



# Ransomware: Lukrativ und professionell organisiert. Wohin geht die Reise?

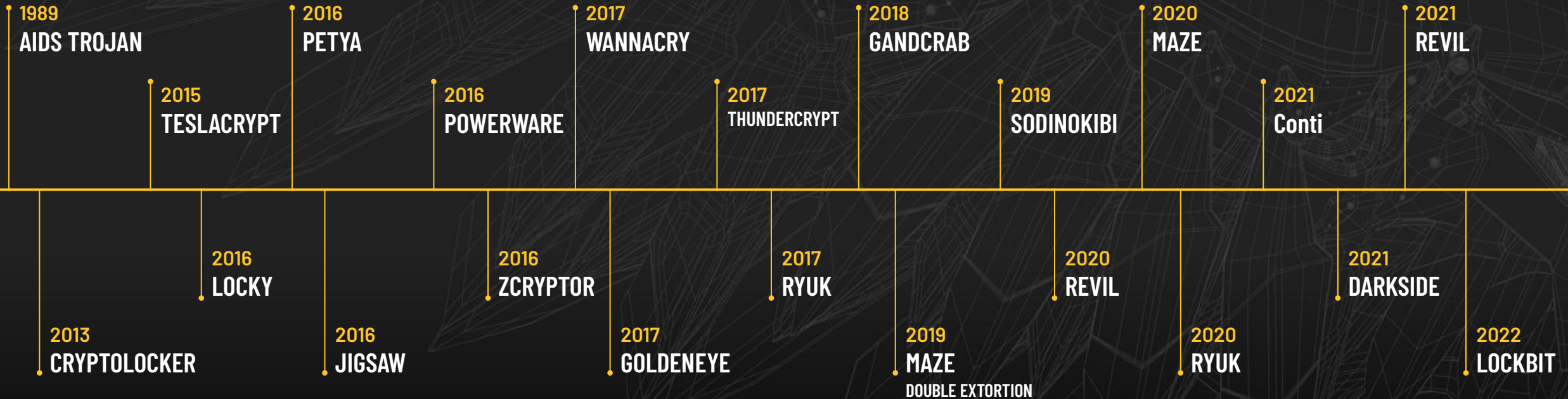
**Alexandre Curty - Cybereason**

Enterprise Sales Director

**Marcel Klomfar - IKARUS**

Senior Executive

# More than 30 years of history



A ransomware attack took place every 11 seconds in 2021  
Ransomware will strike every 2 seconds by 2031 - Cybersecurity Ventures

# The Big Business of Ransomware



Insurance Company / USA  
6'700 Employees  
Annual revenue for 2020 was \$10.808B

March 2021  
**\$40M** Payout after negotiation  
vs \$60M

Phoenix Locker



Meat Supplier / Brazil  
250'00 Employees  
Annual revenue for 2020 was \$52.42B

May 2021  
**\$11M** Payout after negotiation  
vs. \$22.5M

Revil



Chemical distribution / Germany  
17'000 Employees  
Annual revenue for 2020 was \$13.452B

May 2021  
**\$4.4M** Payout after negotiation  
vs. \$7.5M

DarkSide



# Double extortion and Beyond

1

## Encryption

Victims pay to regain access to encrypted data and compromised services that stop working because data and files are encrypted.

2

## Data Theft

Cybercriminals steal data and promise not to sell it if a ransom is paid off.

3

## Denial of Service

Cybercriminals launch denial of service attacks that shut down a victim's service.

4

## Harassment

Cybercriminals contact victims' customers, business partners, employees and media to tell them the organization was hacked.

# From Ransomware to RansomOps

## Initial Access Brokers (IABs)

Infiltrate target networks, establish persistence and move laterally to compromise as much of the network as possible, then sell access to other threat actors

## Ransomware-as-a-Service (RaaS)

Providers: Supply the actual ransomware code, the payment mechanisms, handle negotiations with the target and provide other “customer service” resources to both the attackers and the victims



