CONINT

ncptf
national child protection task force

Using Cyber Threat Intelligence To Combat Ransomware

$~WHOAMI

Security Researcher

Cyber Threat Intelligence

Malware Analysis

OSINT

How to reach me:

@BushidoToken on Twitter

THE MANY HATS CLUB

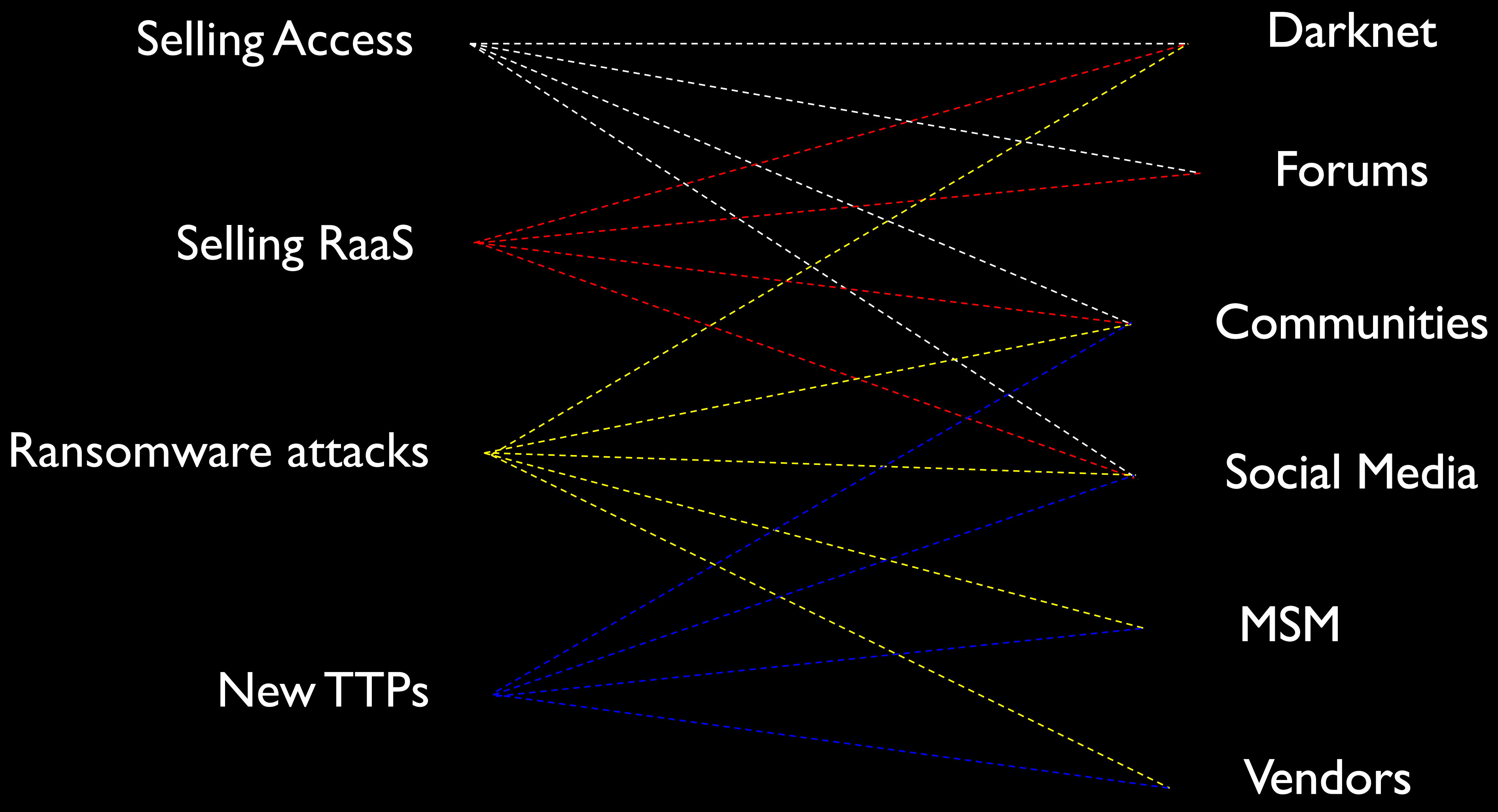
Moderator

The Ransomware Operator Starter Pack
SECURED BY SECTIGO
COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS
WANTED BY THE FBI

Paying 50k for a pentest
Paying 500k for a ransom

Give me my files back.
Give me $500 in Bitcoin.
@freeitdata

Gathering Intelligence on Ransomware



Selling Access

Selling RaaS

Ransomware attacks

New TTPs

Darknet

Forums

Communities

Social Media

MSM

Vendors

Collection – Analysis – Mitigation

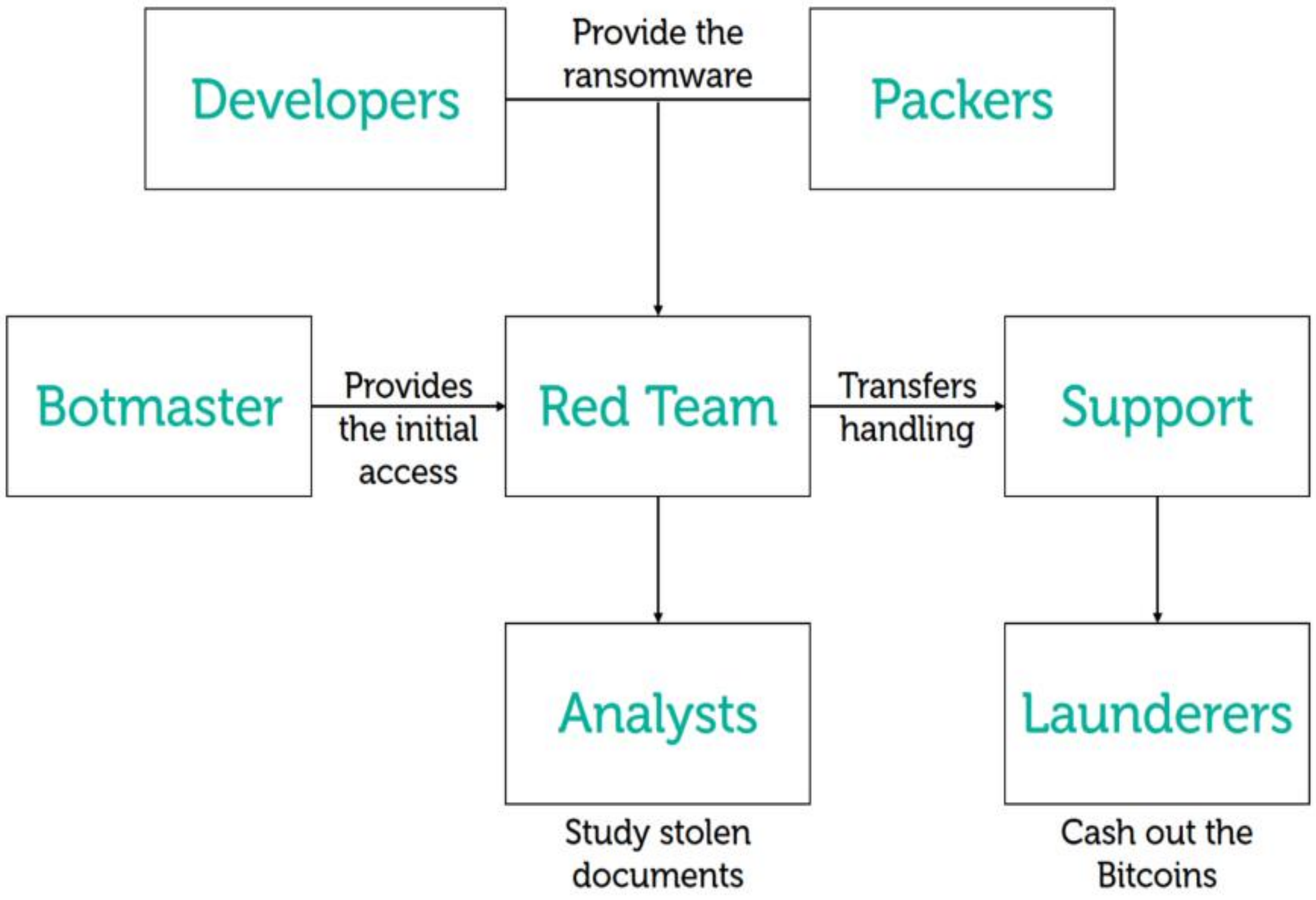
Ransomware:

- ∞ Encrypted Network and Files
- ∞ Denial of Service
- ∞ Data Destruction
- ∞ Ransom Payment Demands
- ∞ Stolen Data
- ∞ Darknet Leak Sites
- ∞ Access Brokers
- ∞ Data Brokers
- ∞ Exploit Brokers

Initial Access:

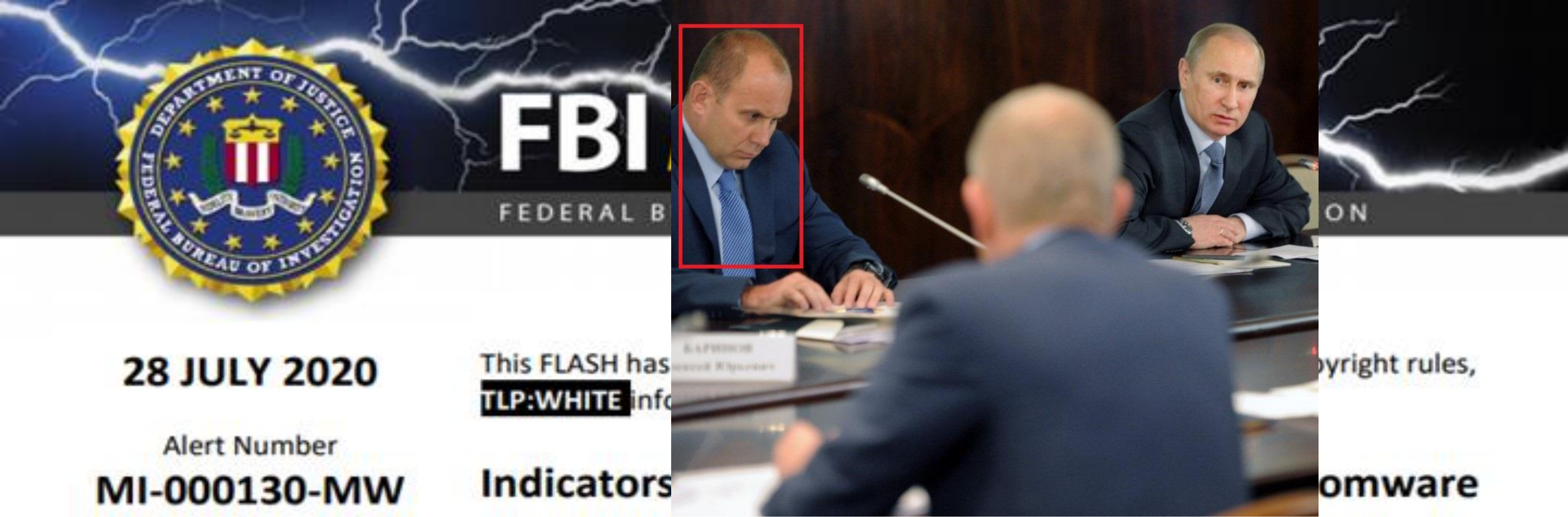
- ∞ RDP Brute Forcing / Stolen Creds
- ∞ Phishing ›› Malware ›› Ransomware
- ∞ Exploitation of Remote Services
- ∞ 0day vulnerability

Diagram to encapsulate clearly how some of the top-tier Ransomware-as-a-Service offerings may work:



