

# RansomOps

How to run a RaaS



# ~~whoami~~ GetUserNameA (lpBuffer, pcbBuffer)

- DFIR nerd
- SecTalks SYD
- Muai Thai
- eCrime (investigation) enthusiast



# Thoughts are my own

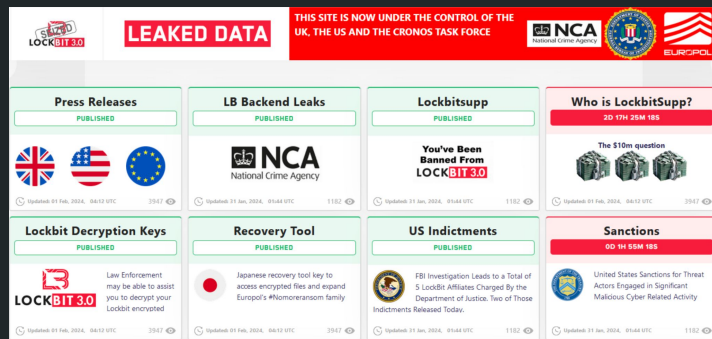
- Not a ransomware operator
- Not giving career advice, not a “how do I break into infosec” talk
- Content is based on leaks/research from/on ransomware operators and affiliates
- I will speak in first/second person at times for added effect
- Attributions to individuals, countries and agencies is based on publicly available analysis and research

*If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle*

*Sun Tzu*

# RaaS is just another XaaS (-crime)

- Share the same challenges as other IT businesses  
(+chances of the door being kicked in)
  - Hiring is hard
  - Performance is not consistent
  - Running costs are high (60k for a 30k CS license)
  - Work is not always interesting
- High level of distrust
- Competitive space



# Why is ransomware (still) so popular?

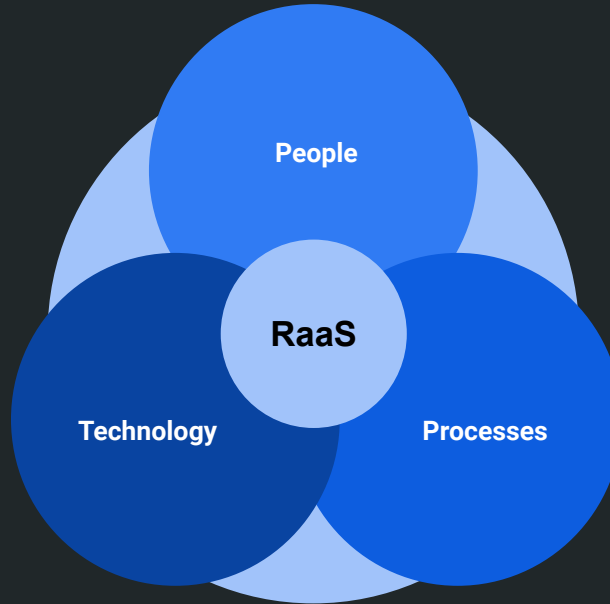
- Still the most profitable eCrime
  - Avg. 1.5m payout in 2023 (Avg. 1.8m recovery cost)
  - 'There is no such money anywhere as there is in ransomware'  
-Mikhail Matveev (Wazawaka)
- Reliable business model
  - 55% payout from revenue >\$5b
  - 36% payout <\$10m
- Federated structure
- Scalable
- Large attack surface
- It's fairly "safe"
- Opportunities in supply chain



# RansomOps

- Reporting
- Affiliates
- Time Tracking
- Training
- Issue Tracking
- OpSec
- Recruitment
- Payroll

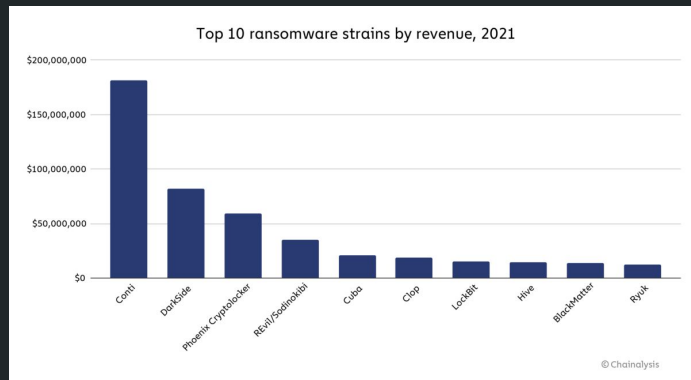
- Domains
- VM
- VPS
- C2
- Scripts
- Emails
- VPN
- Locker
- Loader
- Decryptor
- Admin Panel