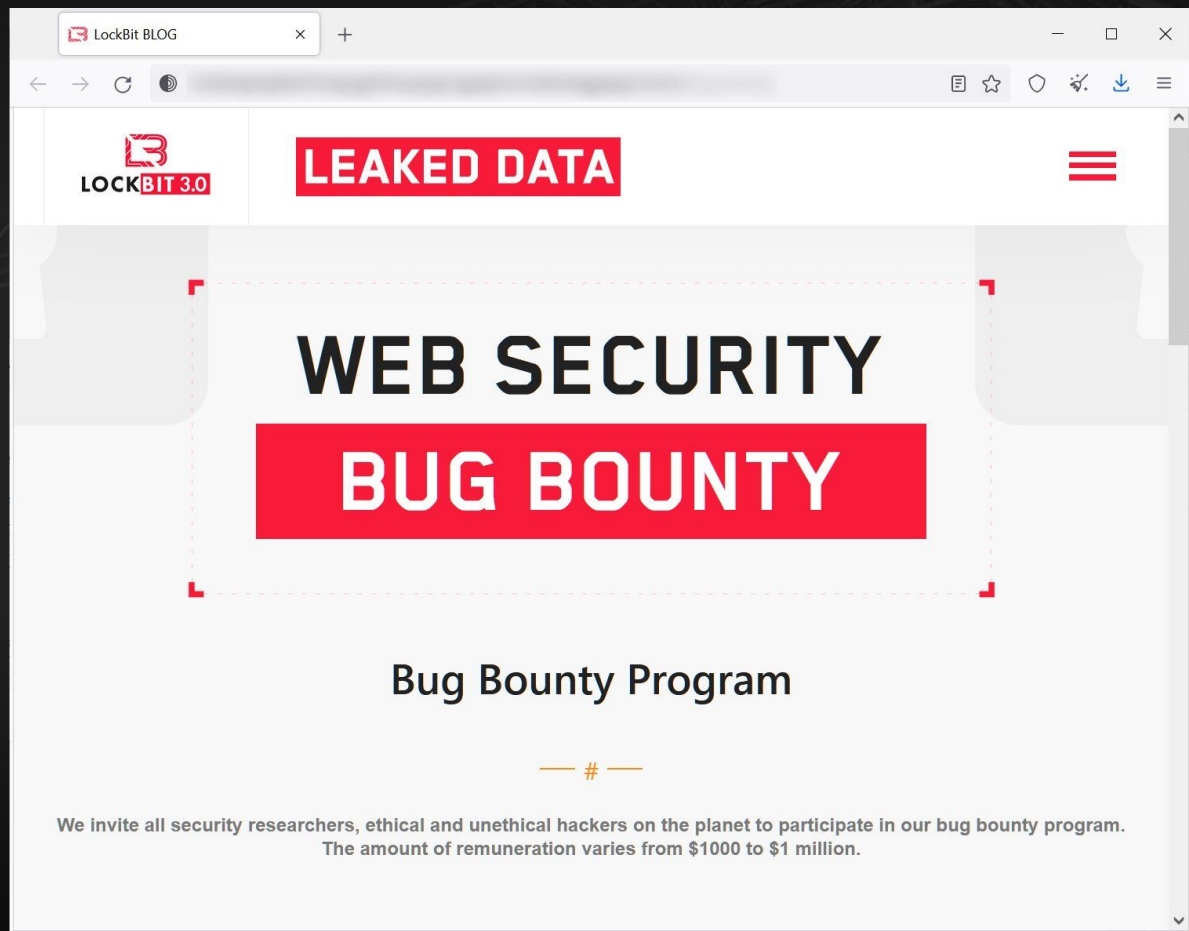
## Cryptocurrency Exchanges

Launder the extorted proceeds

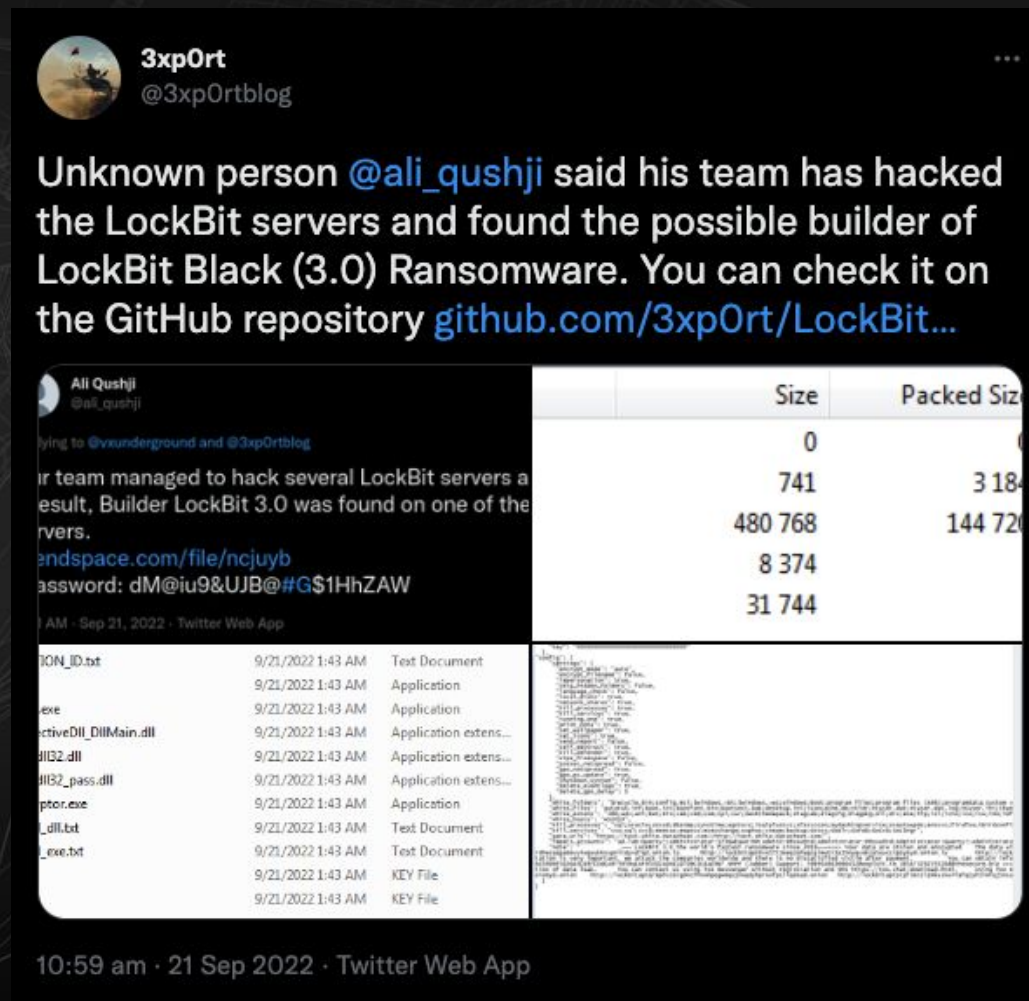
## Ransomware Affiliates

Contract with the RaaS provider, select the targeted organisations and then carry out the actual ransomware attack

# lockbit 3.0 : Following and facing trends



The screenshot shows the LockBit 3.0 website with a white background. At the top left is the 'LOCKBIT 3.0' logo. To its right is a red banner with the text 'LEAKED DATA'. Below these, a large red banner with white text reads 'WEB SECURITY BUG BOUNTY'. Underneath this, the text 'Bug Bounty Program' is centered. At the bottom, a paragraph states: 'We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from \$1000 to \$1 million.'



The screenshot shows a Twitter thread. The top tweet is from @3xp0rtblog, stating: 'Unknown person @ali\_qushji said his team has hacked the LockBit servers and found the possible builder of LockBit Black (3.0) Ransomware. You can check it on the GitHub repository [github.com/3xp0rt/LockBit...](https://github.com/3xp0rt/LockBit...)'. Below it is a reply from Ali Qushji (@ali\_qushji) with a screenshot of a file explorer showing a directory structure. The directory structure includes a 'files' folder containing several files: 'ION\_ID.txt', 'exe', 'ectiveDll\_DllMain.dll', 'HIB2.dll', 'HIB2\_pass.dll', 'ptor.exe', '\_dll.txt', and '\_exe.txt'. The files are listed with their sizes and packed sizes. The tweet is dated 10:59 am · 21 Sep 2022 · Twitter Web App.

File Name	Size	Packed Size
ION_ID.txt	0	0
exe	741	3 184
ectiveDll_DllMain.dll	480 768	144 720
HIB2.dll	8 374	
HIB2_pass.dll	31 744	
ptor.exe		
_dll.txt		
_exe.txt		



Have you ever missed celebrating a holiday or participating in a weekend event because of a ransomware attack?



97%

ITALY



95%

GERMANY



94%

UAE



92%

SINGAPORE



97%

US



84%

SOUTH AFRICA



81%

UK



79%

FRANCE



THANK  
YOU.