Structure of the ransomware ecosystem

https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/



FBI

FEDERAL B ON

28 JULY 2020

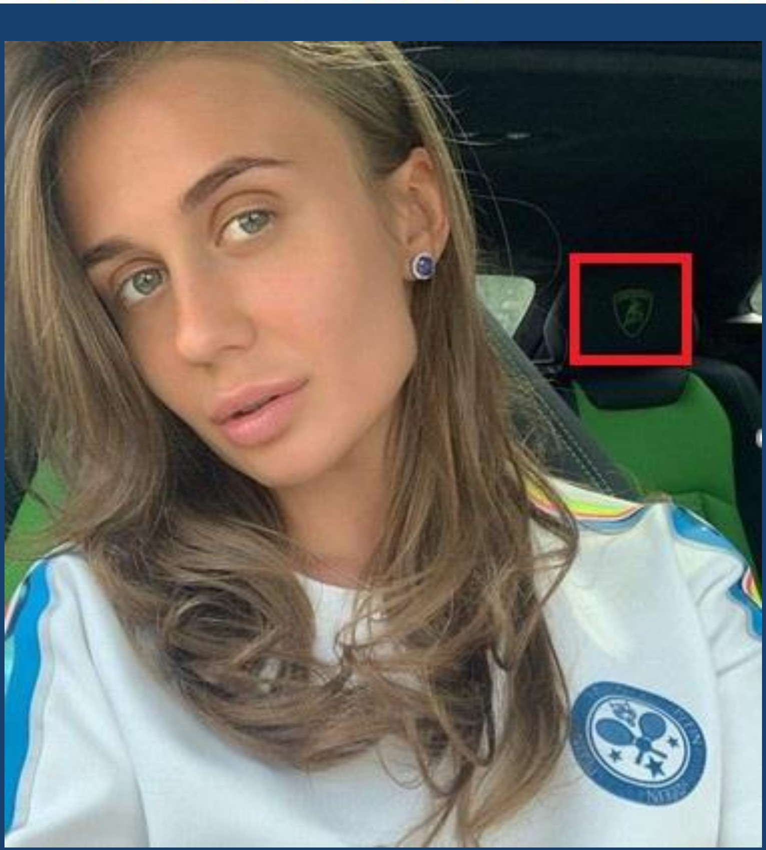
Alert Number

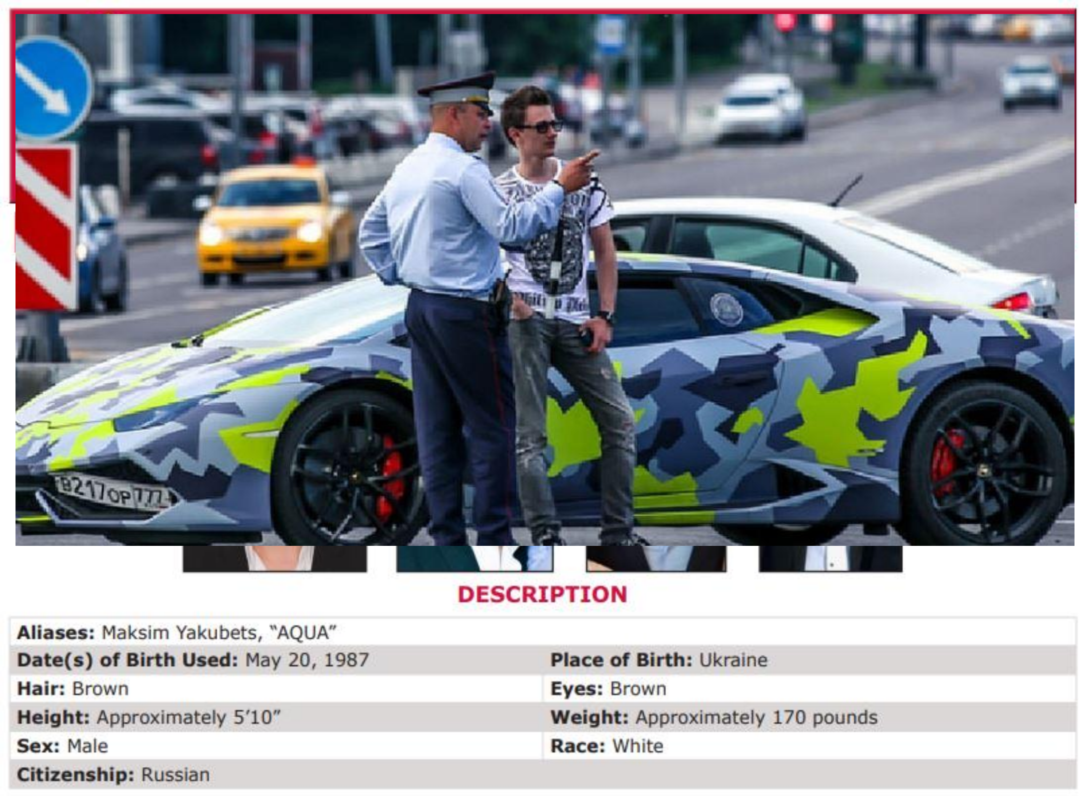
MI-000130-MW

This FLASH has yright rules,

TLP:WHITE inf

Indicators omware





DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

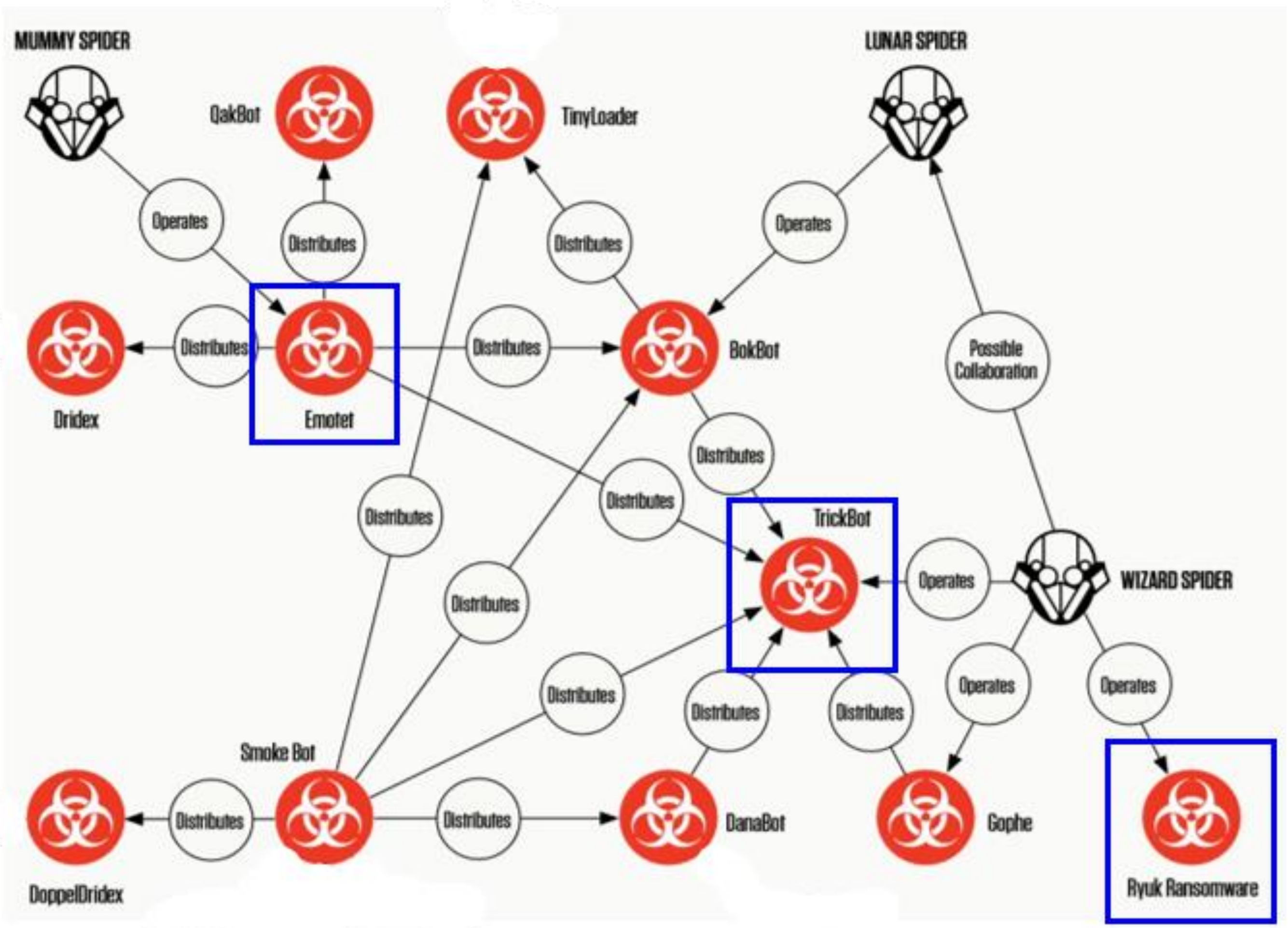
EvilCorp Indictment – December 2019

Ransomware operators:

eCrime groups:

∞ REvil, Ryuk, DoppelPaymer, Maze, RagnarLocker, NetWalker, WastedLocker, BitPaymer, Conti, Cl0p, DarkSide, Avaddon, Sekhmet, ProLock, Egregor, LockBit, Snatch, SunCrypt, MountLocker, and Dharma.

Connected through MaaS:



https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/

Additional attackers:

🇨🇳 ∞APT41 .: ColdLock

🇨🇳 ∞APT41 .: Freezing

🇰🇵 ∞Lazarus .: VHD

🇰🇵 ∞Lazarus .: WannaCry

🇷🇺 ∞Sandworm .: NotPetya

🇷🇺 ∞Sandworm .: BadRabbit

🇮🇷 ∞IRGC .: SamSam

🇮🇷 ∞IRGC .: Dharma

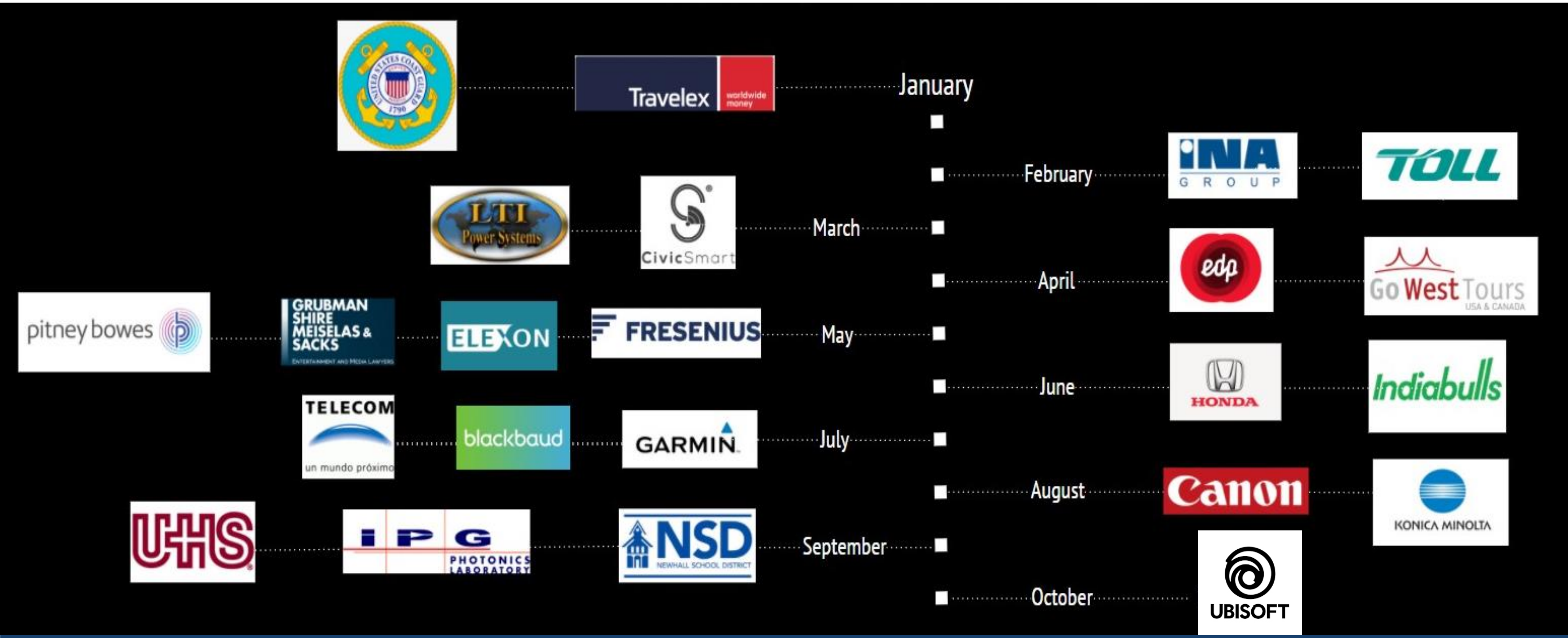
Targets ICS and SCADA:

∞MegaCortex

∞EKANS

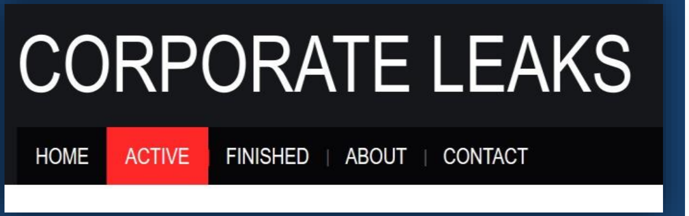
∞LockerGoga

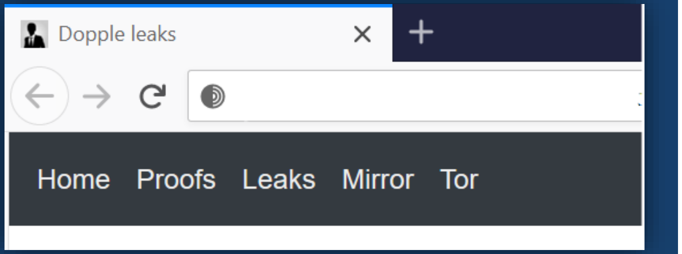
Largest Ransomware Attacks of Q1-Q3 2020

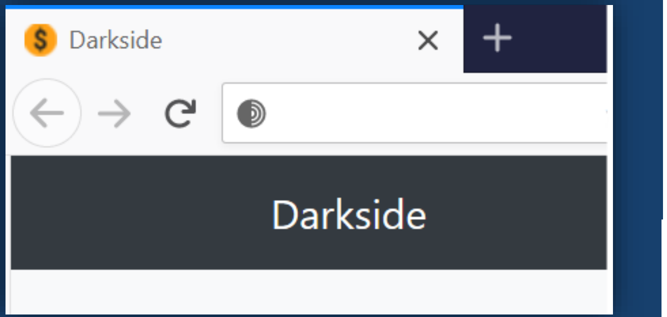


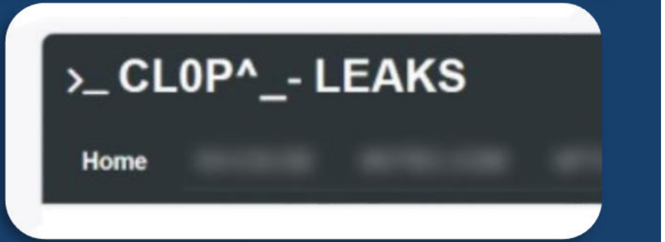
- ∞ Education
- ∞ Tourism
- ∞ Governments
- ∞ Transportation
- ∞ Financial Services
- ∞ Law Enforcement
- ∞ Hospitals
- ∞ Legal
- ∞ Manufacturing
- ∞ Technology
- ∞ Professional Services
- ∞ Energy

