

Digital Frontiers

Exploring Today's Hacker Threats and Countermeasures

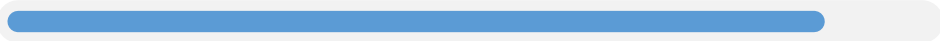
Martin Lutz

Security Evangelist – Central Eastern Europe

 Martin Lutz is an experienced Senior Security Professional with a distinguished history of enhancing the security posture and maturity of various organizations, ensuring robust protection in an ever-evolving threat landscape.

 My passion is Cyber Security.

 Governance, Risk, and Compliance (GRC)



 Strategic Security Planning



 Scuba Diving 🤿



Martin LUTZ



<https://www.linkedin.com/in/martin-lutz-/>



「How do you know,
that you have not
been hacked already?」



Unlock innovation

Drive operational excellence with an AI augmented workforce
Solutions



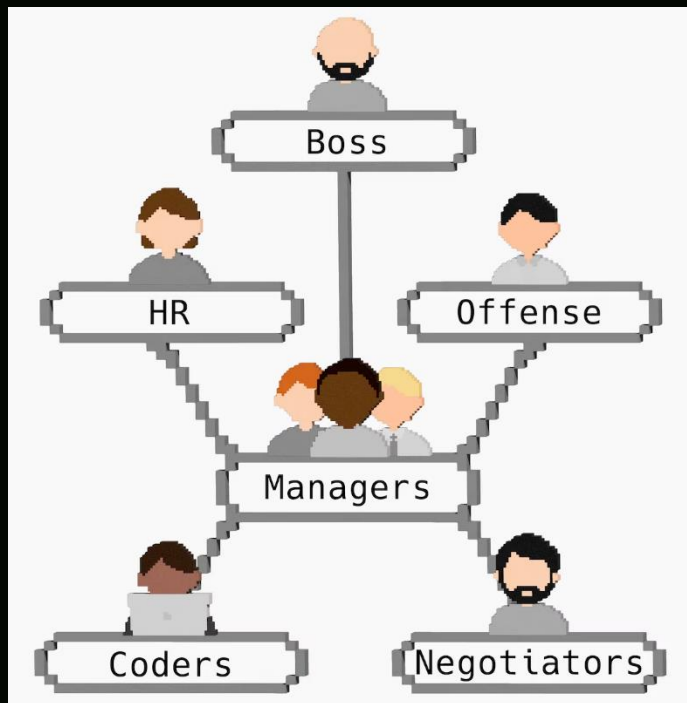
Unlock innovation







How are Hackers groups organized?



Example LockBit

- Probably most successful hacker group in the world
- Ransomware as a Service (RaaS)
- 10 fix employees consisting of pentesters, developers, money launderers, testers, and negotiators.
- More than 50 external developers. Average salary is 1.000-2.000 USD / month.
- Currently working with 100 affiliates. Plan is to increase to 300.
- Affiliates get 20% of profit. More if they do the negotiation with the "customers".
- Founder of Lockbit owns three restaurants in China and two restaurants in New York.

Marketing plays an important role

- LockBit frequently invests into marketing campaigns
- Everybody that gets a LockBit Tattoo is paid 1000 USD

Смелли: In a video that was released, some cl0p ransomware affiliates stored their money under a mattress. Is that where you keep your money too?
 Л80: I don't have money under my mattress, everything I cash out I immediately invest in the business and mix it with legal money, this way I inflate my business profits and launder money. And I spend only the money that is obtained in an honest way from the profits of my business and pay with my card)))

Смелли: Hahahaha. Yes, its been rumored you own a restaurant. Is this true?
 Л80: It's true, now I have 3 restaurants in China, and 2 restaurants in New York

Смелли: Random question: If you had the chance to tell threat intelligence something, what would you say?
 Л80: Work better bums, you have to find all my competitors, but you can never find me.

Смелли: Random question: If you had the chance to talk to the FBI, what would you say?
 Л80: Free Assange.