- Dev
- QA
- AV testing
- Dynamic analysis
- IABs
- Negotiation
- Recon
- Support
- Documentation
- Pentesting

# Rise and fall of Conti

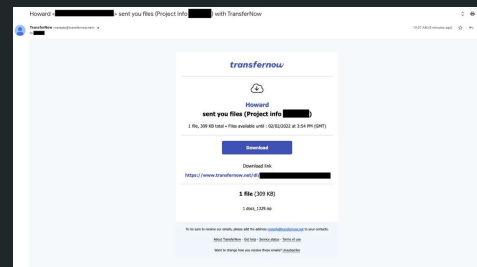
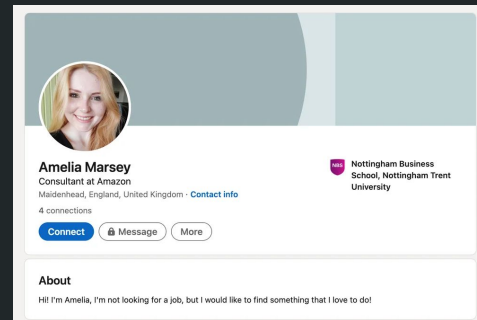
- Once the most successful ransomware operator
- ~\$180m revenue in 2021
- Close ties with the FSB
- Leaks by @contileaks in March 2022
- Shut down in May 2022
- Members sanctioned by DoJ in September 2023





# IABs

- Great value for money (avg. \$2800 for access)
- Types of access
  - Remote Desktop Protocol (RDP)
  - Active Directory (AD)
  - VPN
  - Server Root Credentials
  - Web Shell Access
  - Remote Monitoring & Management (RMM)
  - Control Panels
- Some operators buy directly from employees




## We monetize your corporate access

Team looking for corporate accesses (shell, vnc, hvmc, rdp + vpn, teamviewer, anydesk etc.) Us Countries, Ca and Europe. A good percentage for partners, full transparency of work and confidentiality  
tox:A0E79CB8D18DDA358665BEB91360B79CFCD54040EAD  
197147F1EBAB92DC64D71909CA9E64C  
jabber:everestgroup@exploit.investgroup@thesecure.biz  
email:everestblog@cock.li

# IABs

- **Stealers/loaders**
  - AZORult
  - Racoon
  - Redline
  - Bazar
  - Bumblebee
  - Vidar
- **Markets**
  - Russian Market
  - Genesis 🚒
  - xss
  - Raid 🚒
  - RAMP
  - lolz
- **Sellers**
  - wazawaka
  - fooble
  - pshmm
  - 7h0rf1nn
  - BadMonkey
  - 3lv4n



7h0r1nn

Пользователь

Joined: Nov 3, 2020

Messages: 5

Reaction score: 0

Jan 2, 2021

Corporation name: <REDACTED>

Type: BANKS

I am selling access to 2 banks, one in Poland and the other in France, they have several subnets on the intranet so with a good pivoting I would be able to retain various information, we also do pivoting services in the banks if they pay us more!

Bank access from Poland: 1500 \$ ( RCE )

Access to a bank From France: 1200 \$ ( RCE )

-----

Price of the two banks together is \$ 2000

for pivoting services, etc. they have to be negotiated privately. (I accept escrow tool)

I do not access Telegram or other platforms, only XMPP and by email.

Be direct in negotiation.

