
THE CURRENT STATE OF RANSOMWARE

Sebastian Gebhard

BSidesMunich

15.10.2023



LEAKED DATA

TWITTER >
PRESS ABOUT US >

HOW TO BUY BITCOIN >
AFFILIATE RULES >

CONTACT US >
MIRRORS >

UNTIL FILES 10H00M33S PUBLICATION

Deadline: 21 Oct, 2023 02:30:45 UTC



bsidesmunich.org

BSidesMunich is the premiere, independently organized computer security event in the Munich, Germany area, bringing together both local and internationally renowned experts. As an offshoot of our Meetup group, MUC:SEC, this conference extends our goals of bringing local computer security professionals together, exchanging ideas and experience and most importantly, establishing trust relationship within our community. This event is free.

Security BSides events are hosted all over the world and are community driven conferences. This also means that the conference will be what every attendee makes of it. So the success of the event will depend on your active participation, give a talk (in English), create a workshop, design a challenge for other attendees, help with the CTF or sponsoring.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 29 SEP, 2023 19:43 UTC

UPDATED: 11 OCT, 2023 10:39 UTC

EXTEND TIMER FOR 24 HOURS

DESTROY ALL INFORMATION

DOWNLOAD DATA AT ANY MOMENT

\$ 5000

\$ 250000

\$ 250000

Hi,
P.O.
51
He
Phone: (252) 492-7541 Toll Free: 1-800-232-7541
Fax: (252) 492-2444 (9191)

Vendor	Ordered Date	Ordered By	Location
100	09/22/23	DENIGE USHER	HENDERSON, NC
F.O.B.	Date Required	Backorder	Terms
		YES	Net 10ch

Commercial Card Program. All gray shaded fields are required to be completed.

Part 1. Confirm your company details
 Part 2. Add or change the primary Program Administrator
 Part 3. Add or change other contacts
 Part 4. Set up automated clearing house (ACH) auto-debits (US only)
 Part 5. Set up rebate payment instructions
 Part 6. Confirm these authorizations (signatures)

You don't need to complete all sections if you have already supplied information and it remains current. But your authorized representatives must sign the form's final page.

Please return the signed form, keeping a copy for your records, to either:

- your Implementation contact, if you are a new or onboarding client, or
- your Commercial Card Client Services contact, if you are an existing client working with Servicing.

Please note:

- We can only act on this form until we receive written notice of a change, and we have had reasonable time to act on it.
- Terms not otherwise defined here have the same meaning as in your Commercial Card Agreement.

Requestor: Pateman, Justin
 Run Date: 18-Mar-2022 10:49:20 AM EDT

International High Value (Wire)
 Payment Category: Request Wire

Status: Confirmed by Bank
 Transaction Number: 2236441710XK22

Debit Account Information
 Debit Bank: 053000196
 Debit Account: 25105442615
 Debit Account Name: FT INTERNATIONAL operating acct
 Debit Currency: USD

Beneficiary Details
 Beneficiary Name: FT International LLC, 1817
 Beneficiary Account: 3752547



HOW IT STARTED



A quick overview of
malware history



From: [REDACTED]
To: [REDACTED]
Cc:
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.



LOVE-LET...
(10KB)