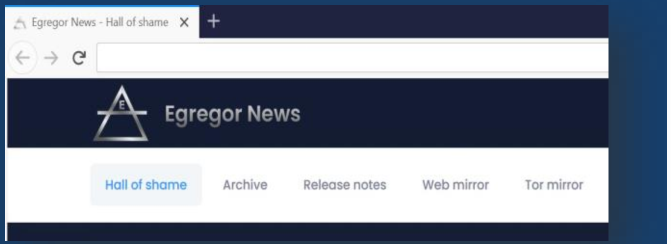
RaaS Leak Blogs:









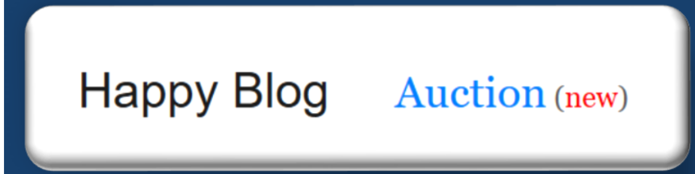


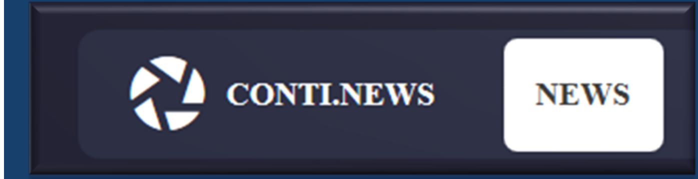
Maze Ransomware

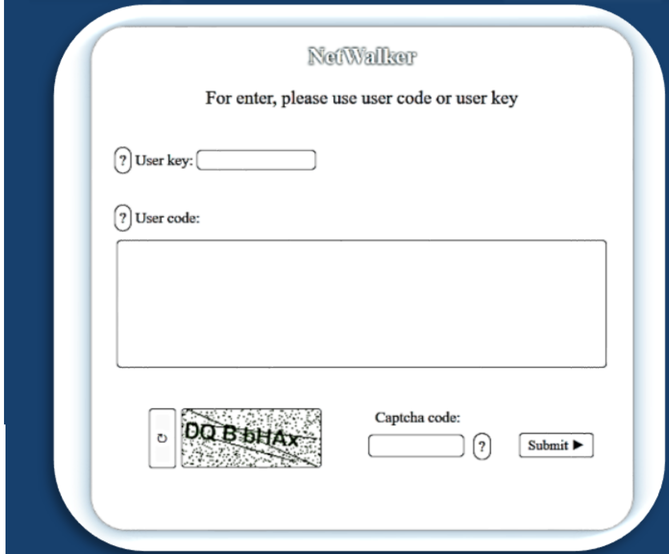
Home Page of Ragnar_Locker Leaks site
RAGNAR_LOCKER

AVADDON
RANSOMWARE

MOUNT LOCKER






NetWalker

For enter, please use user code or user key

Maze Ransomware

Canon

BRUNNER
a BRUNNERWORKS Co.

LG

orange™

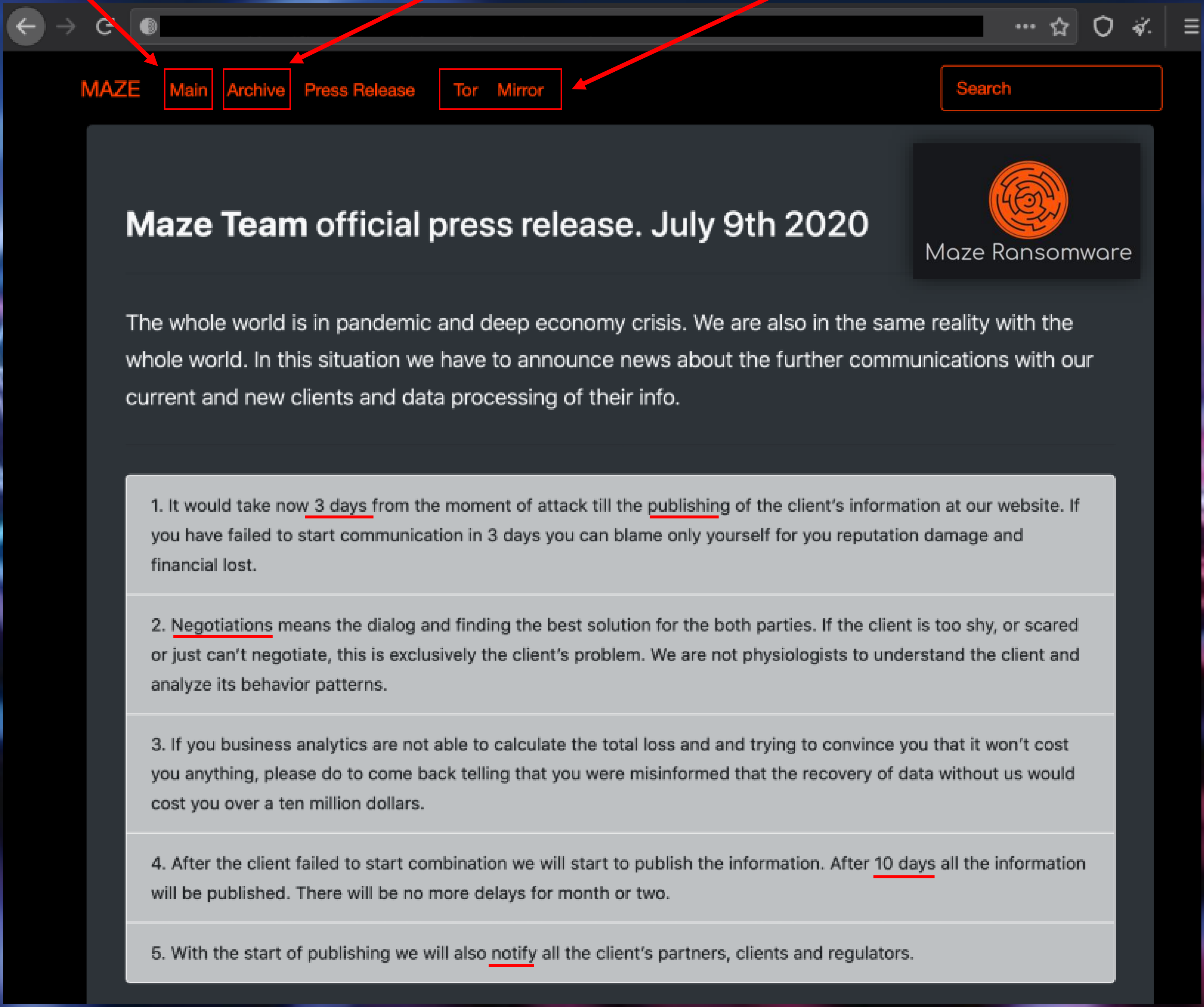
thyssenkrupp

xerox

Current Leaks

Previous Leaks

Duplicate Sites



Maze Team official press release. July 9th 2020

The whole world is in pandemic and deep economy crisis. We are also in the same reality with the whole world. In this situation we have to announce news about the further communications with our current and new clients and data processing of their info.

1. It would take now 3 days from the moment of attack till the publishing of the client's information at our website. If you have failed to start communication in 3 days you can blame only yourself for you reputation damage and financial lost.

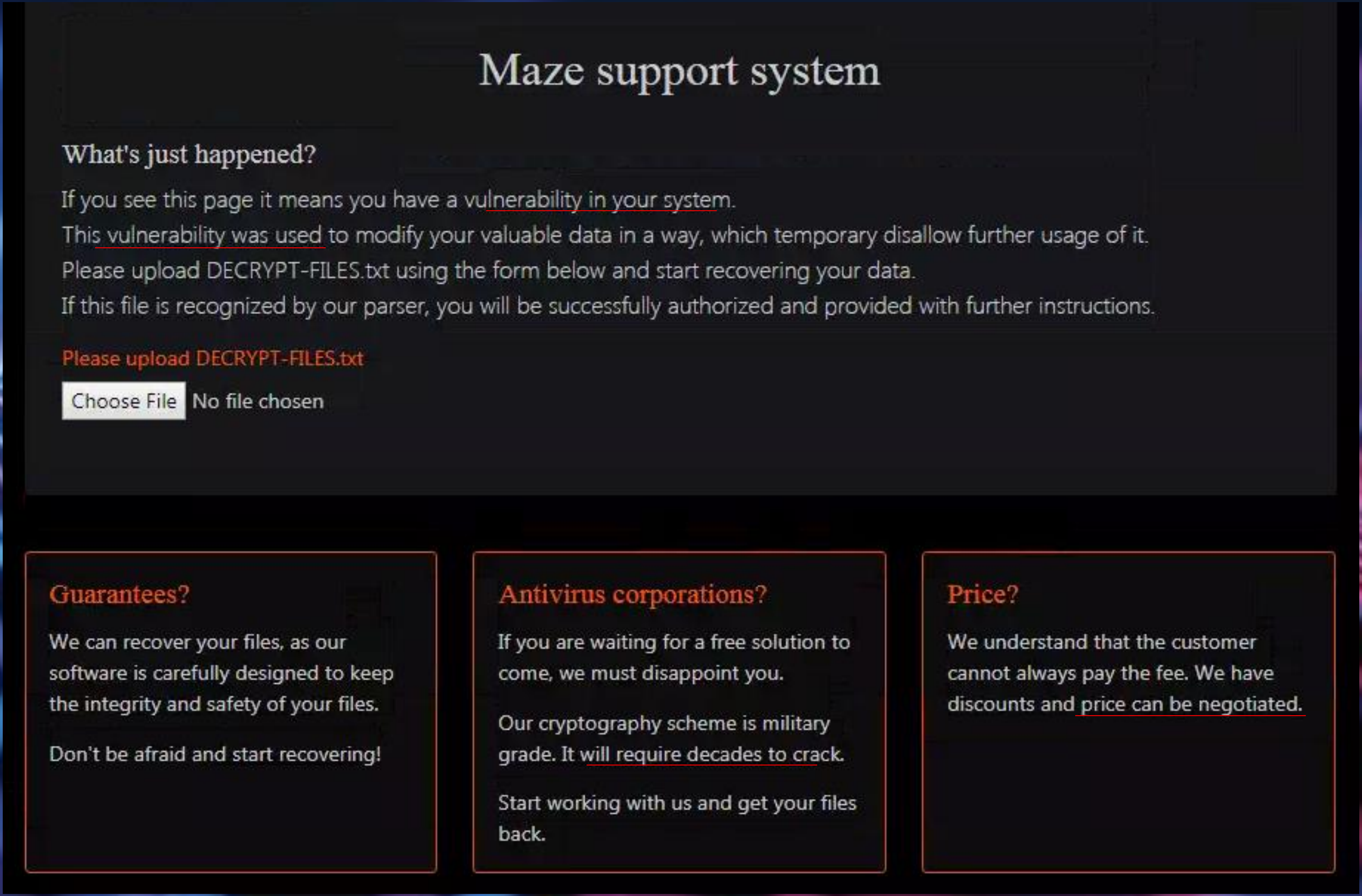
2. Negotiations means the dialog and finding the best solution for the both parties. If the client is too shy, or scared or just can't negotiate, this is exclusively the client's problem. We are not physiologists to understand the client and analyze its behavior patterns.

3. If you business analytics are not able to calculate the total loss and and trying to convince you that it won't cost you anything, please do to come back telling that you were misinformed that the recovery of data without us would cost you over a ten million dollars.

4. After the client failed to start combination we will start to publish the information. After 10 days all the information will be published. There will be no more delays for month or two.

5. With the start of publishing we will also notify all the client's partners, clients and regulators.

Ransomware-as-a-Service (RaaS) Decryption Site:



Maze support system

What's just happened?

If you see this page it means you have a vulnerability in your system.
This vulnerability was used to modify your valuable data in a way, which temporary disallow further usage of it.
Please upload DECRYPT-FILES.txt using the form below and start recovering your data.
If this file is recognized by our parser, you will be successfully authorized and provided with further instructions.

Please upload DECRYPT-FILES.txt

Guarantees?

We can recover your files, as our software is carefully designed to keep the integrity and safety of your files.

Don't be afraid and start recovering!

Antivirus corporations?

If you are waiting for a free solution to come, we must disappoint you.