To buy contact me at: 0601104640662@protonmail.com

My XMPP: 7h011n@xmpp.7h011n.com

Backdoor

Dashboard

Groups

Administrators

Rules

Programs

Hosts

Programs

Plugins

Networks

Network Activity

Tools

Files

Groups

Proxies

Reports

**bots**

Command Builder

Advanced search options

Auto Refresh

142,046 / 8,700 items

Command Builder

Autorefresh of: 1 2 3 4 5 6 7 8 9 10 15 20 30 45 60 90 120 150 180 210 240 270 300 330 360 390 420 450 480 510 540 570 600 630 660 690 720 750 780 810 840 870 900 930 960 990 1020 1050 1080 1110 1140 1170 1200 1230 1260 1290 1320 1350 1380 1410 1440 1470 1500 1530 1560 1590 1620 1650 1680 1710 1740 1770 1800 1830 1860 1890 1920 1950 1980 2010 2040 2070 2100 2130 2160 2190 2220 2250 2280 2310 2340 2370 2400 2430 2460 2490 2520 2550 2580 2610 2640 2670 2700 2730 2760 2790 2820 2850 2880 2910 2940 2970 3000 3030 3060 3090 3120 3150 3180 3210 3240 3270 3300 3330 3360 3390 3420 3450 3480 3510 3540 3570 3600 3630 3660 3690 3720 3750 3780 3810 3840 3870 3900 3930 3960 3990 4020 4050 4080 4110 4140 4170 4200 4230 4260 4290 4320 4350 4380 4410 4440 4470 4500 4530 4560 4590 4620 4650 4680 4710 4740 4770 4800 4830 4860 4890 4920 4950 4980 5010 5040 5070 5100 5130 5160 5190 5220 5250 5280 5310 5340 5370 5400 5430 5460 5490 5520 5550 5580 5610 5640 5670 5700 5730 5760 5790 5820 5850 5880 5910 5940 5970 6000 6030 6060 6090 6120 6150 6180 6210 6240 6270 6300 6330 6360 6390 6420 6450 6480 6510 6540 6570 6600 6630 6660 6690 6720 6750 6780 6810 6840 6870 6900 6930 6960 6990 7020 7050 7080 7110 7140 7170 7200 7230 7260 7290 7320 7350 7380 7410 7440 7470 7500 7530 7560 7590 7620 7650 7680 7710 7740 7770 7800 7830 7860 7890 7920 7950 7980 8010 8040 8070 8100 8130 8160 8190 8220 8250 8280 8310 8340 8370 8400 8430 8460 8490 8520 8550 8580 8610 8640 8670 8700 8730 8760 8790 8820 8850 8880 8910 8940 8970 9000 9030 9060 9090 9120 9150 9180 9210 9240 9270 9300 9330 9360 9390 9420 9450 9480 9510 9540 9570 9600 9630 9660 9690 9720 9750 9780 9810 9840 9870 9900 9930 9960 9990 10020 10050 10080 10110 10140 10170 10200 10230 10260 10290 10320 10350 10380 10410 10440 10470 10500 10530 10560 10590 10620 10650 10680 10710 10740 10770 10800 10830 10860 10890 10920 10950 10980 11010 11040 11070 11100 1113

# Affiliates

- Access to stealers, loaders/droppers, builder, decryptor, admin/chat panel, leaks blog, helpdesk
- No critical infrastructure or healthcare (unless they're \$\$ rich), no friendly fire
- Exfil without locking is an option
- Commission is ~20%
- Split wallet payments
- Vetting done through wallet balance checks, forum reputation, past work/payments, current access, references

# Affiliates

CONTI.Recovery Chats 20:26 bio1

Status 

All active

 Search 

Apply filter

ID	Domain	OP	Status	Updated at
ybdIfd1mzTBPYo5dyj6jZxMmDtmfJ10F4NuyOpQSiAJmHsITJGMe570USnFTRSM	WINNAVEGAS	icen	Wait answer	22 hours ago
UZeMXpgTHd6cxJuArkXwHbRhLIAcG6hyZh70FwZuoqJ4EvbthDZETNIM8mu8H	LAVI	icen	Replied	5 days ago
PDUJTpuDovNaXeb01e2bZRldfXH8QTreggpulWu03Hd9w2hAHpldLxOtoYoQhFo	RLDASSOC	icen	Replied	6 days ago
Hgdna5MEV4lZYJltPQyquzEOJ06BRPHtUmfDYSVVj67ZYXQD3MaUpPaZGgJl	TRANZ	icen	Wait answer	7 days ago
otcpa5UckEz6hoEa7hld1fY2OLmo2s84PrqgJrHRSAWaYR6Z4LzSLqfHza3fn8	AEE	icen	Replied	15 days ago
O34WUyhBhw4cb4dUR8NtbZULwX5LuE3CUZtbLMZUh2p8wcbKsIPcV7hTcQaDr	TCEC	icen	Replied	20 days ago