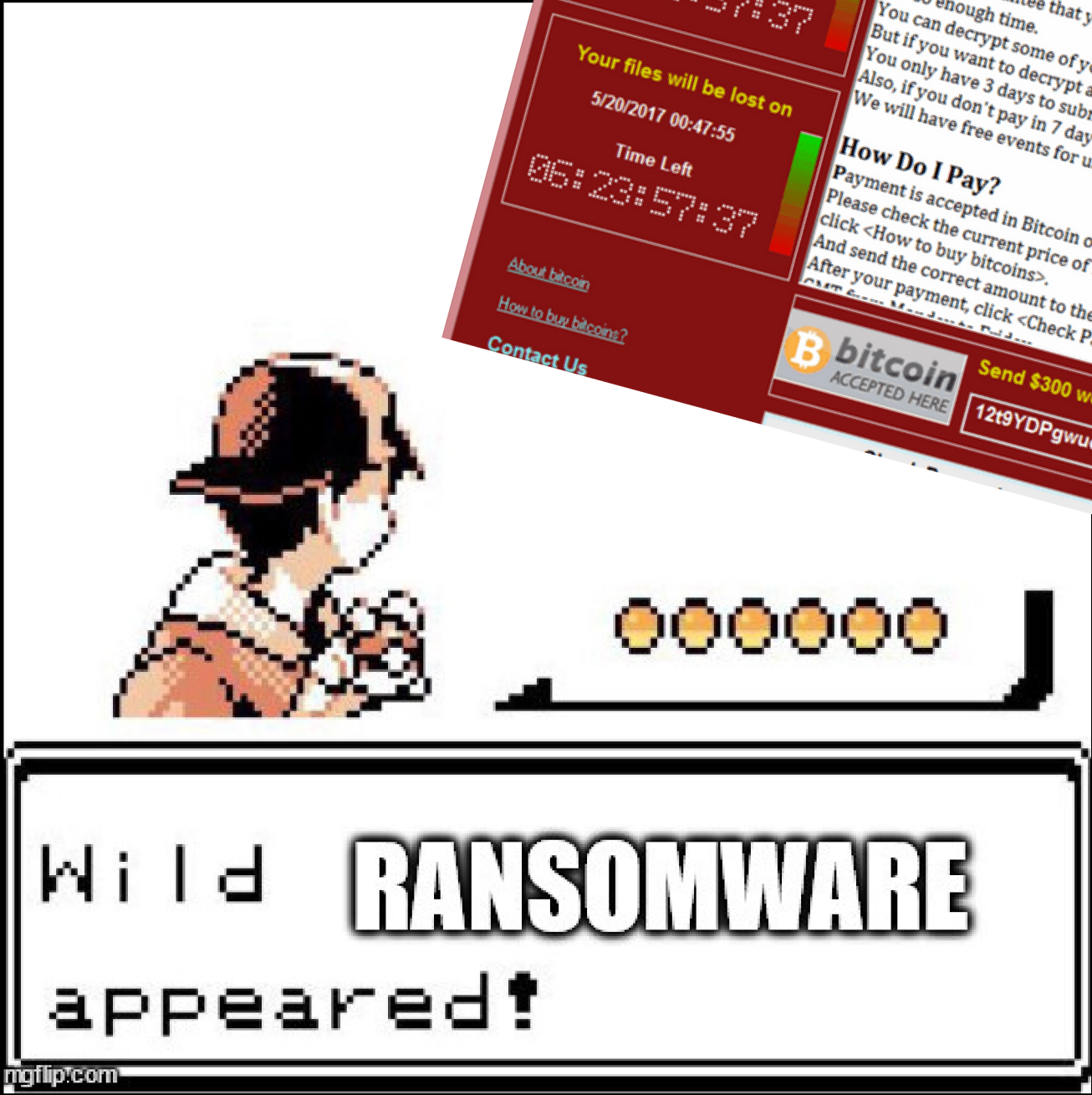
2000: I LOVE YOU





HUNTER BECOMES THE PREY



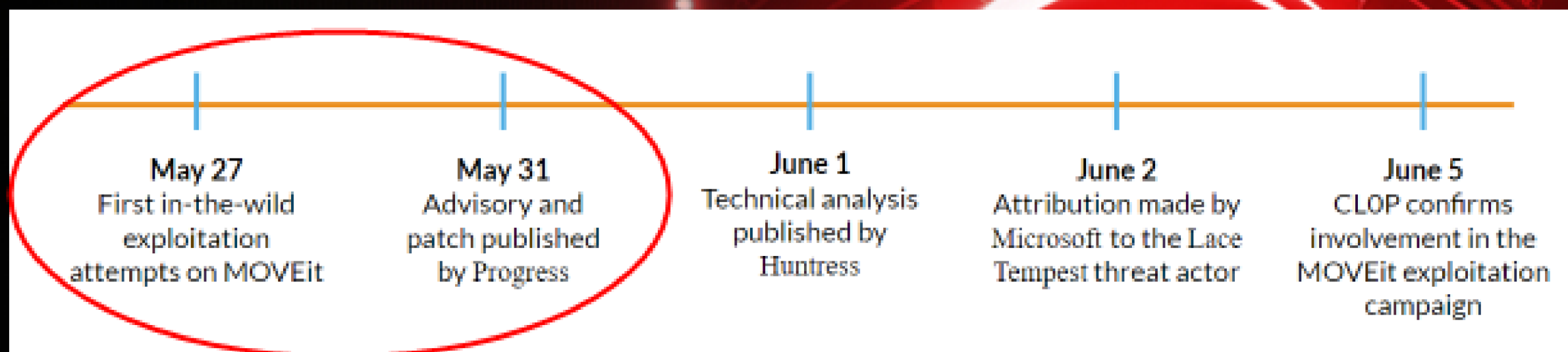


2017: WANNACRY



2023 : MOVEIT

SOC
PRIME



MOVEIT TRANSFER ZERO-DAY

Critical Vulnerability Actively Exploited in the Wild To Target Enterprises Worldwide