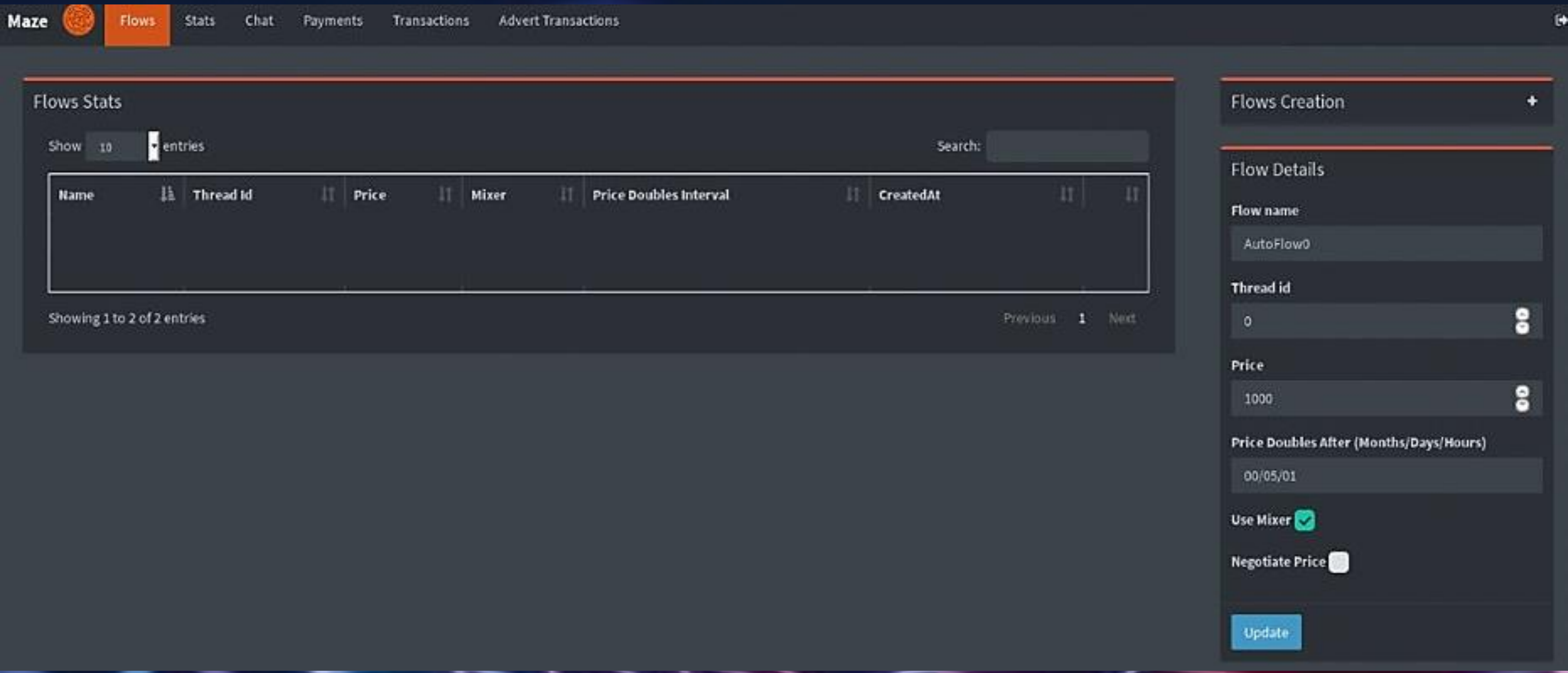
Our cryptography scheme is military grade. It will require decades to crack.

Start working with us and get your files back.

Price?

We understand that the customer cannot always pay the fee. We have discounts and price can be negotiated.

Ransomware-as-a-Service (RaaS) Control Panel:



Flows Stats

Show 10 entries

Search:

Name	Thread Id	Price	Mixer	Price Doubles Interval	CreatedAt

Showing 1 to 2 of 2 entries

Flows Creation

Flow Details

Flow name: AutoFlow0

Thread id: 0

Price: 1000

Price Doubles After (Months/Days/Hours): 00/05/01

Use Mixer ☑

Negotiate Price ☐

https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html

- ∞Web GUI
- ∞Handles Payments
- ∞Handles Decryption
- ∞Handles Malware Development
- ∞Obscures Attribution
- ∞Enables Campaigns

Thanos

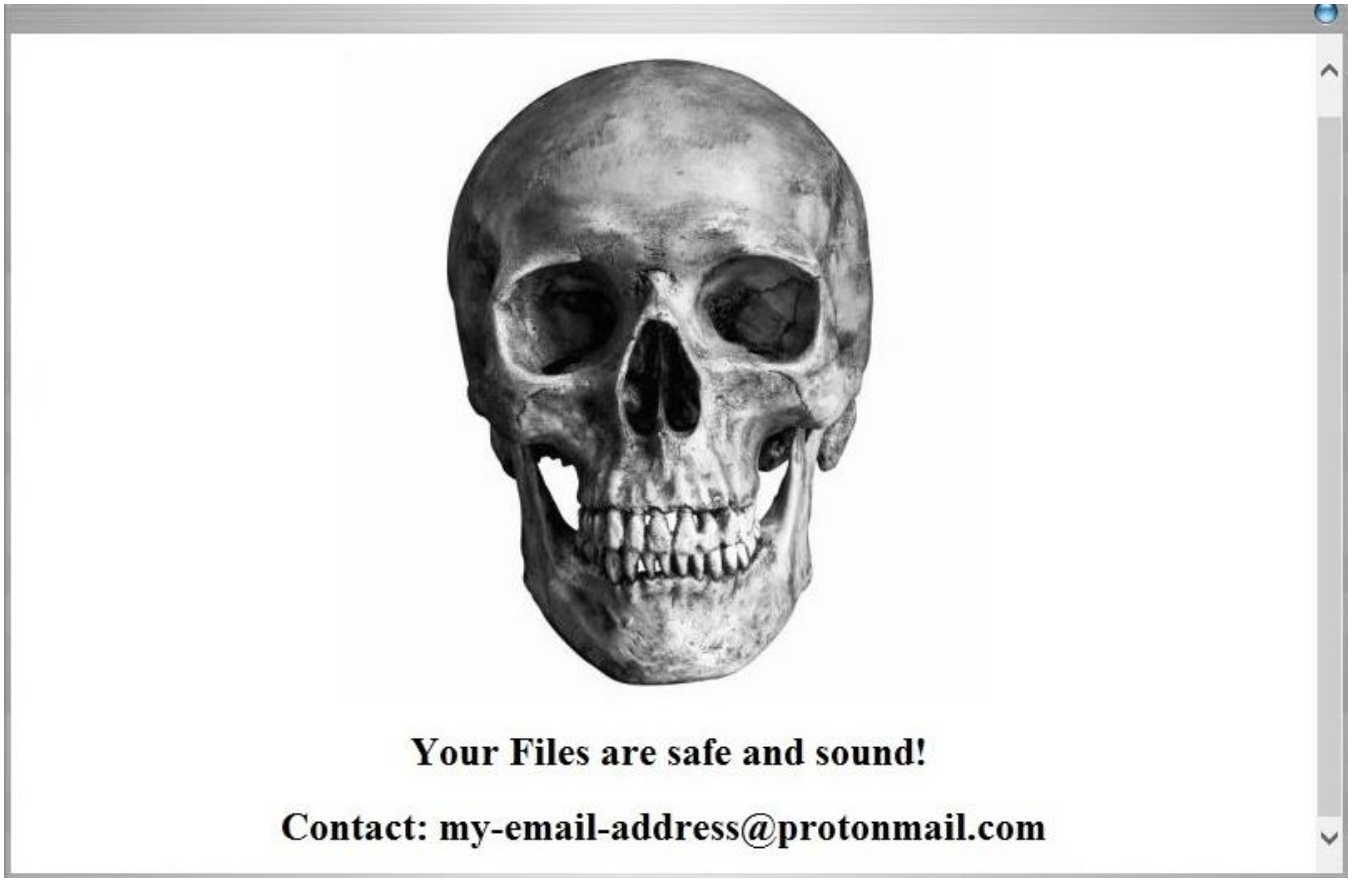
Ransomware-as-a-Service

Processes:

- ∞ OSINT
- ∞ Collection
- ∞ Analysis

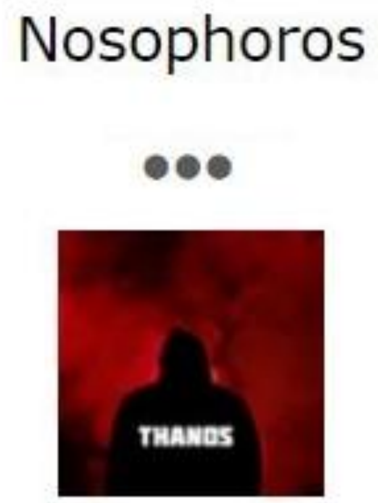
First Appeared in November 2019

Case Study: Gathering Intelligence on a Ransomware Developer



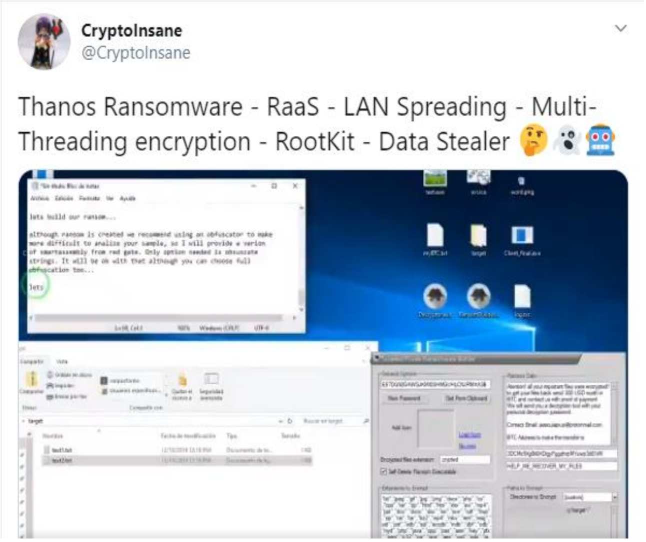
Your Files are safe and sound!

Contact: my-email-address@protonmail.com



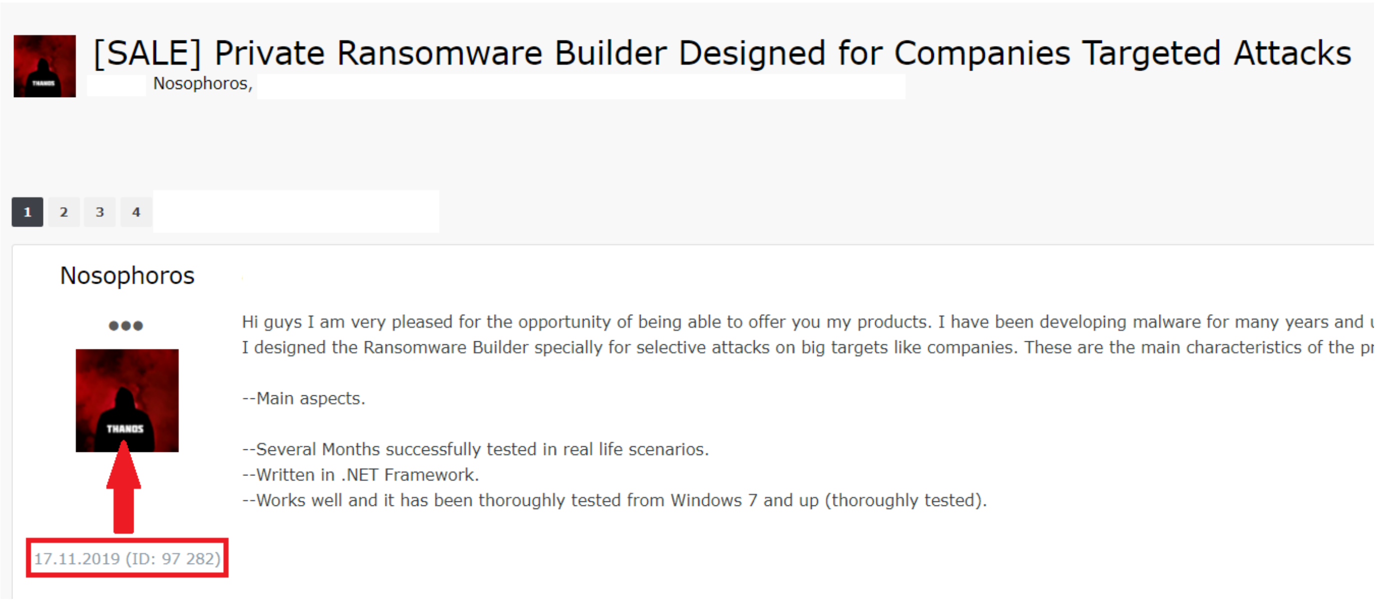
Nosophoros

OSINT:



CryptoInsane
@CryptoInsane

Thanos Ransomware - RaaS - LAN Spreading - Multi-Threading encryption - RootKit - Data Stealer 🤔👻🤖



[SALE] Private Ransomware Builder Designed for Companies Targeted Attacks

Nosophoros,

1 2 3 4

Nosophoros

17.11.2019 (ID: 97 282)

