initial access broker repurposing techniques in targeted attacks against Ukraine

Sep 07, 2022 • 5 min read



Pierre-Marc Bureau  
Threat Analysis Group

Share

Google TAG about Conti affiliate

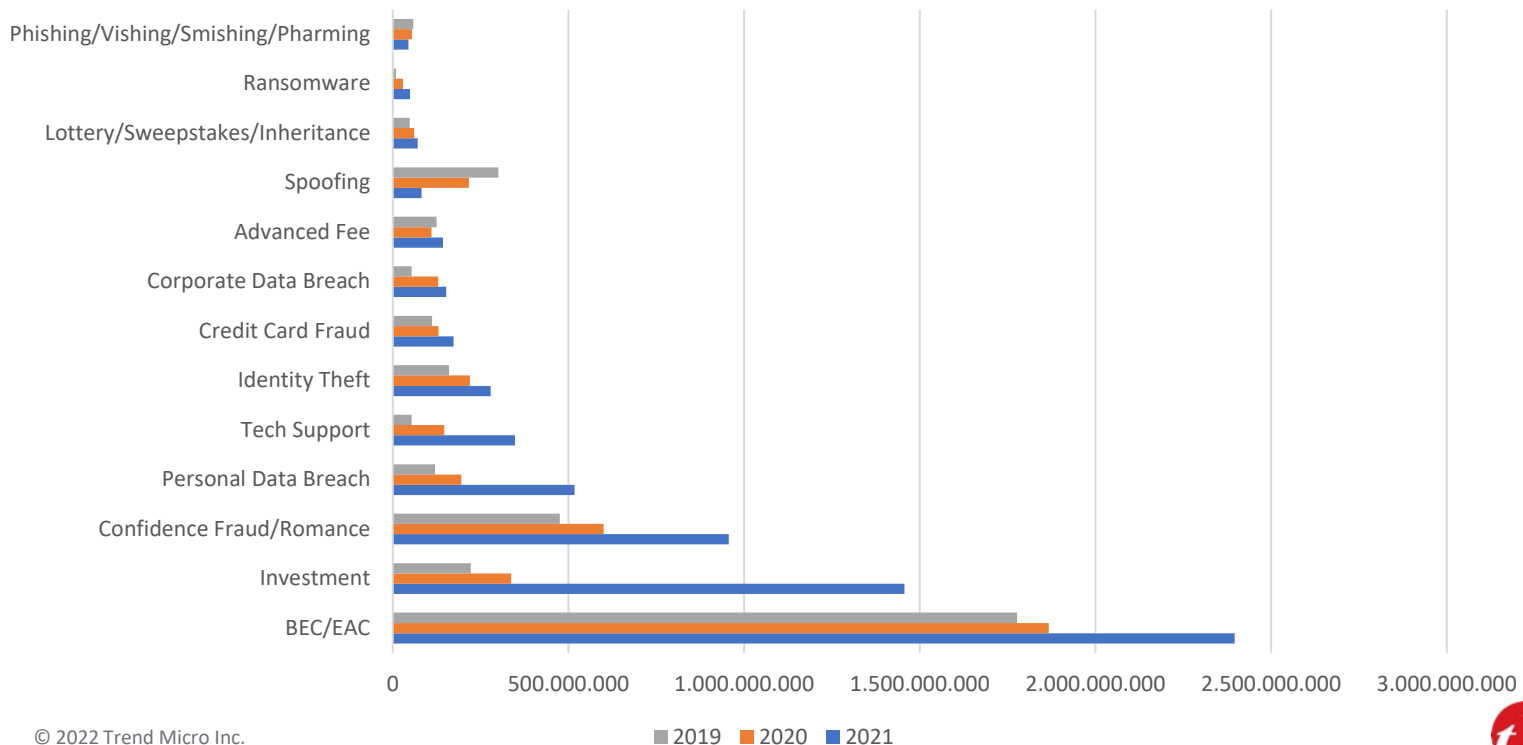


# More Profitable Cybercrime

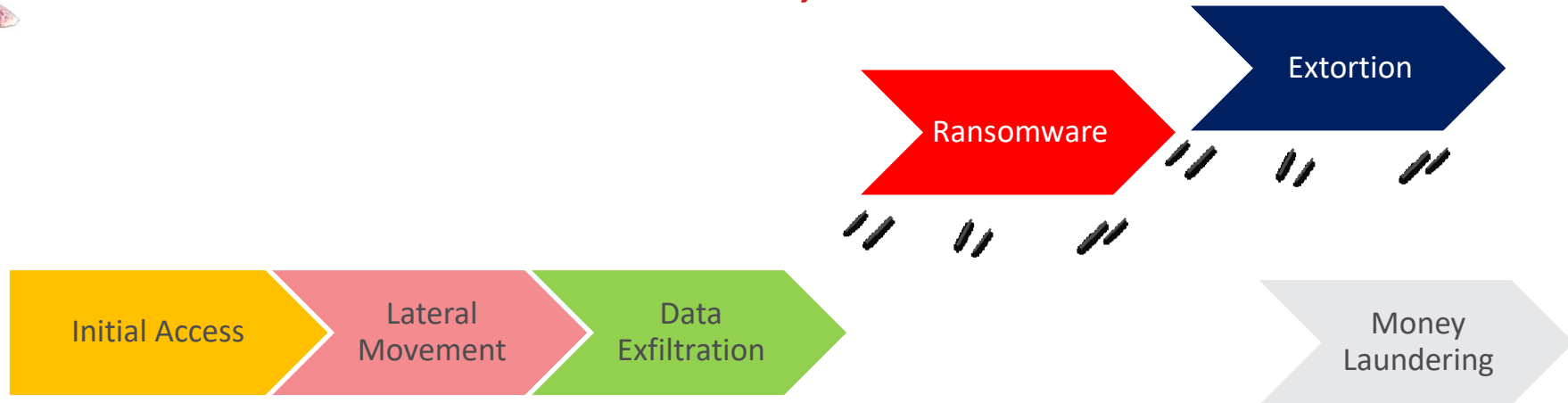


# Reported Victim Losses

Cybercrime. Victim Losses (source: FBI IC3)



# Remove ransomware, extortion







# Kill chain BEC attack





# Kill chain BEC attack

Abnormal

[Why Abnormal](#) / [Products](#) / [Solutions](#) / [Customers](#) / [Partners](#)

Resource Center

## Ransomware and BEC in the Cyber Threat Landscape: Past vs. Present, Perception vs. Reality

Colonial Pipeline. CNA Financial. Quanta. Even the NBA. Hardly a week goes by without a ransomware story hitting the news, as organizations worldwide are targeted by an attack. But are there more dangerous threats out there?