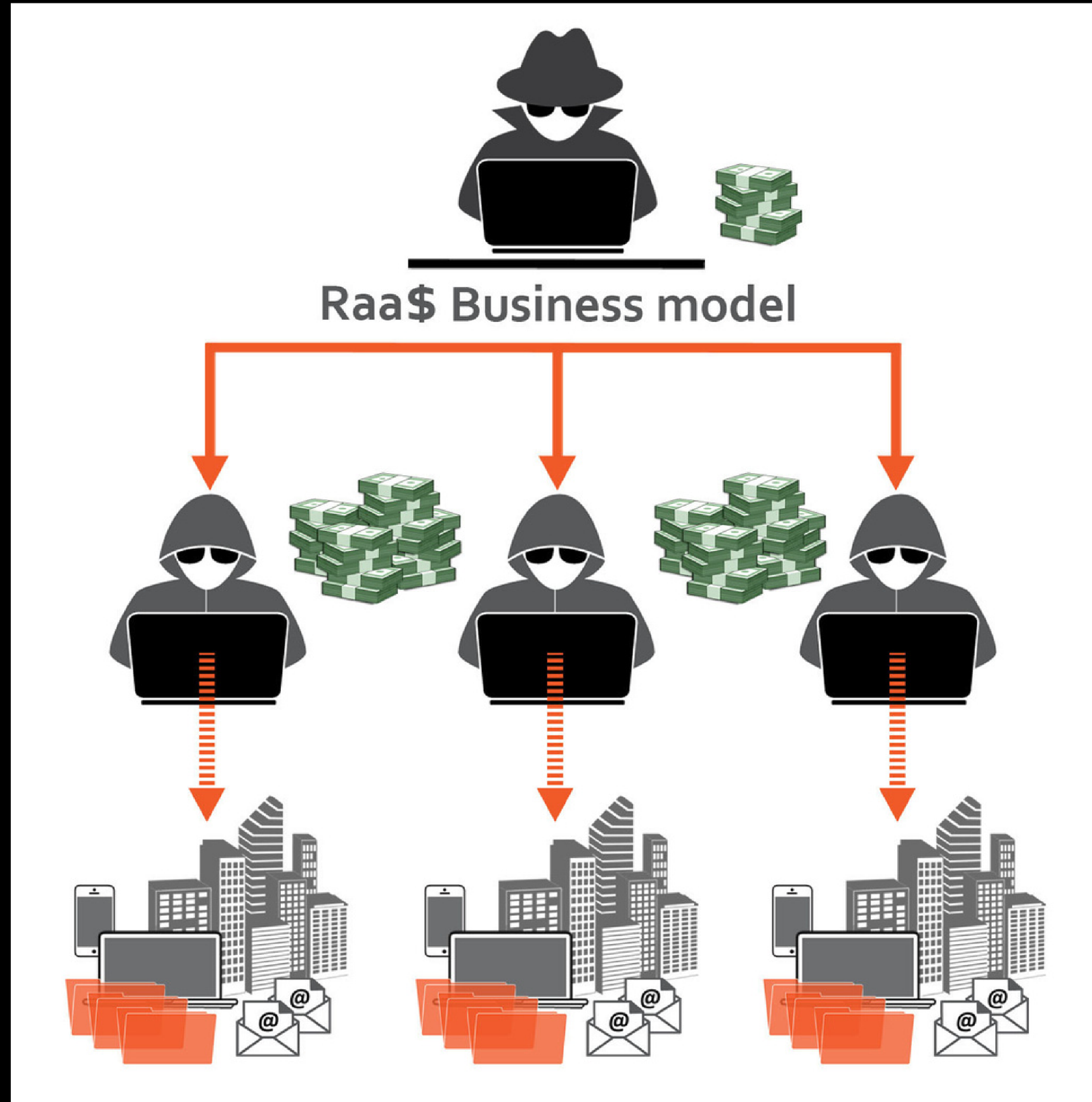
HOW IT'S GOING

The current threat
landscape



RAAS BUSINESS MODEL

Ransomware-as-a-service



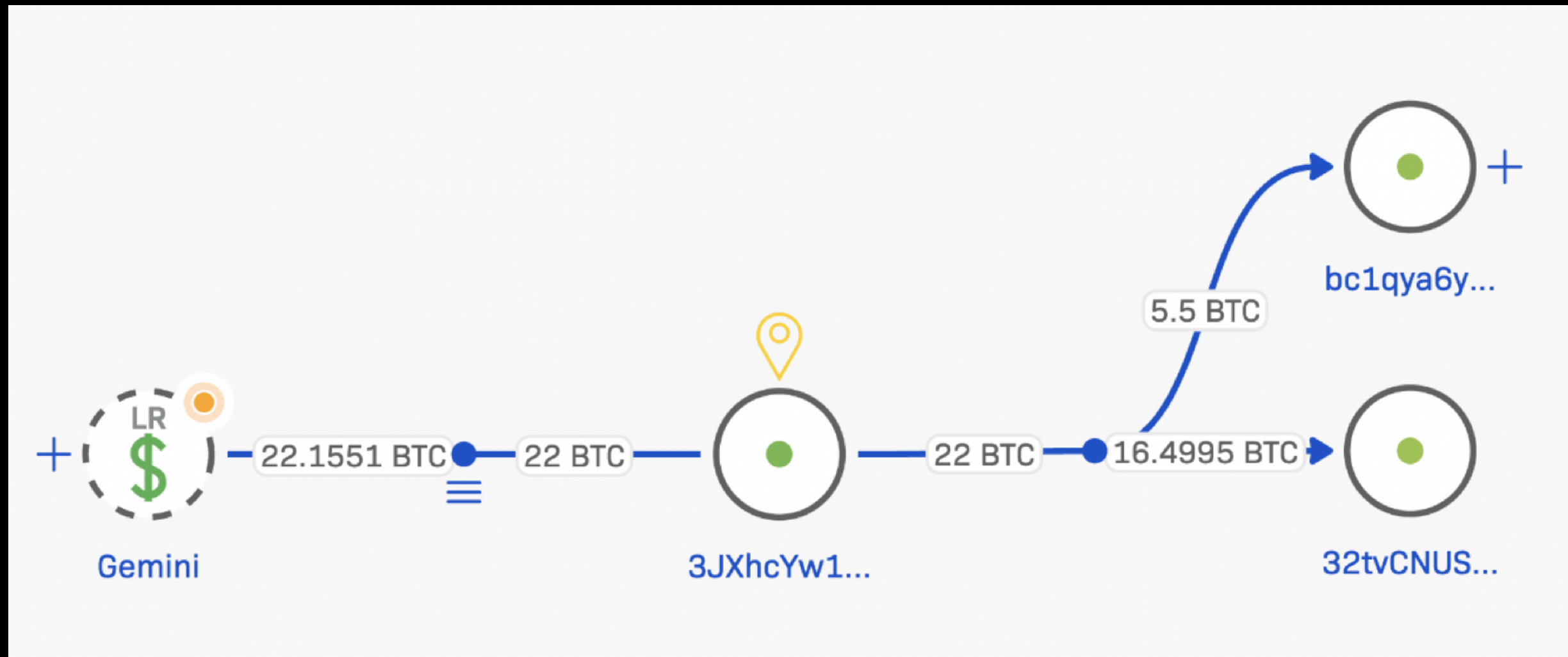
RaaS operator
20 %

Affiliates
80 %

Victims

RAAS BUSINESS MODEL

Ransomware-as-a-service



AFFILIATES?



OnLine Рынок → Партнёрки
[RaaS] AvosLocker - Partnership Program Windows/Linux/ESXi
AvosLocker Продавец
Опубликован: 29 Октября 2021 в 04:42

Avos2, AvosLocker's latest Windows variant, is one of the fastest in the market, with highly scalable threading and selective ciphers.

AvosLocker provides the following services & qualities for its affiliates:

- Supports Windows, Linux & ESXi
- Affiliate panel
- Negotiation panel with push & sound notifications
- Assistance in negotiations
- Consultations on operations
- Automatic builds
- Automatic decryption tests
- Encryption of network resources
- Killing of processes and services with open handles to files
- Highly configurable builds
- Removal of shadow copies
- Data storage
- DDoS attacks
- Calling services
- Diverse network of penetration testers, access brokers and other contacts

Our new variants (avos2 / avoslinux) have the best of both worlds to offer: high performance & high amount of encryption compared to its competitors.