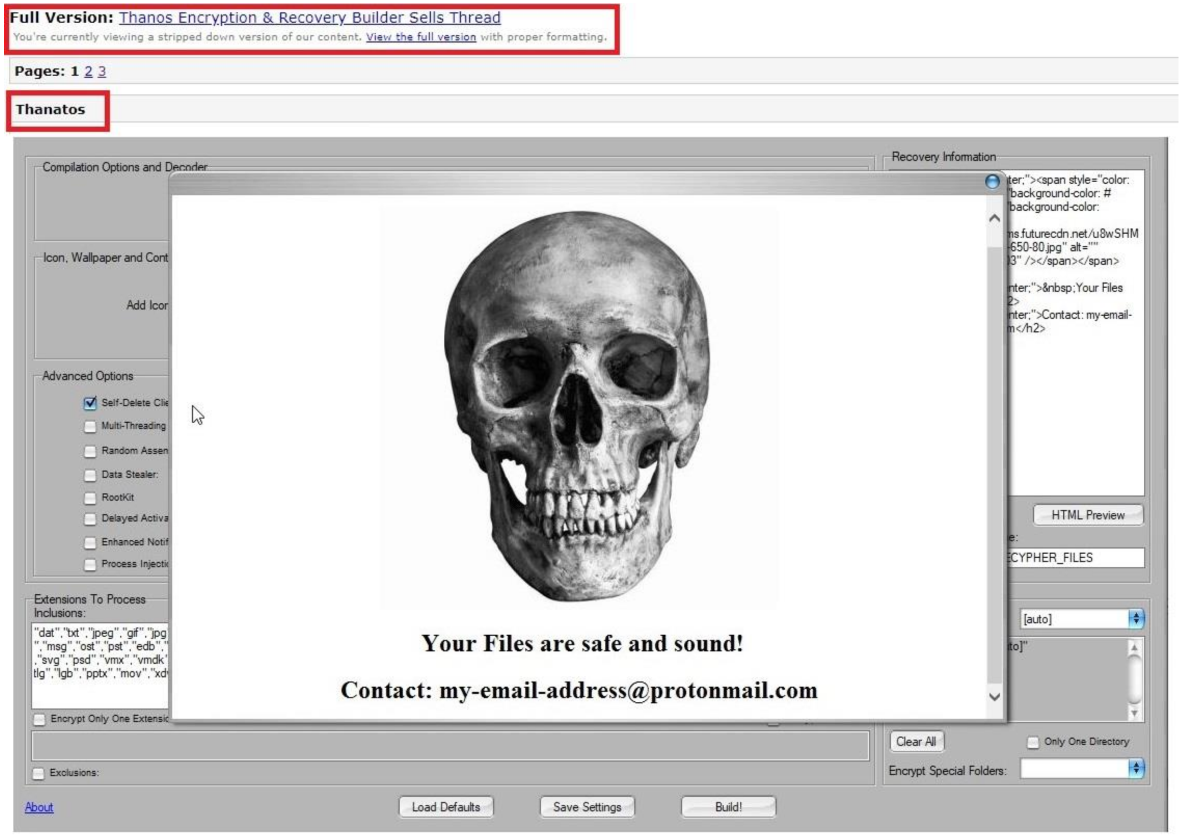
Hi guys I am very pleased for the opportunity of being able to offer you my products. I have been developing malware for many years and u

I designed the Ransomware Builder specially for selective attacks on big targets like companies. These are the main characteristics of the pr

--Main aspects.

--Several Months successfully tested in real life scenarios.
--Written in .NET Framework.
--Works well and it has been thoroughly tested from Windows 7 and up (thoroughly tested).

17.11.2019



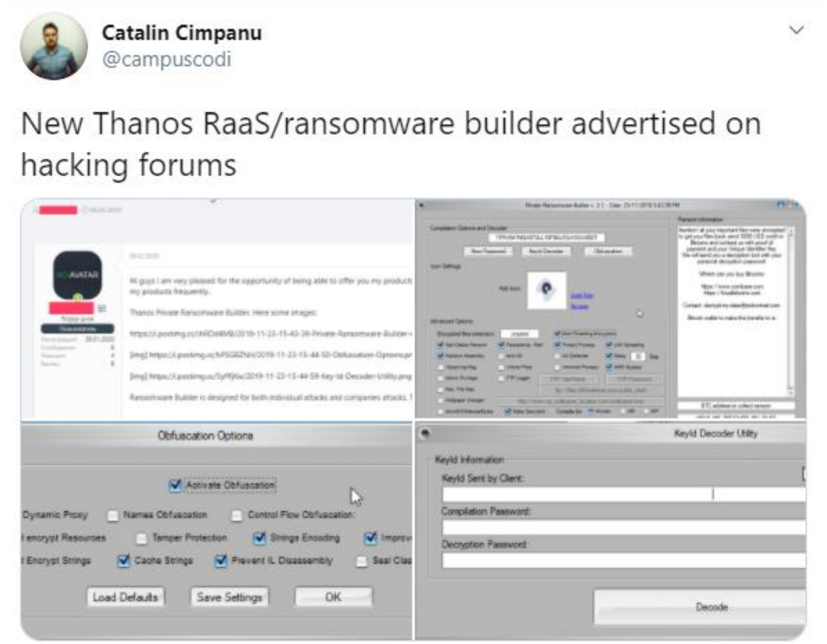
Full Version: Thanos Encryption & Recovery Builder Sells Thread
You're currently viewing a stripped down version of our content. View the full version with proper formatting.

Pages: 1 2 3

Thanatos

Your Files are safe and sound!

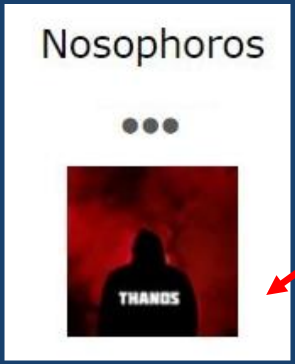
Contact: my-email-address@protonmail.com



Catalin Cimpanu
@campuscodi

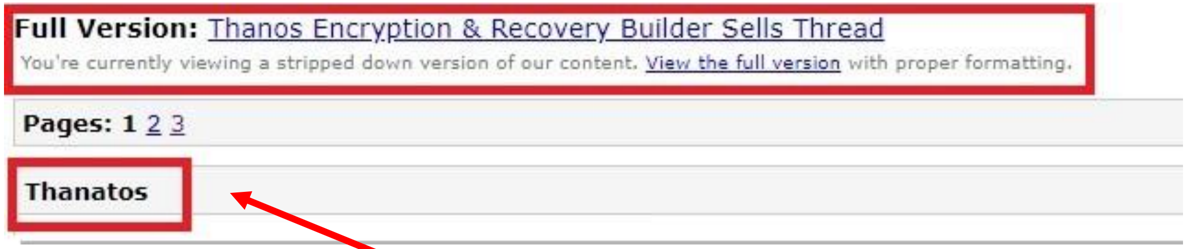
New Thanos RaaS/ransomware builder advertised on hacking forums

What we found:



Nosophoros

●●●

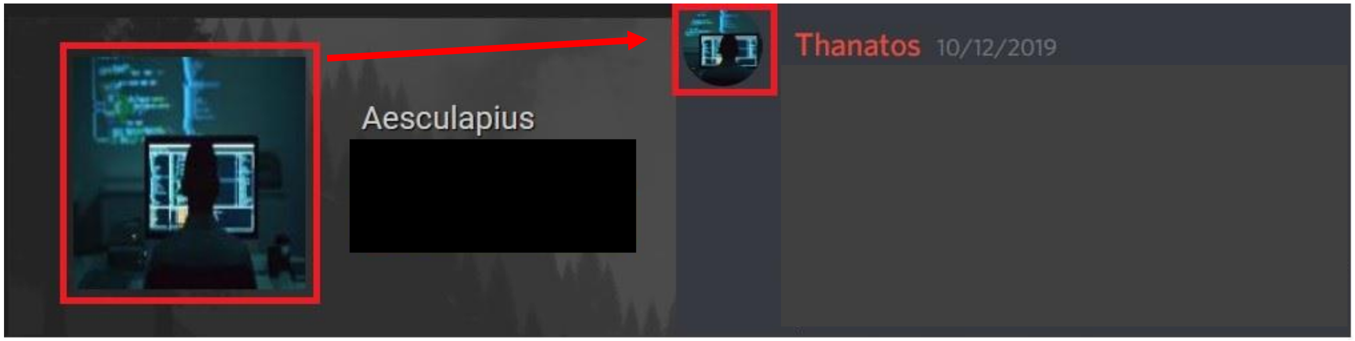


Full Version: Thanos Encryption & Recovery Builder Sells Thread

You're currently viewing a stripped down version of our content. View the full version with proper formatting.

Pages: 1 2 3

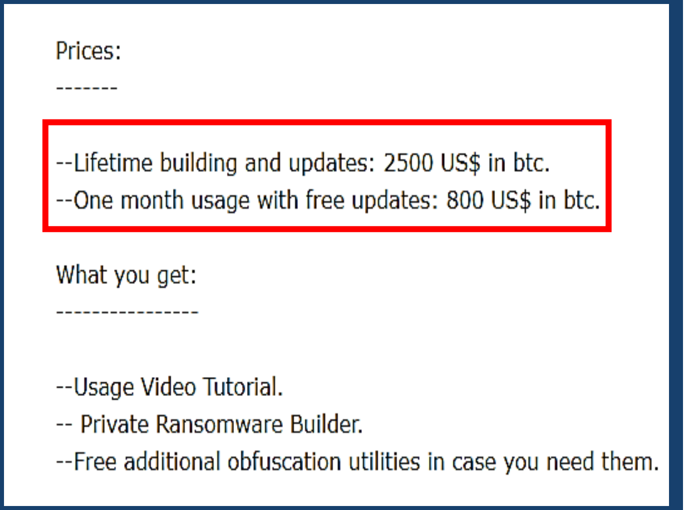
Thanatos



Aesculapius

[redacted]

Thanatos 10/12/2019



Prices:

--Lifetime building and updates: 2500 US$ in btc.

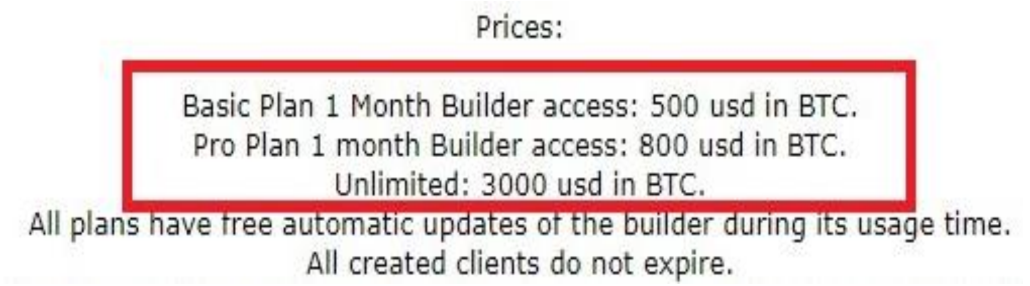
--One month usage with free updates: 800 US$ in btc.

What you get:

--Usage Video Tutorial.

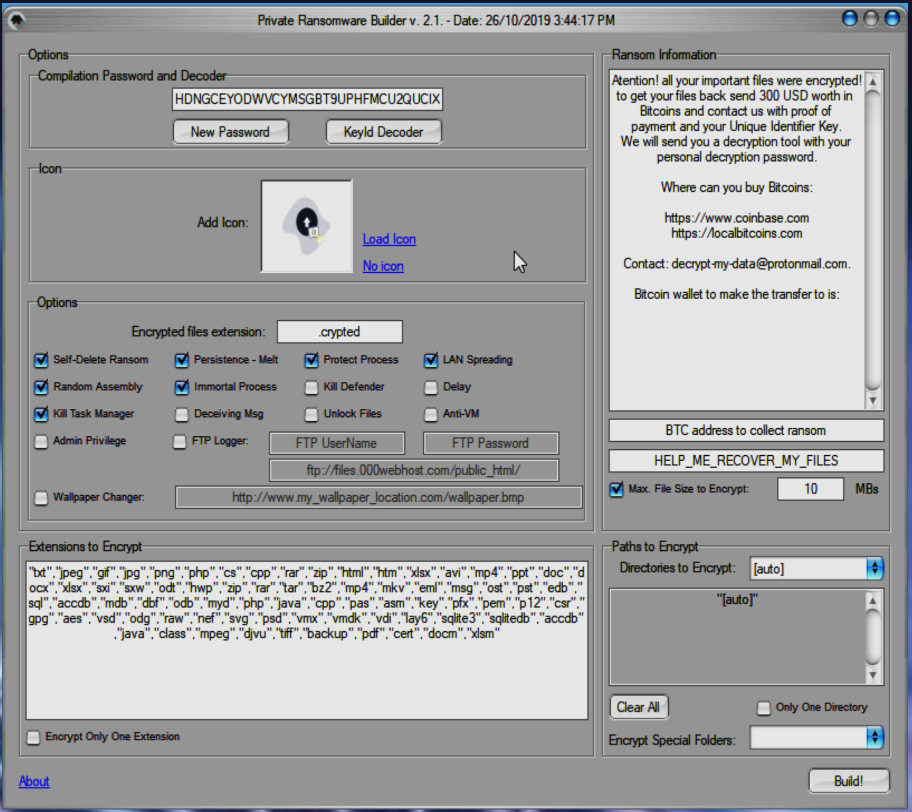
-- Private Ransomware Builder.

--Free additional obfuscation utilities in case you need them.



Prices:

Basic Plan 1 Month Builder access: 500 usd in BTC.
Pro Plan 1 month Builder access: 800 usd in BTC.
Unlimited: 3000 usd in BTC.
All plans have free automatic updates of the builder during its usage time.
All created clients do not expire.



Private Ransomware Builder v. 2.1. - Date: 26/10/2019 3:44:17 PM

Options

Compilation Password and Decoder

HDNGCEYODWVCYMSGBT9UPHFMCU2QUCIX

Icon

Add Icon:

Options

Encrypted files extension: .crypted

☑ Self-Delete Ransom ☑ Persistence - Melt ☑ Protect Process ☑ LAN Spreading
☑ Random Assembly ☑ Immortal Process □ Kill Defender □ Delay
☑ Kill Task Manager □ Deceiving Msg □ Unlock Files □ Anti-VM
□ Admin Privilege □ FTP Logger: FTP UserName FTP Password
ftp://files.000webhost.com/public_html/
□ Wallpaper Changer: http://www.my_wallpaper_location.com/wallpaper.bmp

Ransom Information

Atention! all your important files were encrypted!
to get your files back send 300 USD worth in
Bitcoins and contact us with proof of
payment and your Unique Identifier Key.
We will send you a decryption tool with your
personal decryption password.