CONTI.Recovery Chats 21:58 bio1

Chat created  
System message 2 days ago

OP

Created at  
2 days ago

Updated at  
2 days ago

Online at  
2 days ago

Name

Email

Domain  
@example.com

Comment  
@example.com  
27 min  
1000x1000  
30%

SEND

bio1@winnavegass.com

System message 2 days ago

OP

Created at  
2 days ago

Updated at  
2 days ago

Online at  
2 days ago

Name

Email

Domain  
@example.com

Comment  
@example.com  
27 min  
1000x1000  
30%

SEND

CONTI Recovery service

Please help to decrypt our network.  
3 minutes ago

bio1

bio1

Hello please wait.  
2 minutes ago

bio1

Hello, this is Conti Team.  
If you are here, you want to know what happened.  
We estimated your network, controlled it for a while, examined your data, downloaded sensitive information and finally encrypted your computers.  
Your files are safe, but encrypting. Any attempt to decrypt files with third-party software will permanently corrupt content.  
What now?  
We advise you to be in touch and start negotiations, otherwise your confidential data will be published on few our news sites and promoted in all possible ways.  
Data publication and even the fact of this talk for sure will lead to significant losses for your company - government fees, lawsuits and as a result legal claims payments, additional expenses on law services and data recovery etc.  
Also you shouldn't underestimate huge damage for your reputation, which can cause crash of equity prices, clients withdrawal and other negative consequences.  
But don't panic! We are doing business, not war.  
We can unlock your data and keep everything in secret. All, what we want is a ransom. The amount is 600,000 USD.  
If we can reach an agreement, you also get security report, full file tree of compromised data, downloaded data unrecoverable deletion, support with unlocking and network protection advice.

bio1

We can give you few random files from your data. Please wait.  
3 minutes ago

bio1

We need a complete file tree of the stolen data. We do not believe you because we have read many articles about COPE.  
3 minutes ago

bio1

Full file tree of the stolen data you can see only after payment.  
3 minutes ago

bio1

How much data has been downloaded and what is their structure?  
3 minutes ago

bio1

At least 150 GB of your data downloaded to our secure servers.  
We have financial documents, tax forms, contracts with full information, emails, staff data, etc.  
3 minutes ago

Create Locker

Identifier

Unique Identifier for your stub

Amount (BTC)

17

Persistence Type

Persistence  
Use the original built-in persistence.  
This will protect your stub against unexpected shutdowns, as well as save the state of the encryption to continue later on.

Watchdog™  
Use the SmartLocker WatchDog™ exploit which will inject a system process with malicious code, that will protect the locker from being killed by an AV or by the user.

Directories to encrypt

Mode

C:/Users/Jack/Documents;C:/Users/Jack/Desktop

Manual

If you're using SmartCrypt mode, you can leave the directory input box empty.