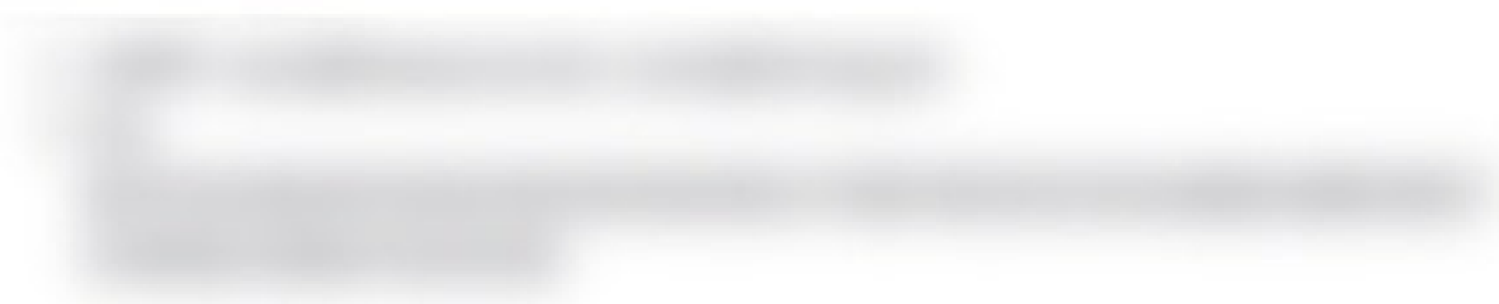
Compared to our competitors, we encrypt the largest amount of data PER FILE, meaning large files are impossible to recover unlike some variants that only encrypt a tiny section of the files. We also achieve the maximum performance possible on any hardware as our cipher is a software stream cipher. We use I/O completion ports in avos2 for our threading model.

We regularly update our products (lockers,panel and everything else) based on our affiliates' feedback.

Terms and conditions vary.

Attacking Post-soviet/CIS is not allowed.

Contact Information



AFFILIATES?

 Рынок → Партнёрки
[RaaS] AvosLocker - Partnership Program Windows/Linux/ESXi
AvosLocker Продавец
Опубликован: 29 Октября 2021 в 04:42

Avos2, AvosLocker's latest Windows variant, is one of the fastest in the market, with highly scalable threading and selective ciphers.

AvosLocker provides the following services & qualities for its affiliates:

- Supports Windows, Linux & ESXi
- Affiliate panel
- Negotiation panel with push & sound notifications
- Assistance in negotiations
- Consultations on operations
- Automatic builds
- Automatic decryption tests
- Encryption of network resources
- Killing of processes and services with open handles to files
- Highly configurable builds
- Removal of shadow copies
- Data storage
- DDoS attacks
- Calling services
- Diverse network of penetration testers, access brokers and other contacts

Our new variants (avos2 / avoslinux) have the best of both worlds to offer: high performance & high amount of encryption compared to its competitors.

Compared to our competitors, we encrypt the largest amount of data PER FILE, meaning large files are impossible to recover unlike some variants that only encrypt a tiny section of the files. We also achieve the maximum performance possible on any hardware as our cipher is a software stream cipher. We use I/O completion ports in avos2 for our threading model.

We regularly update our products (lockers, panel and everything else) based on our affiliates' feedback.

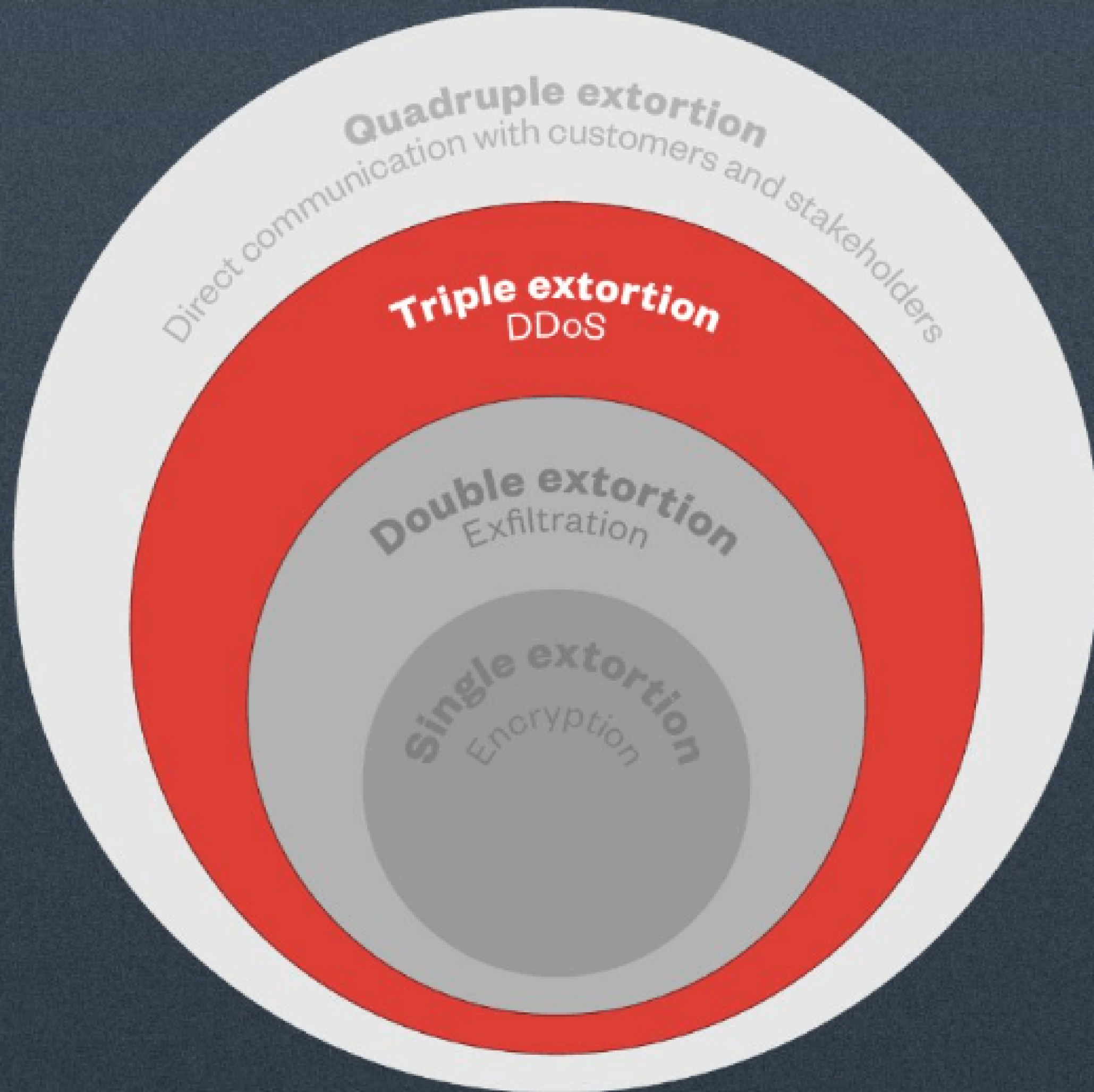
Terms and conditions vary.