Where can you buy Bitcoins:

https://www.coinbase.com
https://localbitcoins.com

Contact: decrypt-my-data@protonmail.com.

Bitcoin wallet to make the transfer to is:

BTC address to collect ransom

HELP_ME_RECOVER_MY_FILES

☑ Max. File Size to Encrypt: 10 MBs

Extensions to Encrypt

"txt","jpeg","gif","jpg","png","php","cs","cpp","rar","zip","html","htm","xlsx","avi","mp4","ppt","doc","docx","xlsx","sxi","sxw","odt","hwp","zip","rar","tar","bz2","mp4","mkv","eml","msg","ost","pst","edb","sql","accdb","mdb","dbf","odb","myd","php","java","cpp","pas","asm","key","pfx","pem","p12","csr","gpg","aes","vsd","odg","raw","nef","svg","psd","vmx","vmdk","vdi","lay6","sqlite3","sqlitedb","accdb","java","class","mpeg","djvu","tiff","backup","pdf","cert","docm","xlsm"

□ Encrypt Only One Extension

Paths to Encrypt

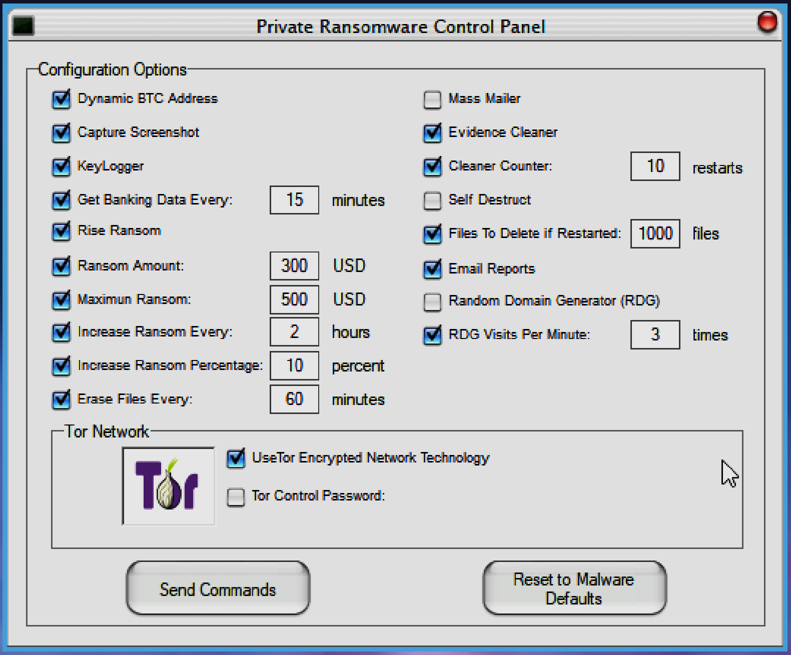
Directories to Encrypt: [auto]

"[auto]"

□ Only One Directory

Encrypt Special Folders:

RaaS Builder



Private Ransomware Control Panel

Configuration Options

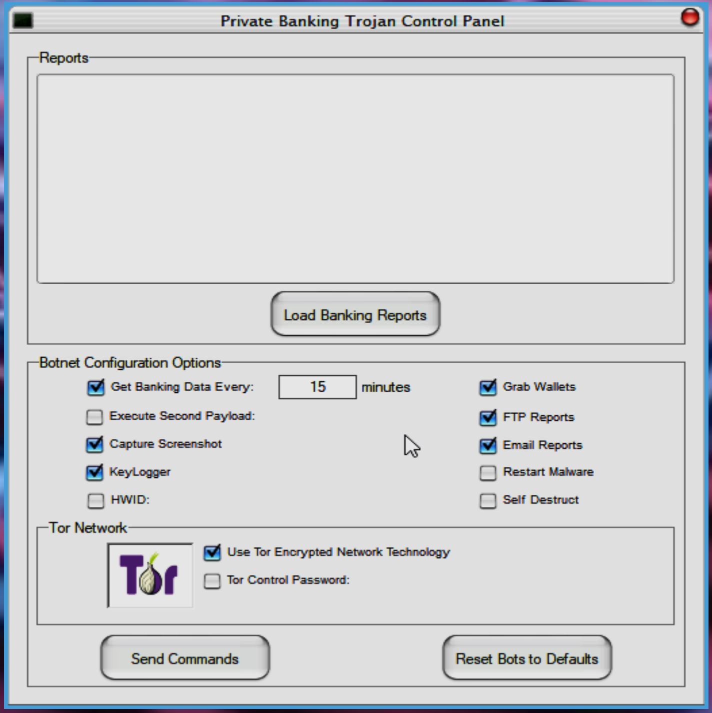
☑ Dynamic BTC Address
☑ Capture Screenshot
☑ KeyLogger
☑ Get Banking Data Every: 15 minutes
☑ Rise Ransom
☑ Ransom Amount: 300 USD
☑ Maximun Ransom: 500 USD
☑ Increase Ransom Every: 2 hours
☑ Increase Ransom Percentage: 10 percent
☑ Erase Files Every: 60 minutes

□ Mass Mailer
☑ Evidence Cleaner
☑ Cleaner Counter: 10 restarts
□ Self Destruct
☑ Files To Delete if Restarted: 1000 files
☑ Email Reports
□ Random Domain Generator (RDG)
☑ RDG Visits Per Minute: 3 times

Tor Network

☑ UseTor Encrypted Network Technology
□ Tor Control Password:

RaaS Control Panel



Private Banking Trojan Control Panel

Reports

Botnet Configuration Options

☑ Get Banking Data Every: 15 minutes
□ Execute Second Payload:
☑ Capture Screenshot
☑ KeyLogger
□ HWID:

☑ Grab Wallets
☑ FTP Reports
☑ Email Reports
□ Restart Malware
□ Self Destruct

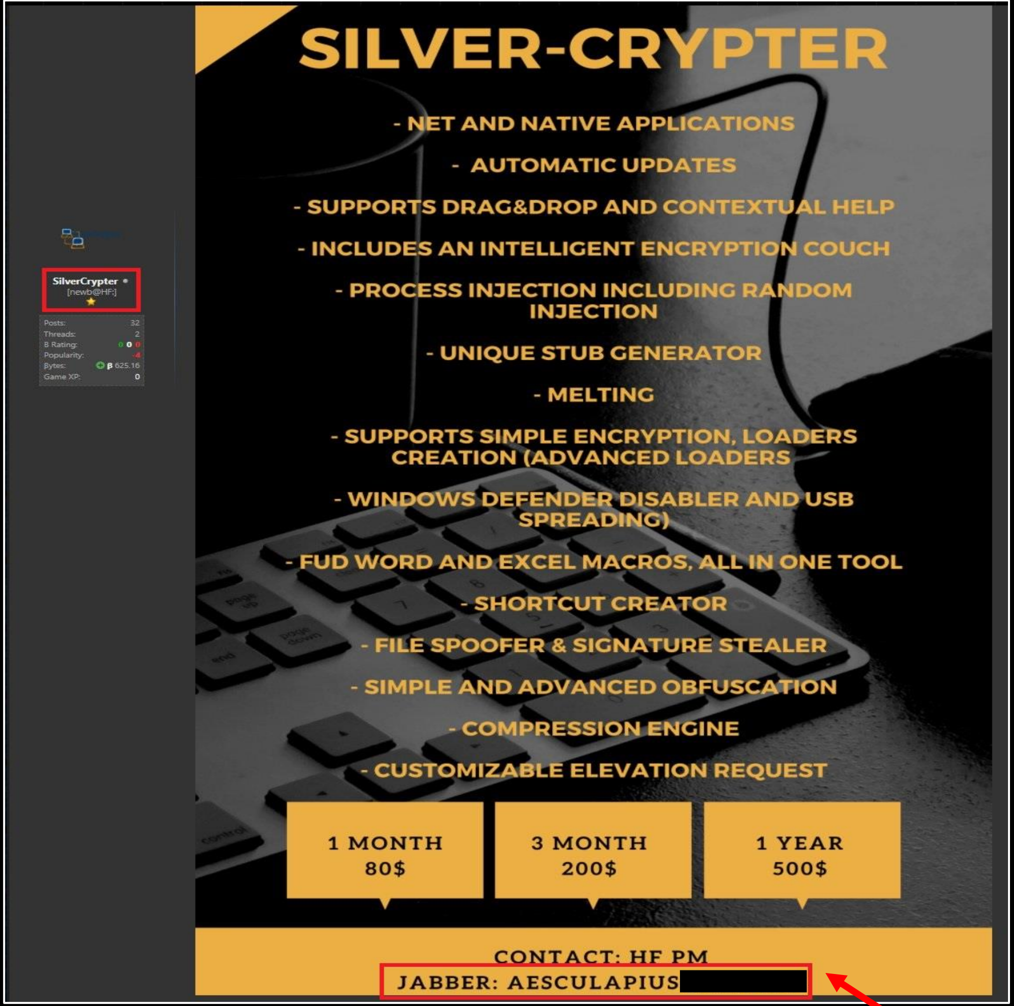
Tor Network

☑ Use Tor Encrypted Network Technology
□ Tor Control Password:

Banking Trojan

From the Forums:

Detection Evasion Tools



SilverCrypter
[newb@HF:]

Posts:	32
Threads:	2
B Rating:	0 0 0
Popularity:	-4
βytes:	β 625.16
Game XP:	0

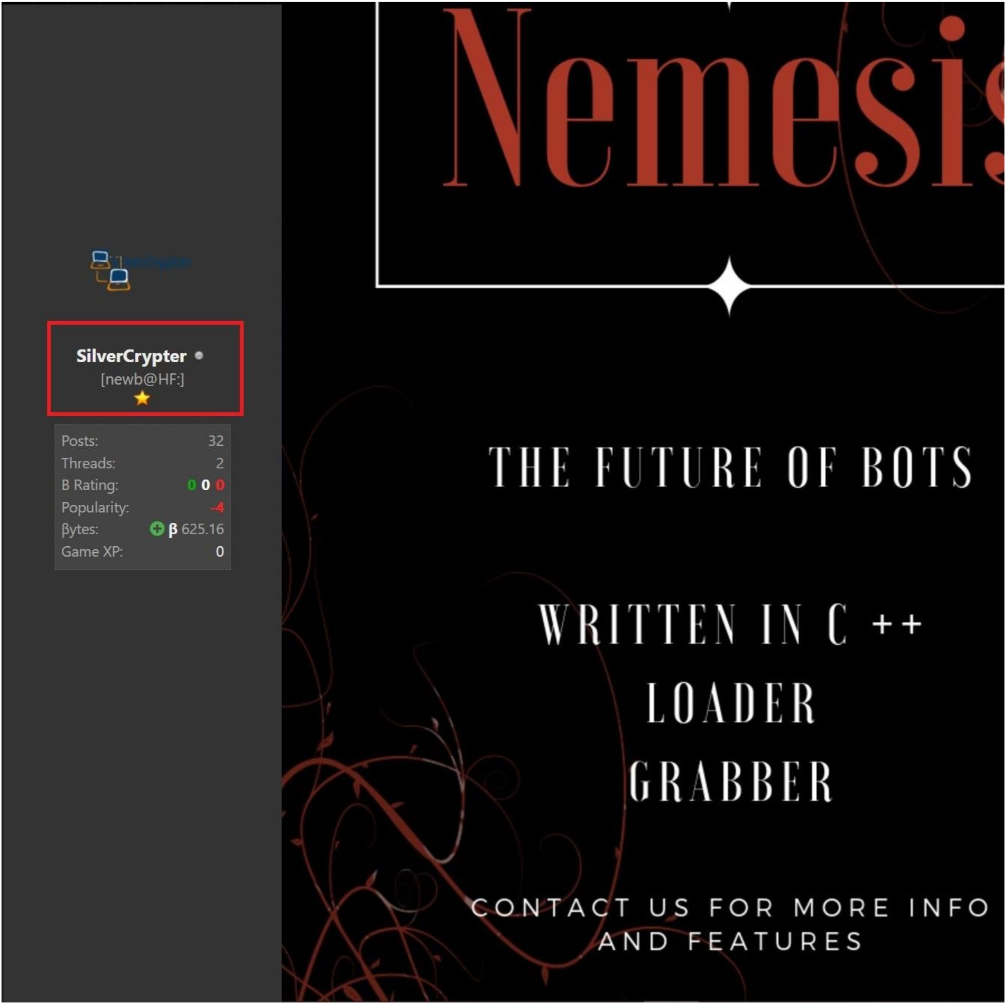
SILVER-CRYPTER

- NET AND NATIVE APPLICATIONS
- AUTOMATIC UPDATES
- SUPPORTS DRAG&DROP AND CONTEXTUAL HELP
- INCLUDES AN INTELLIGENT ENCRYPTION COUCH
- PROCESS INJECTION INCLUDING RANDOM INJECTION
- UNIQUE STUB GENERATOR
- MELTING
- SUPPORTS SIMPLE ENCRYPTION, LOADERS CREATION (ADVANCED LOADERS
- WINDOWS DEFENDER DISABLER AND USB SPREADING)
- FUD WORD AND EXCEL MACROS, ALL IN ONE TOOL
- SHORTCUT CREATOR
- FILE SPOOFER & SIGNATURE STEALER
- SIMPLE AND ADVANCED OBFUSCATION
- COMPRESSION ENGINE
- CUSTOMIZABLE ELEVATION REQUEST