Webinars

Business Email Compromise

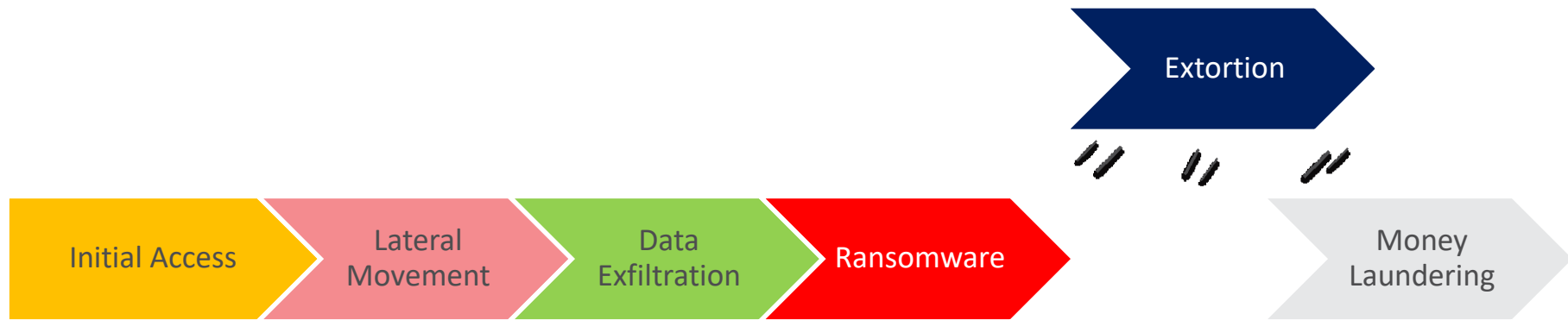
Ransomware



# Kill chain typical ransomware attack

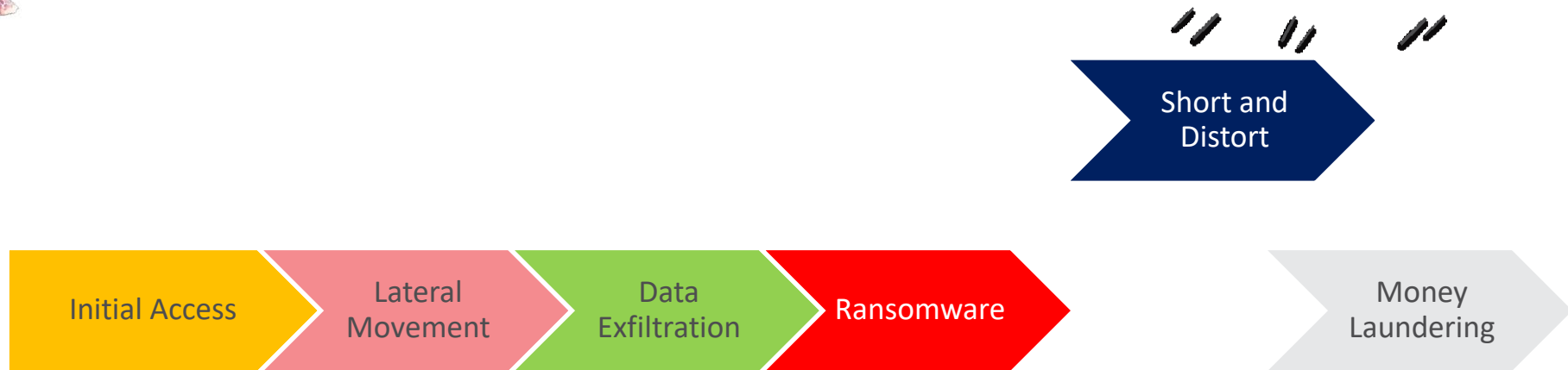


# Kill chain typical ransomware attack





# Kill chain typical ransomware attack





# Kill chain ransomware + short and distort



# Short and Distort

https://www.smh.com.au/business/markets/caught-in-a-bear-trap-how-short-and-distort-attacks-are- 80% Search

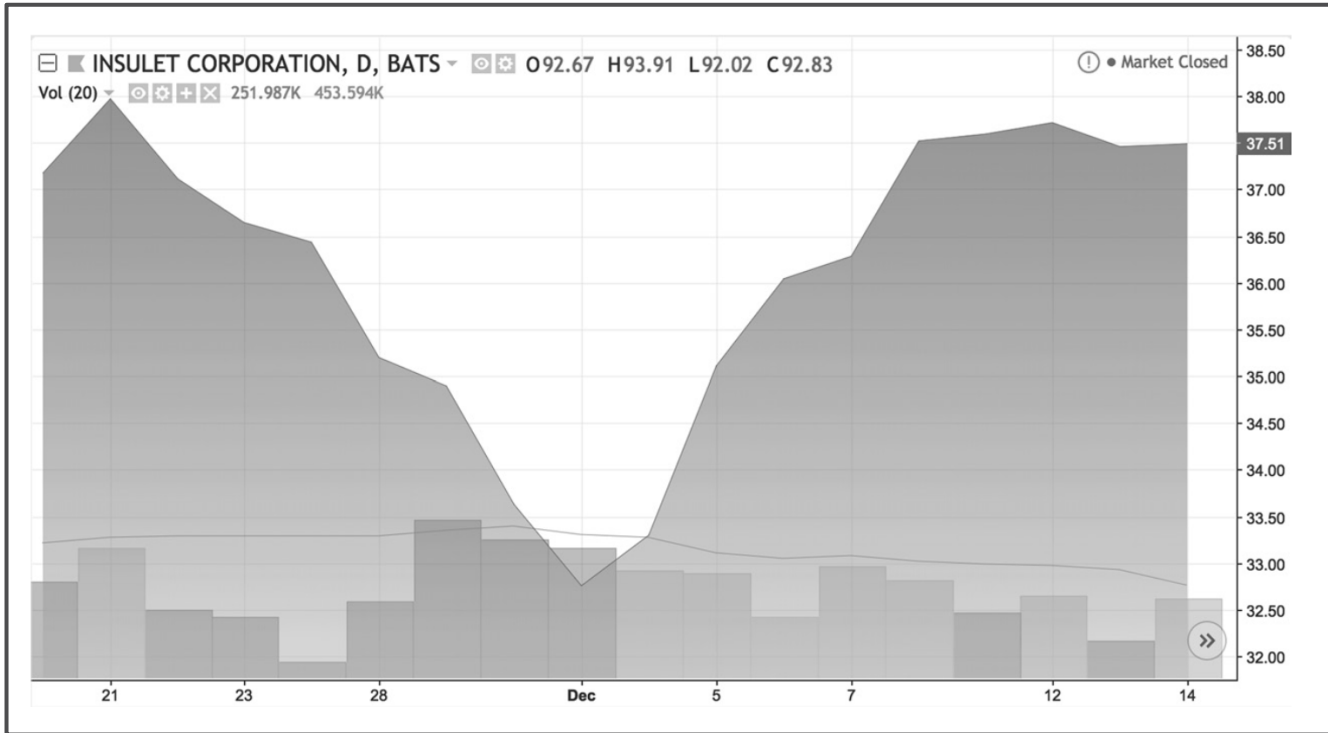
## Caught in a bear trap: How 'short and distort' attacks are costing Australian investors billions