Attacking Post-soviet/CIS is not allowed.

Contact Information



QUADRUPLE EXTORTION



AFFILIATES?

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.



Would you like to earn millions of dollars?

Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.

You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.

Companies pay us the foreclosure for the decryption of files and prevention of data leak.

You can communicate with us through the Tox messenger


<https://tox.chat/download.html>

Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

If you want to contact us, use ToxID:



If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser





AFFILIATES?

After many years of experience, we concluded that the most effective way to test a candidate for accession is a deposit. When you join, **you deposit 1 bitcoin in our wallet**, in fact, **this amount is an advance** and will be used at your subsequent payments as payment for our 20% share. For example, the company paid you a ransom for decrypting 100 bitcoins, you have to transfer a share of 20 bitcoins to us, but thanks to the deposit you made when you joined, the amount of the share paid will be 19 bitcoins. This procedure is required only once, only when you join the affiliate program. The **deposit weeds out insecure newbies, cops, FBI agents, journalists, white haters, web pentesters, competitors, and other small rodent pests**. The deposit amount may be reduced or not required at all, depending on what reputation you have and what information you can provide about yourself.

Recommended, but not required, application form when joining:

1. Links to your **profiles on various hacker forums** - the older your account, the better.
2. Describe your **experience with other affiliate programs**, preferably with some **evidence**, such as screenshots and transactions that show your **payouts**.
3. **Show your balance in cryptocurrency** at the moment.
4. Explain the reasons **why you left another affiliate program and want to work with us**.
5. Tell about the **current accesses you have and are ready to attack immediately** after joining us. It is recommended to prove yourself immediately after joining - the sooner you get the first payment, the less doubt will be cast on your identity.
6. It is desirable to have already downloaded information for the blog from the intended target for the attack and provide evidence of the existence of this information, such as screenshots, file tree or access to these files.
7. Ask your friends or acquaintances who already work with us to vouch for you.
8. Request a bitcoin or monero wallet to **make a deposit**, in case you are confident in your abilities and ready to earn millions of dollars with us.

We do not audit

next categories of organizations



Hospitals

Except private plastic surgery clinics, private dental clinics



Non-Profit

Any non-profitable charitable foundation



Schools

Except the major universities



Small Business

Companies with annual revenue less than 4 mln\$ (info about revenue we take from zoominfo)

RULES

We do not audit

next categories of organizations



Hospitals

Except private plastic surgery clinics, private dental clinics



Non-Profit

Any non-profit charitable foundation

Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

We do not audit

next categories of organizations



Hospitals

Except private plastic surgery clinics, private dental clinics



Non-Profit

Any non-profit charitable foundation

Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

sickkids.ca

We formally apologize for the attack on sickkids.ca and give back the decryptor for free, the partner who attacked this hospital violated our rules, is blocked and is no longer in our affiliate program.

<http://lockbitfile2tcudkcqqt2ve6btssyvqwlizbpv5vz337lslmhff2uad.onion/r/n2JhJ1SdnB#JjXDyRUIUIb7Gg3PNIGtI5zJGPOdacCVtW6lMytOd80=>

ALL AVAILABLE DATA PUBLISHED !



Figure 1: Top Threat Groups for Ransomware-as-a-Service Ecosystem



VENDOR RANKING

INNOVATION ABILITY

AS OF MARCH 2023

Source: Halcyon (March 2023)



WAR STORIES

Inside an incident



Initial Compromise

Lateral Movement

Encryption

Reconnaissance

Exfiltration

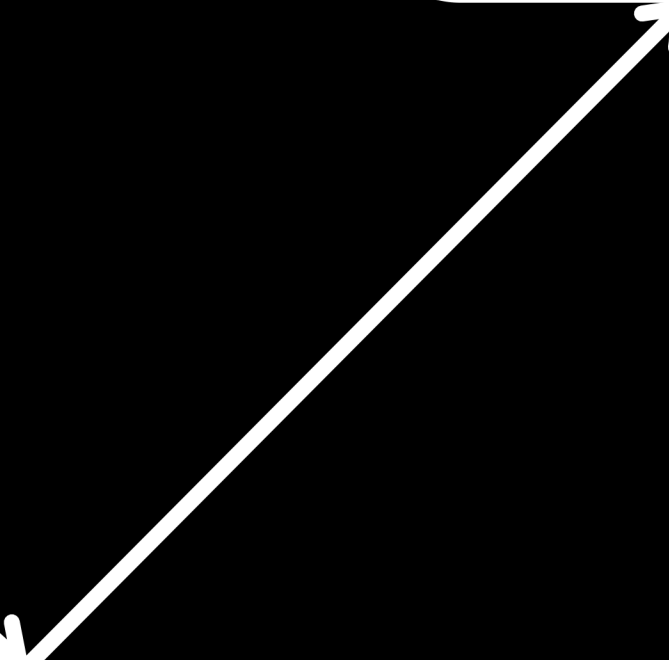
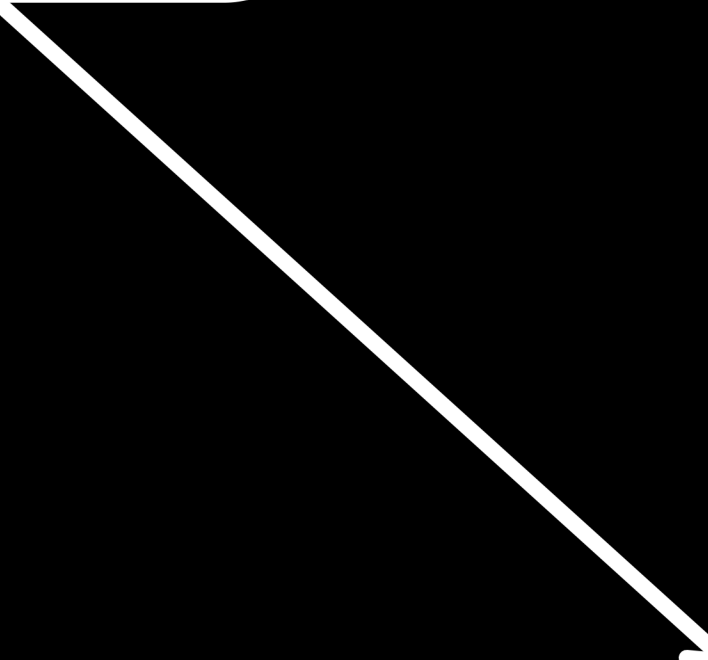
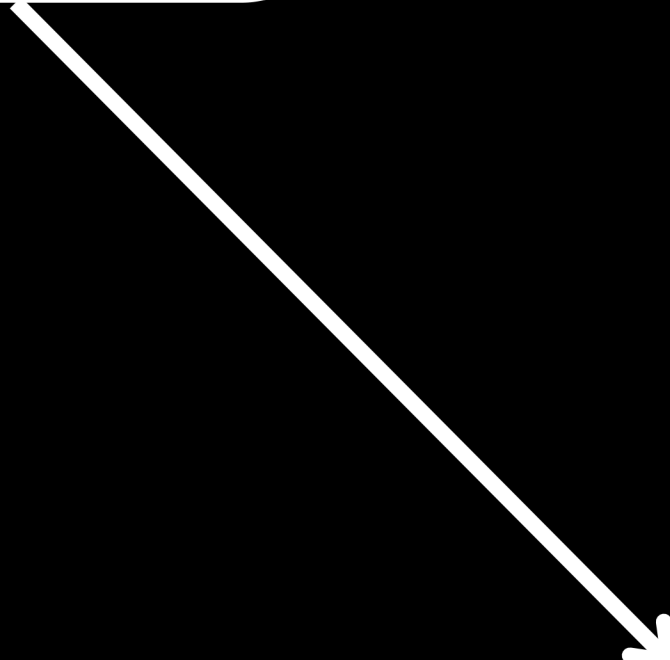