1 MONTH	3 MONTH	1 YEAR
80$	200$	500$

CONTACT: HF PM
JABBER: AESCULAPIUS[redacted]

Information Stealer



SilverCrypter
[newb@HF:]

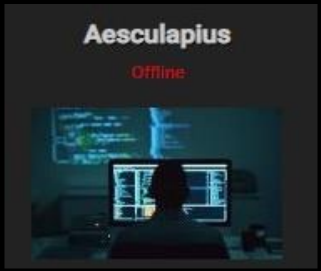
Posts:	32
Threads:	2
B Rating:	0 0 0
Popularity:	-4
βytes:	β 625.16
Game XP:	0

Nemesis

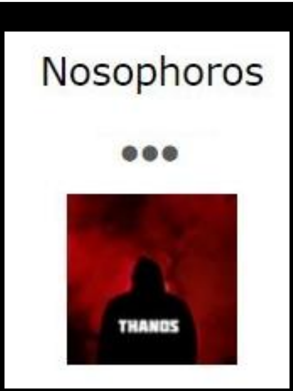
THE FUTURE OF BOTS

WRITTEN IN C ++
LOADER
GRABBER

CONTACT US FOR MORE INFO AND FEATURES



Aesculapius
Offline



Nosophoros
●●●

RaaS & Access brokers working together:

Access-as-a-Service:

∞ Underground Forums

∞ Marketplaces

∞ Access brokers

Types of Access:

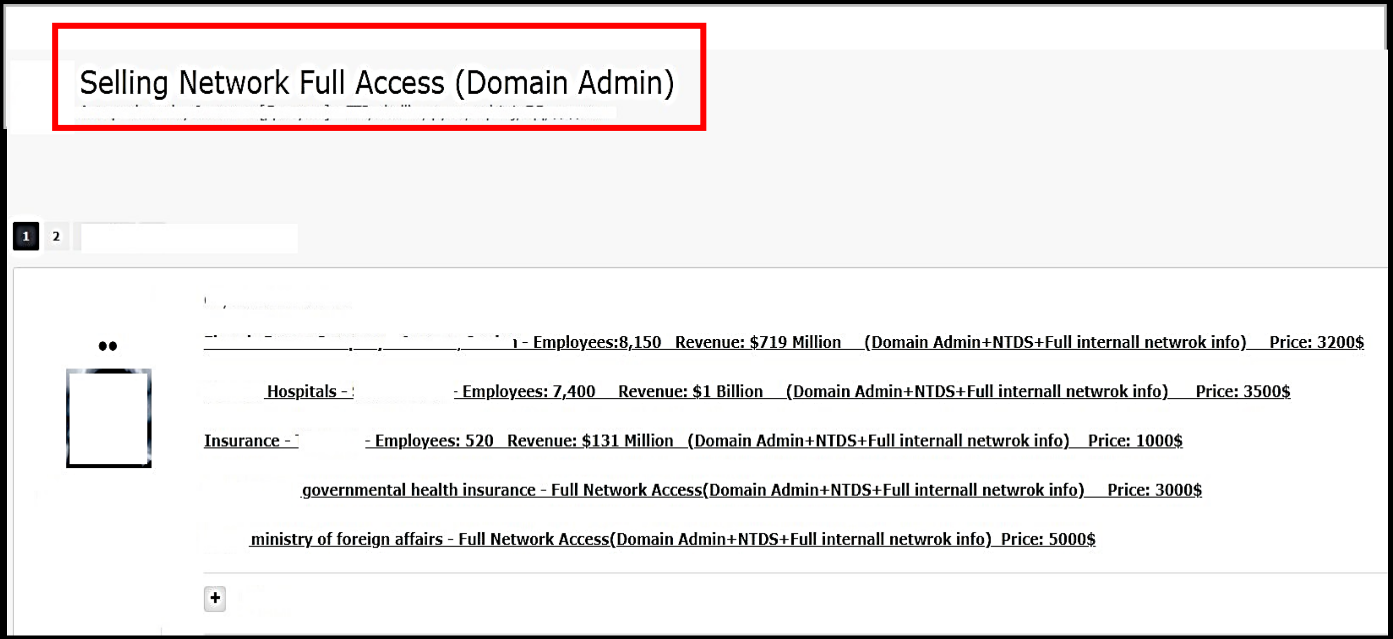
∞ VPNs (Pulse Secure, Citrix, etc)

∞ Domain Admin creds

∞ Web shells

∞ F5 BIG-IP

∞ Microsoft Exchange



Selling Network Full Access (Domain Admin)

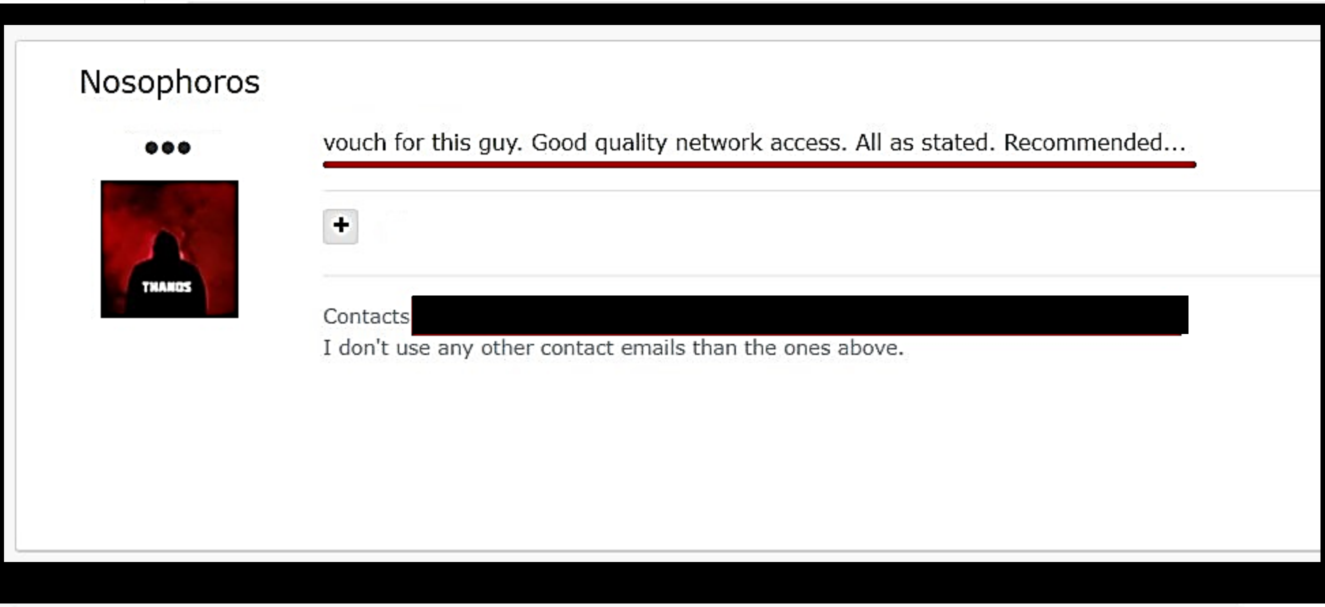
n - Employees:8,150 Revenue: $719 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 3200$

Hospitals - - Employees: 7,400 Revenue: $1 Billion (Domain Admin+NTDS+Full internall netwrok info) Price: 3500$

Insurance - - Employees: 520 Revenue: $131 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 1000$

governmental health insurance - Full Network Access(Domain Admin+NTDS+Full internall netwrok info) Price: 3000$

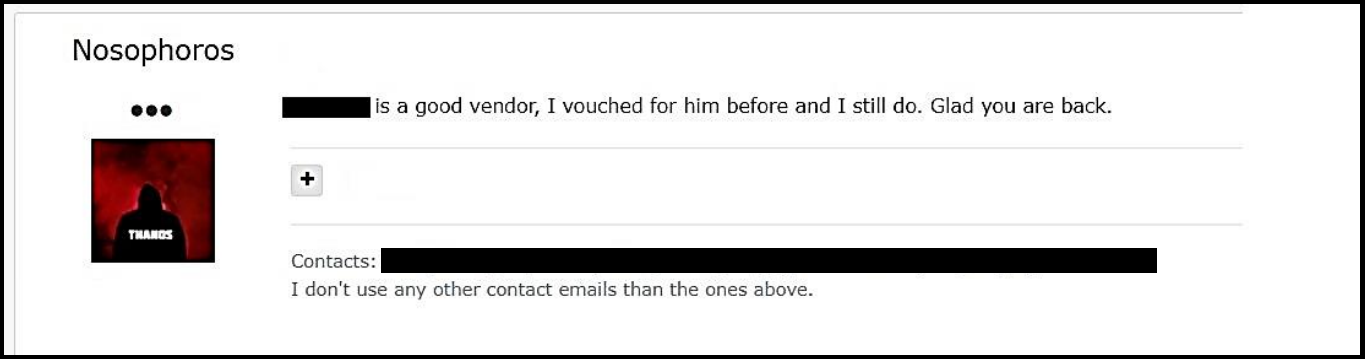
ministry of foreign affairs - Full Network Access(Domain Admin+NTDS+Full internall netwrok info) Price: 5000$



Nosophoros

vouch for this guy. Good quality network access. All as stated. Recommended...

Contacts [redacted]
I don't use any other contact emails than the ones above.



Nosophoros

[redacted] is a good vendor, I vouched for him before and I still do. Glad you are back.

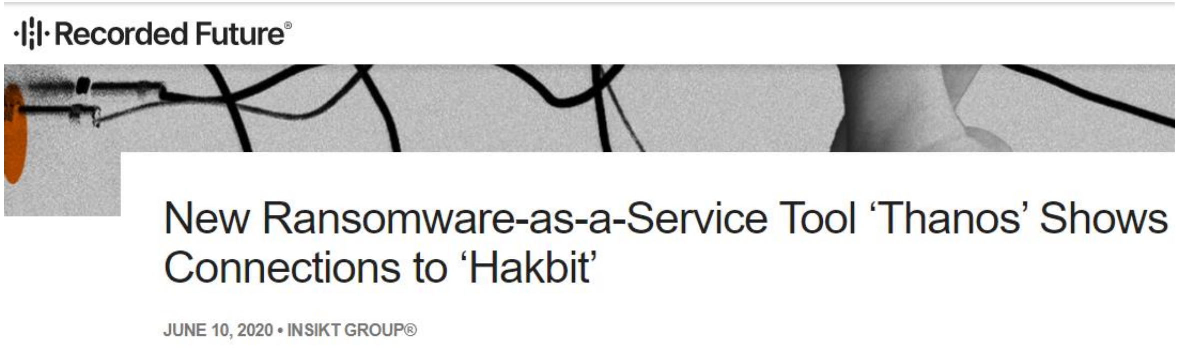
Contacts: [redacted]
I don't use any other contact emails than the ones above.

Threat Reports:

- Recorded Future
- SentinelOne
- Palo Alto Networks Unit 42
- ClearSky
- TTPs, IOCs, Malware Analysis

Key Takeaways:

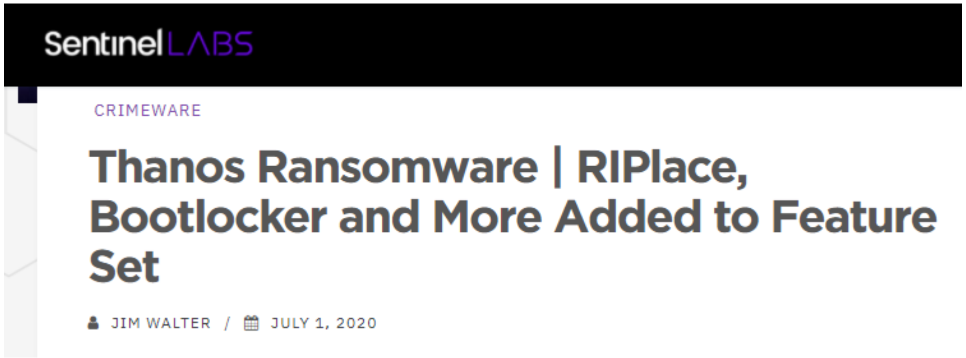
- Written in C#, .NET executable
- RIPlace technique
- Related to Hakbit ransomware
- "Ransomware Affiliate Program"
- AES File encryption, cannot be decrypted
- Targeted MENA countries
- Wake-on-LAN (WoL)
- Connected to MuddyWater *



Recorded Future®

New Ransomware-as-a-Service Tool 'Thanos' Shows Connections to 'Hakbit'