Kill Processes

Kill Services

chrome.exe paint.exe

wuauclt spooler

Run Commands on Execution

taskkill /f /im rofl.exe

Delay

5

UAC Bypass Attempt

Remove Background

Enabled

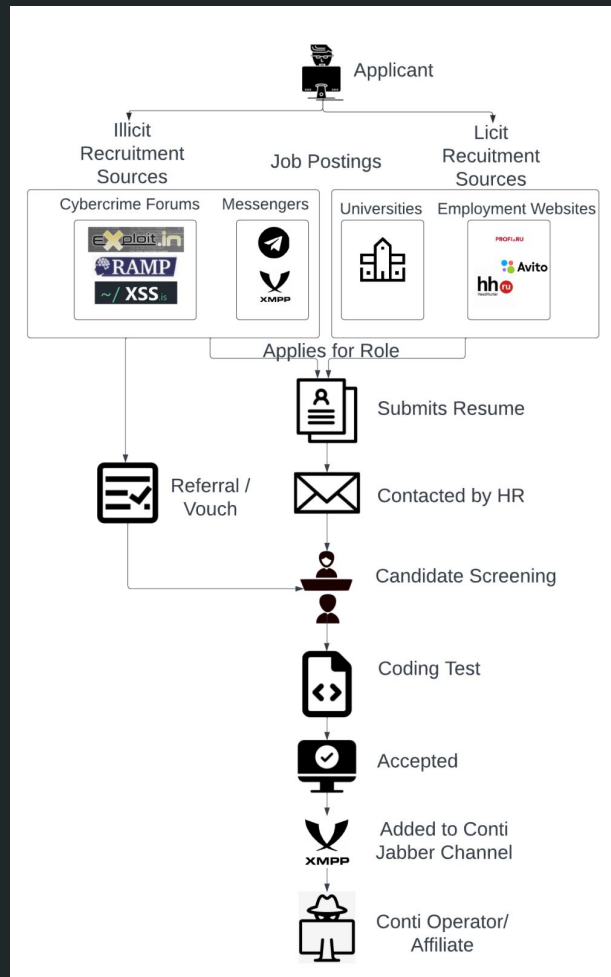
Enabled

Cancel

Compile Locker

# Recruitment

- Working hrs 09:00-18:00
- Remote working allowed
- Paid fortnightly (btc or bank)
- Unpaid/reduced pay probation
- Roles advertised
  - C++ Programmer (with reverse engineering skills)
  - Full-stack web developer for PHP, NodeJS
  - Windows System Administrator
  - Data Analyst
  - Business Analyst
  - UI/UX Designer
  - HTML Designer
  - Pentester
  - Phone operators



# Roles/hats

- HR
- Tech Lead (malware devs, QAs)
- Task Manager (Engineering Manager)
- General Manager (Team lead/supervisor)
- Developer (admin panel, general dev)
- Pentester
- Crypter (Locker dev)
- Negotiator
- QA
- Infrastructure/sysadmin

## Candidate - C++/C# programmer (Salary expectation RUB70k / AUD1100 per month)

August 2017 —October 2017	Forest, LLC Beloretsk, <a href="http://www.for-est.ru">www.for-est.ru</a> Information systems developer Development of information systems for automating business processes
September 2014 —July 2017	Uralmetindustry LLC Beloretsk Automated process control system software engineer Construction of automatic weighing systems, implementation, commissioning
March 2012 —September 2014	Energotekhservis, LLC <a href="http://tmenergo.ru">tmenergo.ru</a> programmer Development of a dispatch system for heat metering of residential buildings A dispatch system for 120 metering nodes was built based on a wi-fi network deployed in a residential complex Software was developed for <b>tibbo controllers</b>
January 2008 —January 2010	Magnitogorsk Iron and Steel Works, OJSC Magnitogorsk, <a href="http://mmk.ru/">mmk.ru/</a> <b>lead engineer programmer</b> Development of 1st and 2nd level automated process control software, communication interfaces, process visualization systems. Industrial and Ethernet network services
January 1999 —January 2003	Beloretsk Metallurgical Plant, OJSC engineer programmer Software development for level 1 <b>automated process control systems, industrial communication interfaces</b>
Education	1993 Ufa State Aviation Technical University, Ufa Faculty of Aviation Instrumentation, Information and Measuring Equipment and Technologies
Skills	Knowledge of <b>scada systems</b> and basic protocols Knowledge of tibbo controllers Knowledge of C# Knowledge of C++ Software development for tibbo controllers  Features of building systems and visualization systems for process control systems of any level, <b>industrial controllers, microcontrollers</b> . Complete knowledge of Windows OS families. UNIX and related software. Complete knowledge of PC repair and maintenance. Learning abilities: Capable of developing automation systems and software from scratch.

# Transparency is optional

Yes, I don't even know the purpose of this software

as if with a trick, you definitely drove half the world through servers)) and what did you mean by that?

Well, they're just collecting something .. I don't know) my job is to accept it and put it in the database .. I don't know what it does

I mean the same thing, they collect analytics

come on, analytics)

well there's a bunch of data going through it)

for advertising))))



# Conti Salaries (monthly)

- OSINT - \$2200
- Project manager - \$2000
- Research - \$2000
- Reverse engineering - \$1400-\$2000
- Dev - \$1300-\$1800
- Probation - \$1000
- Testers - \$800-\$1200

## Conti managers' gross pay

- tramp - \$1.2M
- mango - \$470K
- baget - \$400K
- bullet - \$280K
- andy - \$98K

# Management

- Everything is about results, you are allowed to break any rule for achieving them
- Always ask “Why do we need it? What benefits will it bring”?
- Magic practices from the IT world (scrums, standups etc.) don’t work, think critically and apply only what works
- You can hire someone to write code, buy or steal

# Culture

- Friendly environment, there are rewards and punishments
  - Employees of the month
  - Bonuses and fines
- Be kind, people are different, when you encounter stubbornness and misunderstanding, you will need great patience
- Be firm when needed, but also commend people to raise their self esteem
- If a tech lead fires someone because they can't cope, this is a minus for them
- It's a plus if they get someone to learn to work together
- Leads should highlight the qualities and strengths of a person