Photo by [Pablo Merchán Montes](#) on [Unsplash](#)

personal files

Datei Start Freigeben Ansicht

Navigationbereich Bereiche

Layout

Extra große Symbole Große Symbole
Mittelgroße Symbole Kleine Symbole
Liste Details

Aktuelle Ansicht Ein-/ausblenden Optionen

← → ▾ ↑ > Dieser PC > Dokumente > personal files

personal files durc...

Name	Änderungsdatum	Typ	Größe
Approval Guidelines CISO Organisation.pptx.fgn9c24	12.02.2022 11:16	FGN9C24-Datei	4.925 KB
Default.rdp.fgn9c24	28.11.2021 20:02	FGN9C24-Datei	3 KB
Deutschland 2020 - 4.docx.fgn9c24	16.11.2021 21:42	FGN9C24-Datei	3.394 KB
Ergebnisse Softwareaudit.pptx.fgn9c24	16.02.2022 01:16	FGN9C24-Datei	6.781 KB
GesaSlides20211001a FOD.pptx.fgn9c24	01.10.2021 11:04	FGN9C24-Datei	3.018 KB
RECOVER-fgn9c24-FILES.txt	07.02.2023 21:53	Textdokument	2 KB
Strategie 24 26.pptx.fgn9c24	07.04.2022 19:04	FGN9C24-Datei	49 KB

7 Elemente

YOU ARE
ENCRYPTED

RANSOMNOTE

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorhythm.

Backups were either encrypted or deleted or backup disks were formatted.

We exclusively have decryption software for your situation.

DO NOT RESET OR SHUTDOWN - files may be damaged.

DO NOT RENAME the encrypted files.

DO NOT MOVE the encrypted files.

This may lead to the impossibility of recovery of the certain files.

To get info(pay-to-decrypt your files) contact us at:

██████████@protonmail.com

or

██████████@tutanota.com

BTC wallet:

To confirm our honest intentions.

Send 2 different random files and you will get it decrypted.

It can be from different computers on your network to be sure we decrypts everything.

Files should have .LOCK extension of each included.

2 files we unlock for free.

Your network was compromised.

Important files on **your network** was **downloaded** and **encrypted**.

Our custom **Decrypt App** is capable of **restoring** your **files**.

In order to buy it you have to follow **Instructions** below. If you have questions please feel free to use **Live-Chat**.

Act quickly to get a **Discount!**

Decrypt App Price

You have **5 days, 05:42:12** until:

- **Decrypt App** special discount period will be discontinued.
- **Discount Price** is available until **2/1/22, 6:02 AM**

Discount Price: **\$9000000**

Full Price: **\$14000000**

Status

Awaiting payment of **\$9000000** to one of the following wallets:



Bitcoin

[Redacted Bitcoin address]

Monero

[Redacted Monero addresses]

Instructions

Live-Chat

Trial Decrypt

Intermediary

I wish to pay with
Bitcoin



1. Create a Bitcoin Wallet.

14M USD

Egregor News - Delta fire prote X Support chat X

egregor4u5ipdzhv.onion

Instructions Buy bitcoins

To recover your data and prevent leakage to public, you must pay in bitcoins.

Your current price must be discussed in chat.

Contact us in chat and we give you further details.

The information on how to buy bitcoins is written under the [Buy Bitcoins](#) tab.

Support chat

13:27:24 20-10-2020 You

file: RECOVER-FILES.txt

Support 13:56:23 20-10-2020

Please introduce your company's name.

Type a message

Upload file SEND

COMPANY NAME?

PROOF

Thanks for your information so far. We take your action seriously and would like to discuss further steps with you. To be able to evaluate the data you have downloaded, we ask you to send us some data examples. Regards

PROOF

Your filelist

▼ Von: [REDACTED]

1 Anhang:



[REDACTED] filelist.7z

[REDACTED] Thanks for your information so far. We take your action seriously and would like to discuss further steps with you. To be able to evaluate the data you have downloaded, we ask you to send us some data examples. Regards

NO PROOF?