JUNE 10, 2020 • INSIKT GROUP®

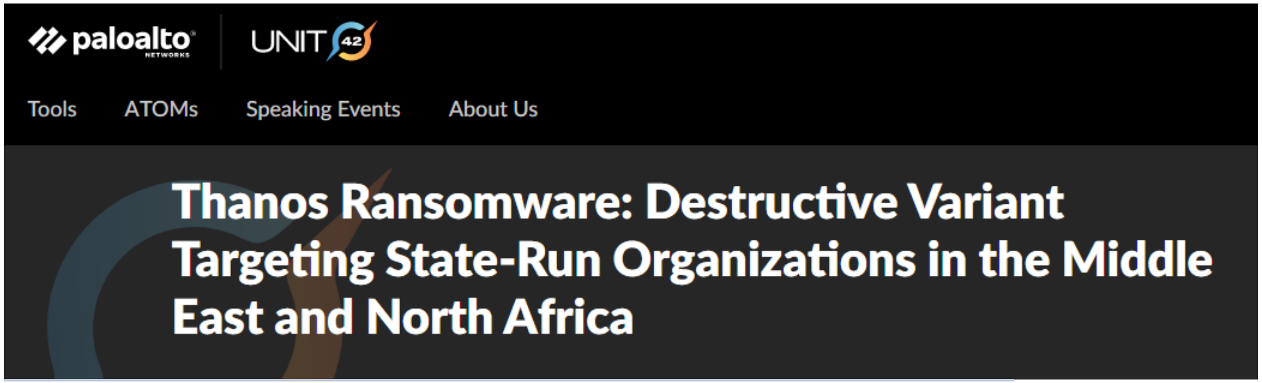


SentinelLABS

CRIMEWARE

Thanos Ransomware | RIPlace, Bootlocker and More Added to Feature Set

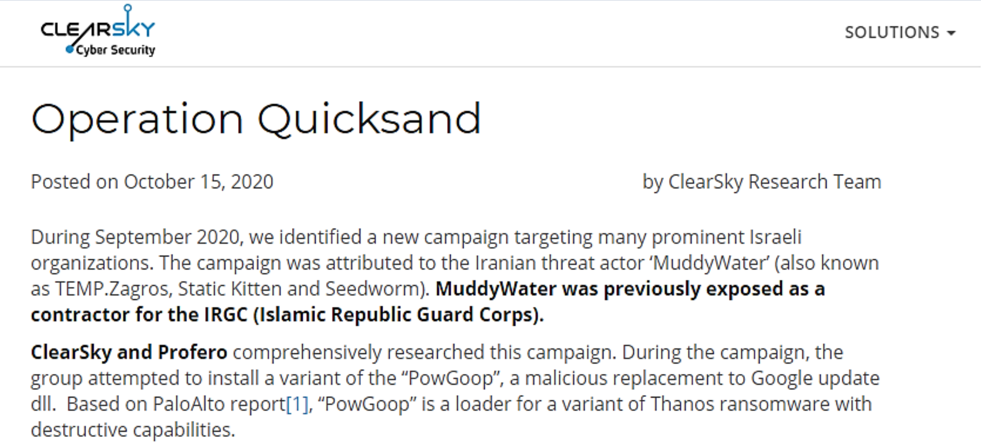
JIM WALTER / JULY 1, 2020



paloalto NETWORKS | UNIT 42

Tools ATOMs Speaking Events About Us

Thanos Ransomware: Destructive Variant Targeting State-Run Organizations in the Middle East and North Africa



CLEARSKY Cyber Security

SOLUTIONS ▾

Operation Quicksand

Posted on October 15, 2020 by ClearSky Research Team

During September 2020, we identified a new campaign targeting many prominent Israeli organizations. The campaign was attributed to the Iranian threat actor 'MuddyWater' (also known as TEMP.Zagros, Static Kitten and Seedworm). **MuddyWater was previously exposed as a contractor for the IRGC (Islamic Republic Guard Corps).**

ClearSky and Profero comprehensively researched this campaign. During the campaign, the group attempted to install a variant of the "PowGoop", a malicious replacement to Google update dll. Based on PaloAlto report[1], "PowGoop" is a loader for a variant of Thanos ransomware with destructive capabilities.

What?
So What?

What?

- This threat actor is responsible for developing, distributing, and advertising the Thanos Ransomware-as-a-Service offering. They are continuously working on the ransomware by adding new features and making sure it maintains a low detection rating on antivirus engines.

So What?

- The RaaS market is a growing threat that is attracting more cybercriminals
- More features will be added to ransomware to attract customers
- Building a community around their services, risk vs reward

Aliases for Thanos:

∞ Aesculapius

∞ Nosophoros

∞ Thanatos

∞ RaaS operators relies on communication with their customers.

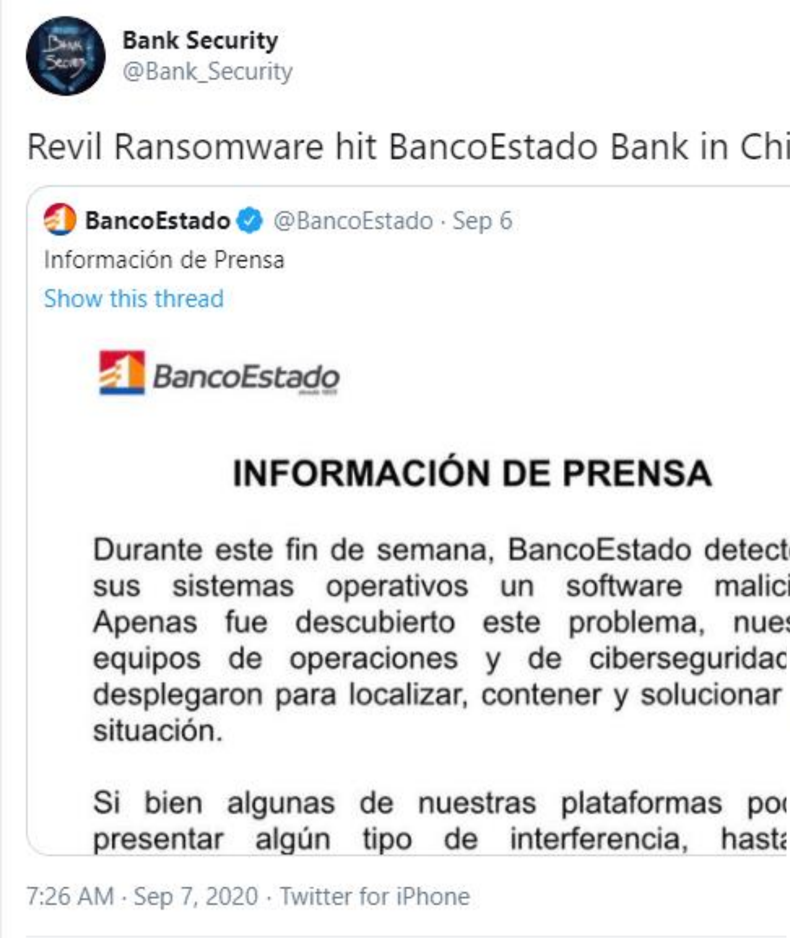
∞ Like most Darknet markets, trust needs to be maintained.

∞ Demonstrations to prove its effectiveness.

∞ Receive feedback for improvements.

∞ Tools: Thanos RaaS, Silver Crypter, Nemisis, Remcos RAT, Quasar RAT, Chimera Crypter, and an unknown Banking Trojan.

Example of Ransomware & Access:



Bank Security
@Bank_Security

Revil Ransomware hit BancoEstado Bank in Chile 🇨🇱

BancoEstado @BancoEstado · Sep 6
Información de Prensa
Show this thread

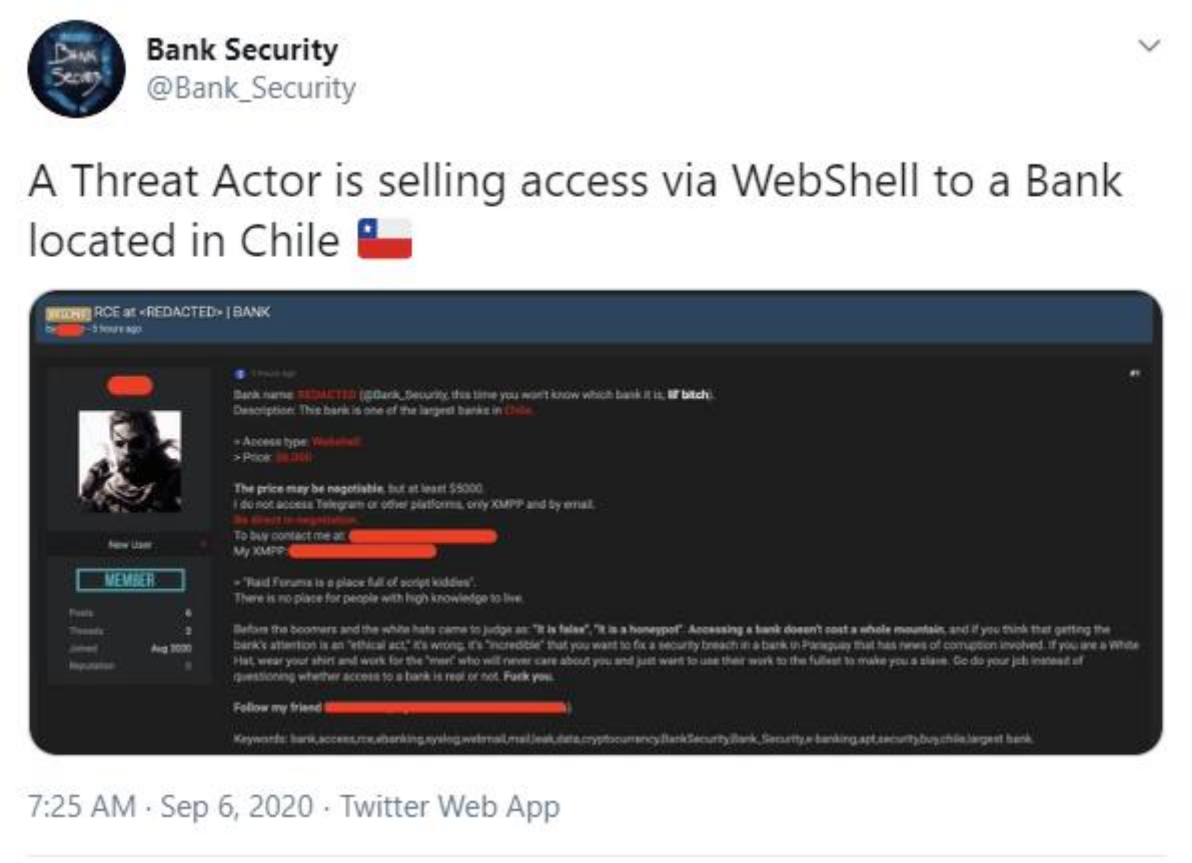
BancoEstado

INFORMACIÓN DE PRENSA

Durante este fin de semana, BancoEstado detectó en sus sistemas operativos un software malicioso. Apenas fue descubierto este problema, nuestros equipos de operaciones y de ciberseguridad desplegaron para localizar, contener y solucionar situación.

Si bien algunas de nuestras plataformas po presentar algún tipo de interferencia, hasta

7:26 AM · Sep 7, 2020 · Twitter for iPhone



Bank Security
@Bank_Security

A Threat Actor is selling access via WebShell to a Bank located in Chile 🇨🇱

RCE at <REDACTED> | BANK
by [redacted] - 5 hours ago

[redacted]

New User

MEMBER

Posts	6
Threads	2
Joined	Aug 2020
Reputation	0

Bank name: REDACTED (@Bank_Security, this time you won't know which bank it is, **lil' bitch**).
Description: This bank is one of the largest banks in Chile.

> Access type: Webshell
> Price: $6,000

The price may be negotiable, but at least $5000.
I do not access Telegram or other platforms, only XMPP and by email.
Be direct in negotiation.
To buy contact me at: [redacted]
My XMPP: [redacted]

> "Raid Forums is a place full of script kiddies".
There is no place for people with high knowledge to live.

Before the boomers and the white hats came to judge as: **"It is false", "It is a honeypot". Accessing a bank doesn't cost a whole mountain**, and if you think that getting the bank's attention is an "ethical act," it's wrong, it's "incredible" that you want to fix a security breach in a bank in Paraguay that has news of corruption involved. If you are a White Hat, wear your shirt and work for the "men" who will never care about you and just want to use their work to the fullest to make you a slave. Go do your job instead of questioning whether access to a bank is real or not. **Fuck you.**

Follow my friend [redacted])

Keywords: bank,access,rce,ebanking,syslog,webmail,mail,leak,data,cryptocurrency,BankSecurity,Bank_Security,e-banking,apt,security,buy,chile,largest bank.

7:25 AM · Sep 6, 2020 · Twitter Web App

(Thanks to @Bank_Security)

RANSOM!
Your files have been encrypted

conINT

ncptf
national child protection task force

Thank you conINT 2020!!

@BushidoToken on Twitter

blog.bushidotoken.net

trace labs

CTF

References:

- https://twitter.com/demonslay335
- https://twitter.com/GrujaRS
- https://twitter.com/Amigo_A_
- https://twitter.com/CryptoInsane/status/1226173390244810752
- https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/
- https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/
- https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
- https://www.proofpoint.com/us/blog/threat-insight/hakbit-ransomware-campaign-against-germany-austria-switzerland
- https://www.recordedfuture.com/thanos-ransomware-builder/
- https://unit42.paloaltonetworks.com/thanos-ransomware/
- https://www.clearskysec.com/operation-quicksand/
- https://twitter.com/Bank_Security/status/1302855863141629952
- https://twitter.com/Bank_Security/status/1302493192563109893
- https://www.rferl.org/a/in-lavish-wedding-photos-clues-to-an-alleged-russian-cyberthief-fsb-family-ties/30320440.html
- https://arstechnica.com/information-technology/2020/04/sophos-firewall-0day-allowing-remote-code-execution-comes-under-attack/
- https://app.any.run/tasks/68228222-4c8e-4f01-aa1d-4b1f4a6c390a/