# Coding

- Simplicity
  - Don't make plans for years to come, don't write what's not needed
  - Use someone else's code as much as you can (ideal code should occupy 0 bytes)
- Consistency:
  - Commits are required everyday, even if the code is not complete and does not work, it's better than losing your job in a day (people are fired without notice)
  - Indicate the number of the bug or task from ticketing system, so it gets linked to the ticket
- Clarity
  - Explain intentions with detailed comments, not only "what and how", but "why"
  - A commit should always have a comment in Russian, describing a brief summary of the changes. It should
- Security
  - Public/exposed code should not indicate your nationality
  - Forbidden to commit, any texts with real names, nicknames, passwords, URLs and IP addresses of our resources, wallets etc. or any archives or binaries not part of the project's build steps



# Training

- In person
  - Induction
  - Malware hunting
  - Building crypters
  - BazarLoader
  - Testing and automation
- Self paced
  - Windows Red Team Lab
  - Powershell for Pentesters
  - GCB Cyber Range
  - Cobalt Strike
  - GeekBrains Reverse Engineering



# Tools (>\$3m/year)

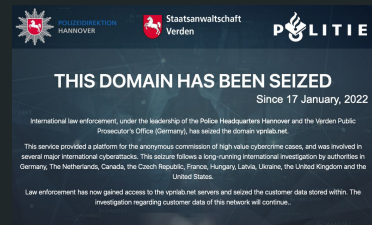
- Redmine/Jira
- VoIP (support)
- Mail (spam)
- VPN
- VMWare
- VPS (Burning through heaps of C2s)
- ZoomInfo
- Crunchbase
- AnyDesk
- Ngrok
- Cobalt Strike
- Metasploit
- RClone
- Dyncheck
- ...

VPS DAY



bacloud

HOSTSAILOR



# Transactions

- Exchange - no KYC
- DEX
- Bridges
- Dealers club packs (debit + creds + ID)





# OpSec

- Anonymous browsing all the time
- Different personalities for different activities, no unique handles, learn to invent names and biographies
- **Use different handles in social networks, at work or in other places**
- Don't stand out on social media, don't post data, photos, addresses, phone numbers etc. If you really need to do it, it should be only under a pseudonym
- Run the built files only in a VM with a configured rollback point
- Check unknown files on services like VirusTotal, including documents
- Test yourself on whoer.net, what do you look like to analysts

Member of the hacker group "TRICKBOT"  
(also known as the Wizard Spiders)  
"Ryur", "Maze", "Conti", "Diavol")

Account (nicknames): zulas



Citizen of the Russian Federation  
Name: **Sergey Loguntsov**  
Date of birth: **July 15, 1983**

Lives in St. Petersburg, Russia  
Mobile phone number: [REDACTED]

Telegram:  
Telegram-ID: [REDACTED]  
Username: @loguntsov

Skype: begemot\_sun;

Jabber: zulas@q3mcco35auwcstmt.onion  
Jabber: begemot\_sun@jabber.ru

Social networks:  
- <https://ru.linkedin.com/in/sergey-loguntsov-b104b652>  
- <https://www.gitmemory.com/loguntsov>  
- [https://habr.com/ru/users/begemot\\_sun/](https://habr.com/ru/users/begemot_sun/)  
- <https://www.youtube.com/user/begemotsun>  
- <https://vk.com/id174832549>  
- <https://ok.ru/profile/554045979166>

# OpSec

- Don't use smartphones for anything related to work
- Do not run anything received from the network on your personal computer
- Encrypt your work partition, store your work files in encrypted containers
- If you need to attach a file (log, screenshot etc.) you directly attach the file to the task, its forbidden to add links to file sharing websites
- Make backups as often as possible, copy them to a separate medium, store it separately, it's advisable to store the media with backups in another room. Backup media must be encrypted
- Files should always be shared as encrypted rar files
- File names should not be revealing, create table of contents for files separately
- Avoid transferring files through privnote.com and similar services, remember transferred text will remain in server logs
- DO NOT OPEN other people's .doc, .docx, .xls, .pdf, .rtf on your personal machine, these are used for delivering payloads
- Use .txt primarily, with the exception of images

# Final thoughts

- Too big to fail (for now)
- Lucrative to a vast pool of talent
- Groups with the strongest engineering culture are the most successful
- Targets are always available (opportunity not selection)
- Payments are a business decision (not legislation)
- Individuals are the ultimate victims of most leaks not companies
- No significant consequences for either side

# Questions?



Hossein Danesh



hndanesh