Good afternoon, yet we cannot provide, the person who has access to data - does not contact for the reasons unknown to us. But it already was, I think will appear in the nearest future.

NO PROOF?

Good afternoon, yet we cannot provide, the person who has access to data - does not contact for the reasons unknown to us. But it already was, I think will appear in the nearest future. You can send files for test interpretation. Did you estimate mashtaba? how to you?



vx-underground  @vxunderground · 8. Juli


Earlier this morning we spoke with Lockbit ransomware group administrative staff. We asked why there has been a significant decrease in victim postings and blog activity.

They informed us they're currently on holiday and enjoying the nice summer weather.

~_(\ツ)_/

 34

 212

 1.285

 157.135



VACATION



vx-underground  @vxunderground · 8. Juli

Earlier this morning we spoke with Lockbit ransomware group administrative staff. We asked why there has been a significant decrease in victim postings and blog activity.

They informed us they're currently on holiday and enjoying the nice summer weather.

~_(\ツ)_/

 34  212  1.285  157.135 

VACATION

Make a decision faster, our team is going on vacation

> On 2022-10-11 15:27, kluke01 wrote:
>> bro , how to decrypt and how much ?
>>
>> Please contact: volkzidonov@cock.li
>> spare email: volkzidonov@morke.org
>> Your identity code: XdM5FGoro1Tj
>>
>> kluke01
>>
>> kluke01@126.com

NEGOTIATION

NEGOTIATION

> On 2022-10-11 15:27, kluke01 wrote:
>> bro , how to decrypt and how much ?
>>
>> Please contact: volkzidonov@cock.li
>> spare email: volkzidonov@morke.org
>> Your identity code: XdM5FGoro1Tj
>>
>> kluke01
>>
>> kluke01@126.com

On 2022-10-11 19:45, volkzidonov@cock.li wrote:

> Dear
> First of all, thank you for contact us, we're sorry to attack your
> company, we are a mature and integrity team. We hope to reach an
> agreement with you with the fastest speed to solve this case. If you
> have any questions, you can tell us, we are willing to communicate
> with you with the greatest sincerity.
> Please buy \$510,000(usd) worth of ETH to send to our wallet address.
> ETH address:0x282dC843E849914082Ec54c494a6D65738568979
> After we receive ETH, I will send all the passwords to you.We randomly
> generate a password for each server, each password is only taken
> effect on one server. AES encryption is the most advanced encryption
> algorithm in the world, without anyone can crack. Even the US FBI and
> the Ministry of Defense cannot be decrypt. Please don't try scan disk
> or recovery. This will make data damage, once the data is damaged,
> even if you pay the ETH, I can't restore the data. Data will be
> permanently lost.
>
> In addition, we will provide you with test password. Decrypt software:
> C:\crypt\bcbmgr.exe
> Select the volume and click "decrypt volume". Enter the password to
> decrypt.
>
> SERVER-TEST-005 192.168.12.130 abcdefgh
> VMWARE_99-2021 192.168.12.132 E:\ abcdefgh
> KLZSRV32-TEST 192.168.12.155 abcdefgh
> KLZSRV19 192.168.12.54 abcdefgh

NEGOTIATION

> On 2022-10-11 15:27, kluke01 wrote:
>> bro , how to decrypt and how much ?
>>
>> Please contact: volkzidonov@cock.li
>> spare email: volkzidonov@morke.org
>> Your identity code: XdM5FGoro1Tj
>>
>> kluke01
>>
>> kluke01@126.com

Gesendet: Montag, 13. Oktober 2022 um 16:19 Uhr
Von: volkzidonov@cock.li
An: mailadresse@corporate-trust-verhandlungsteam
Betreff: Re: help

I have reply.

On 2022-10-11 19:45, volkzidonov@cock.li wrote:

> Dear
> First of all, thank you for contact us, we're sorry to attack your
> company, we are a mature and integrity team. We hope to reach an
> agreement with you with the fastest speed to solve this case. If you
> have any questions, you can tell us, we are willing to communicate
> with you with the greatest sincerity.
> Please buy \$510,000(usd) worth of ETH to send to our wallet address.
> ETH address:0x282dC843E849914082Ec54c494a6D65738568979
> After we receive ETH, I will send all the passwords to you.We randomly
> generate a password for each server, each password is only taken
> effect on one server. AES encryption is the most advanced encryption
> algorithm in the world, without anyone can crack. Even the US FBI and
> the Ministry of Defense cannot be decrypt. Please don't try scan disk
> or recovery. This will make data damage, once the data is damaged,
> even if you pay the ETH, I can't restore the data. Data will be
> permanently lost.
>
> In addition, we will provide you with test password. Decrypt software:
> C:\crypt\bcbmgr.exe
> Select the volume and click "decrypt volume". Enter the password to
> decrypt.
>
> SERVER-TEST-005 192.168.12.130 abcdefgh
> VMWARE_99-2021 192.168.12.132 E:\ abcdefgh
> KLZSRV32-TEST 192.168.12.155 abcdefgh
> KLZSRV19 192.168.12.54 abcdefgh



The money, even with the 20% discount, is unfortunately over our financial possibilities. We have heard that in other cases 10% of the EBIT of the last years is paid. The EBIT of the last 3 years for ██████████ Holding was 4.8 ██████████ \$. We can send you the balance sheet data if you would like to see it. This gives a total of \$484,000. That's the maximum because we can't make any sales because of your cyber attack.

NEGOTIATION

You, 10:48



The money, even with the 20% discount, is unfortunately over our financial possibilities. We have heard that in other cases 10% of the EBIT of the last years is paid. The EBIT of the last 3 years for ██████████ Holding was 4.8 ██████████ \$. We can send you the balance sheet data if you would like to see it. This gives a total of \$484,000. That's the maximum because we can't make any sales because of your cyber attack.



Basta Group, 11:11

No need to tell us Wilhelm Hauff's fairy tales. Our analytical department analyzed your financial documents and appointed the amount you are able to pay without any problems. Therefore, our price is \$880,000. You have 3 days to make the payment. After that, our price will be \$1,100,000 again.