Смелли: Random question: If you had a chance to tell an anti virus company something. What would you say?
 Л80: Don't watch your users please

Encryption speed comparative table for some ransomware							
PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002
RansomEXX	14 Dec, 2020	138 MB/s	12M	20H	No	156	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17	109842



What happened to Lockbit?

 LOCKBIT 3.0	LEAKED DATA	 TWITTER  PRESS ABOUT US	>  HOW TO BUY BITCOIN >  AFFILIATE RULES	>  CONTACT US >  MIRRORS
Instant search × Company name:				
File Name ↓	File Size ↓	Date ↓		
 sigma-alimentos.com/	-	June 24, 2022		
 incedg.com_inces.com/	-	June 24, 2022		
 expeditors.com/	-	June 24, 2022		
 wabteccorp.com/	-	August 19, 2022		
 entrust.com/	-	August 19, 2022		
 tapcocu.org/	-	October 4, 2022		
 samyang.com/	-	October 6, 2022		
 marktel.es/	-	October 30, 2022		
 botswanatourism.co.bw/	-	February 23, 2024		

What can law enforcement do?

 **LOCKBIT 3.0**

LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE
UK, THE US AND THE CRONOS TASK FORCE

 **NCA**
National Crime Agency



 **EUROPOL**



Who is LockbitSupp?

LockbitSupp has claimed to live in the United States... **he doesn't**
LockbitSupp has claimed to live in the Netherlands... **he doesn't**
LockbitSupp has claimed to have a Lamborghini... **he drives a Mercedes**
(though parts may be hard to source)



We know who he is.
We know where he lives.
We know how much he is worth.

LockbitSupp has engaged with Law Enforcement :)

The MOST important thing for Hacker

REPUTATION

All FBI actions are aimed at destroying the reputation of my affiliate program, my demoralization, they want me to leave and quit my job, they want to scare me because they can not find and eliminate me, I can not be stopped, you can not even hope, as long as I am alive I will continue to do pentest with postpaid.

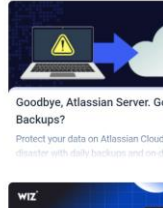
February 24, 2024

What else?

Exit Scam: BlackCat Ransomware Group Vanishes After \$22 Million Payout

Mar 06, 2024 Newsroom

Cyber Crime / Ransomware

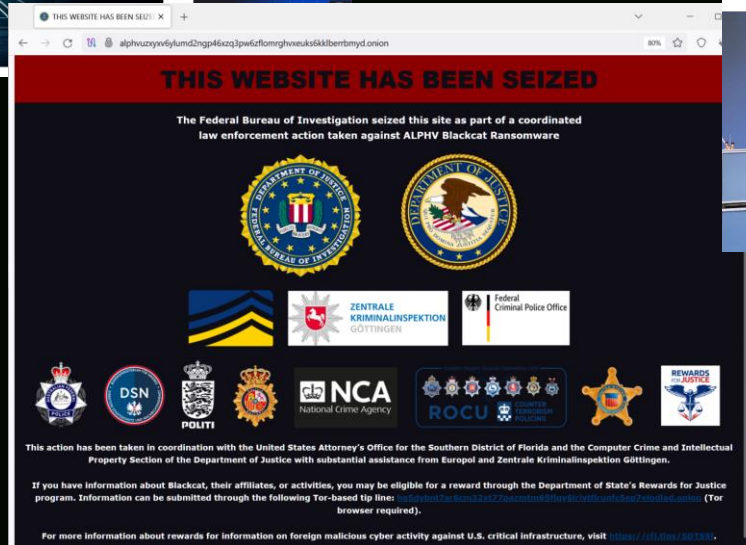


UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages

Ransomware gang ALPHV/BlackCat claims huge breach of US patient records

Zack Whittaker @zackwhittaker / 4:15 PM GMT+1 • February 29, 2024

Comment



What can we do?





Thank you!