Australia has become a paradise for a new, aggressive form of short selling. And regulators' failure to act is costing investors billions.

Adele Ferguson  
DECEMBER 7, 2020



# Example: Insulet Corporation



Source: Joshua Mitts. (2020). University of Chicago Press. "Short and Distort." The Journal of Legal Studies, Vol. 49, Issue no. 2, p. 287–334.



# Canon (Maze attack: Jul/Aug 2020)

- Initial drop 18%
- V-shape

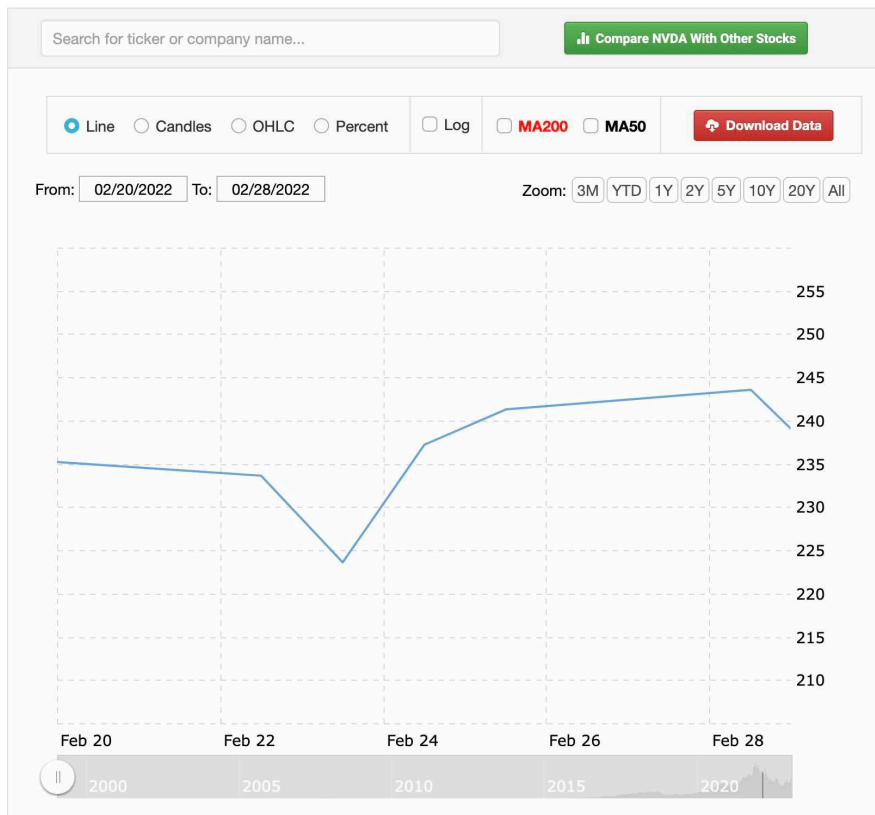


Source: macrotrends.net



# Nvidia (Lapsu\$ attack: Feb 2022)

- Drop 4%
- V-shape



Source: macrotrends.net



# Payloads that might replace ransomware

- Theft of intellectual property and other sensitive data
- Business Email Compromise
- Stocks manipulation schemes like short and distort
- Theft of cryptocurrencies at scale



# Advice 1

**XDR solutions will be increasingly important in the near and far future.**

Near Future: Ransomware will be optimized

Far Future: Ransomware will be replaced by other other profitable payloads. Emphasis on the left and middle of the kill chain is critical.