NEGOTIATION

NEGOTIATION

We decrypt a lot of companies every day and we don't want to waste time. Your order is a very little business. We don't care much. So, if you want to get the password, then pay for it, if not, just ignore it, no need to contact us.



Toxing on qTox



I can sell a decoder that will decrypt all your files.

20:10:27

It costs 0.16 BTC

Payment is accepted only in bitcoins.

You can send me 2-3 files for free decryption, the files should not contain valuable information - it's just a way to prove that the decoder works and is able to recover files without data loss.

20:10:27

I also want to warn you that after 2 days, the price of buying a decoder will increase by \$100 every day.

20:32:15

NEGOTIATION

Support: In September we sent you an email containing the exploits in the attached document.

It was opened by a user with citrix access [REDACTED] password [REDACTED]. Then, using the CVE-2020-0796 vulnerability, rights were raised to the local administrator. After that, using the program Blood Hound were found computers where there are authorization data domain administrators.

The computer was found, we were able to get access to it and spread the network. We found local administrator computers where passwords to different resources were stored in the open. We found out where there were backups, SQL, etc. Then we found the local computers of your domain administrators. With the help of mimikatz, passwords of administrators on these computers were obtained. Going to the RDP on them, we found Key Pass programs from where we got access to your AV server.

Support: Our advice to you. Put a server in the domain that will download daily updates from Microsoft. And once a week or twice a week, distribute updates from this server to all computers and servers on your network. Thus, in the future you will protect your network from known public vulnerabilities. Also install Kaspersky or Sentinel antivirus. Make it a rule to change all important passwords once a month. Tell your administrators to turn off their local computers when they go home.



Support: In September we sent you an email containing the exploits in the attached document.

It was opened by a user with citrix access [redacted] password [redacted]. Then, using the CVE-2020-0796 vulnerability, rights were raised to the local administrator. After that, using the program Blood Hound were found computers where there are authorization data domain administrators.

The computer was found, we were able to get access to it and spread the network. We found local administrator computers where passwords to different resources were stored in the open. We found out where there were backups, SQL, etc. Then we found the local computers of your domain administrators. With the help of mimikatz, passwords of administrators on these computers were obtained. Going to the RDP on them, we found Key Pass programs from where we got access to your AV server.

Support: Our advice to you. Put a server in the domain that will download daily updates from Microsoft. And once a week or twice a week, distribute updates from this server to all computers and servers on your network. Thus, in the future you will protect your network from known public vulnerabilities. Also install Kaspersky or Sentinel antivirus. Make it a rule to change all important passwords once a month. Tell your administrators to turn off their local computers when they go home.



Support: In September we sent you an email containing the exploits in the attached document.

It was opened by a user with citrix access [redacted] password [redacted]. Then, using the CVE-2020-0796 vulnerability, rights were raised to the local administrator. After that, using the program Blood Hound were found computers where there are authorization data domain administrators.

The computer was found, we were able to get access to it and spread the network. We found local administrator computers where passwords to different resources were stored in the open. We found out where there were backups, SQL, etc. Then we found the local computers of your domain administrators. With the help of mimikatz, passwords of administrators on these computers were obtained. Going to the RDP on them, we found Key Pass programs from where we got access to your AV server.

Support: Our advice to you. Put a server in the domain that will download daily updates from Microsoft. And once a week or twice a week, distribute updates from this server to all computers and servers on your network. Thus, in the future you will protect your network from known public vulnerabilities. Also install Kaspersky or Sentinel antivirus. Make it a rule to change all important passwords once a month. Tell your administrators to turn off their local computers when they go home.



Support: In September we sent you an email containing the exploits in the attached document.

It was opened by a user with citrix access [redacted] password [redacted]. Then, using the CVE-2020-0796 vulnerability, rights were raised to the local administrator. After that, using the program Blood Hound were found computers where there are authorization data domain administrators.

The computer was found, we were able to get access to it and spread the network. We found local administrator computers where passwords to different resources were stored in the open. We found out where there were backups, SQL, etc. Then we found the local computers of your domain administrators. With the help of mimikatz, passwords of administrators on these computers were obtained. Going to the RDP on them, we found Key Pass programs from where we got access to your AV server.

Support: Our advice to you. Put a server in the domain that will download daily updates from Microsoft. And once a week or twice a week, distribute updates from this server to all computers and servers on your network. Thus, in the future you will protect your network from known public vulnerabilities. Also install Kaspersky or Sentinel antivirus. Make it a rule to change all important passwords once a month. Tell your administrators to turn off their local computers when they go home.



NB [REDACTED] 44.12 Windows Server 2019 Standard
HA [REDACTED] 214.12 Windows Server 2019 Standard
KI [REDACTED] 114.12 Windows Server 2019 Standard
HH [REDACTED] Windows 2000 Server
PS [REDACTED] 16.47 Windows Server 2003
PS [REDACTED] 16.48 Windows Server 2003
HH [REDACTED] Windows Server 2003
PS [REDACTED] 16.107 Windows Server 2003
BW [REDACTED] Windows Server 2003
EA [REDACTED] Windows Server 2008 HPC Edition
H0 [REDACTED] Windows Server 2008 R2 Enterprise

PROOF OF DELETION

Support: Is it ok for you that we will use this program <https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete> to delete files from our server. After deletion we will provide you proof log?



Support: We will provide both reports in 1-2 days. We need some time to proceed with them.



Support: deletion log

<https://www.sendspace.com/file>

<https://www.sendspace.com/delete>



HOW TO STAY SAFE

What you can do to avoid a
ransomware incident.

PREVENT

REACT

PREVENT

Patching

REACT

PREVENT

Patching

Hardened Infrastructure



REACT

PREVENT

Patching

Hardened Infrastructure

REACT

Emergency Preparedness



PREVENT

Patching

Hardened Infrastructure

REACT

Emergency Preparedness

Backups



PREVENT

Patching

Hardened Infrastructure

REACT

Emergency Preparedness

Backups

Visibility





GEBHARD@CORPORATE-TRUST.DE

WWW.LINKEDIN.COM/IN/SEBASTIAN-GEBHARD/