## Advice 2

**Advanced protection against Linux based cybercrime (server, cloud and IOT) will continue to rise in importance during the next 2 years and beyond.**



## Advice 3

**Tracking campaigns and actors is key for understanding how future threats will look like and see the way criminal business models, and the top tier groups themselves, are evolving.**



# Advice 4

**Collaboration between**

**LE**

**Certs**

**Governments**

**Law Makers**

**Private Industry**



# Further reading




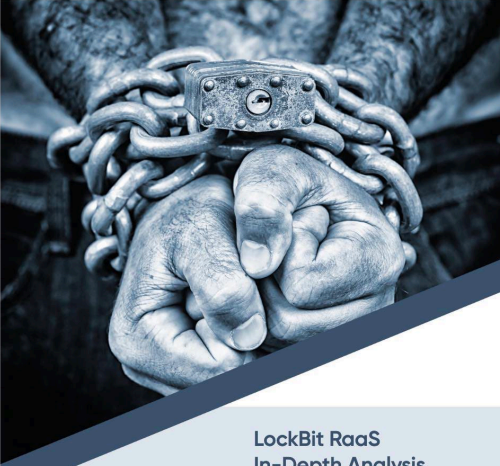
## The Near and Far Future of Ransomware Business Models

Feike Hacquebord, Stephen Hilt, and David Sancho






# Recommended reading

 PRODAFT  
PROACTIVE DEFENSE AGAINST FUTURE THREATS



**LockBit RaaS  
In-Depth Analysis**


 Y-Parc, rue Gallée 7, 1400 Yverdon-les-Bains, Switzerland  +41225481923  info@prodaft.com

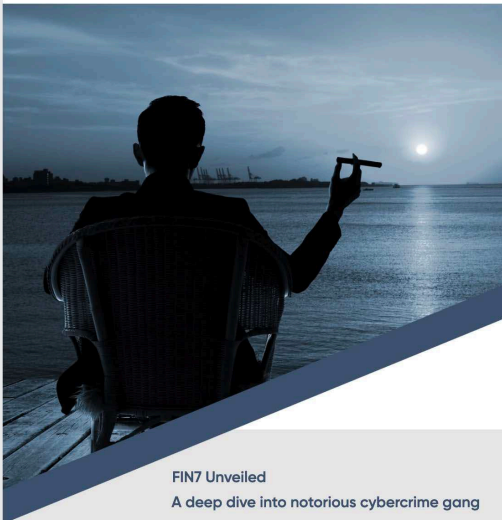
 PRODAFT  
PROACTIVE DEFENSE AGAINST FUTURE THREATS






**Wizard Spider  
In-Depth Analysis**

 Y-Parc, rue Gallée 7, 1400 Yverdon-les-Bains, Switzerland  +41225481923  info@prodaft.com

 PRODAFT  
PROACTIVE DEFENSE AGAINST FUTURE THREATS



**FIN7 Unveiled**  
A deep dive into notorious cybercrime gang

 Y-Parc, rue Gallée 7, 1400 Yverdon-les-Bains, Switzerland  +41225481923  info@prodaft.com



# Contact details

Twitter: @FeikeHacquebord

FeikeHacquebord@infosec.exchange



The Near and Far Future of  
Ransomware Business Models

Feike Hacquebord, Stephen Hilt, and David Sancho

An abstract digital artwork featuring a central white DNA double helix structure. The helix is surrounded by numerous colorful, textured spheres and teardrop shapes in shades of pink, purple, and blue, connected by thin black lines. The overall composition is dynamic and futuristic, set against a light gray background.

# THE ART OF CYBERSECURITY

Threat detection and response across multiple attack vectors by Trend Micro. Created with real data by artist **Brendan Dawes**.