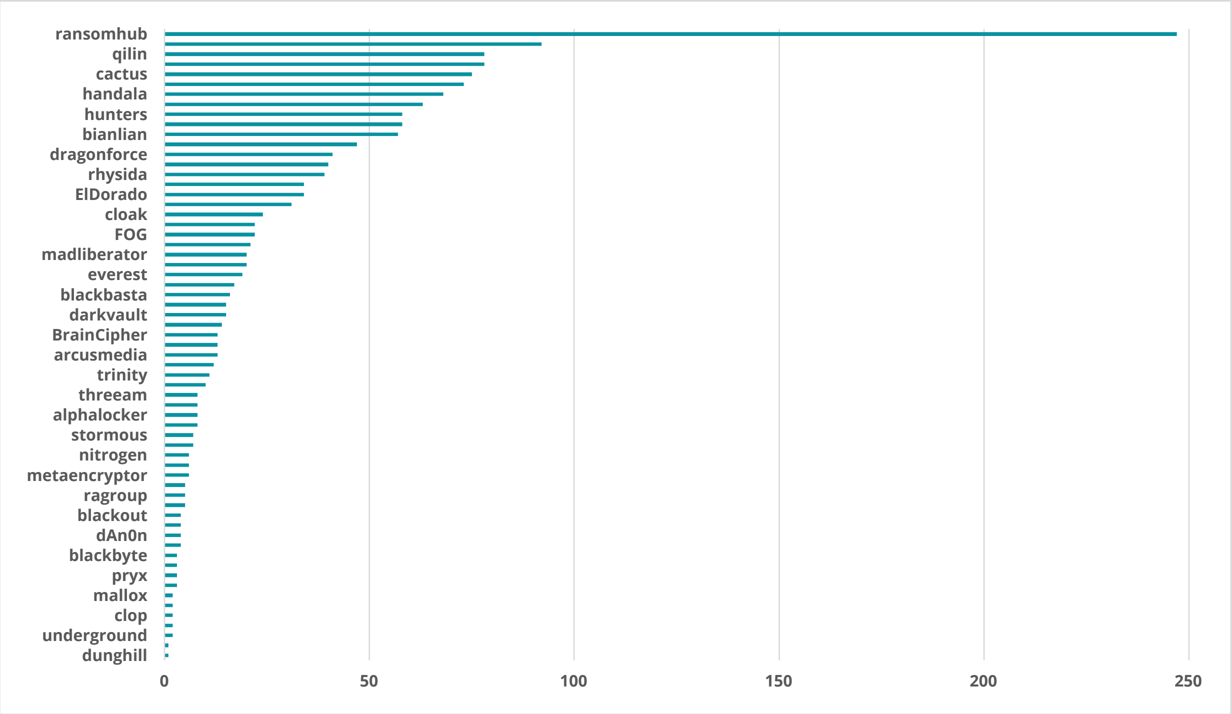
Quarterly Ransomware Research Report

Published by CyberMaxx

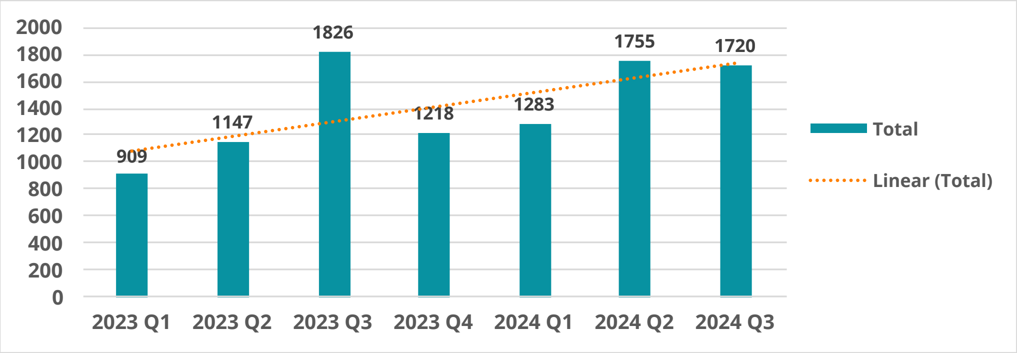
Ransomware Report Q3 2024

Ransomware Industry

The total number of ransomware attacks in Q3 of 2024 has not lost any momentum from Q2, and finished with 1720 observed attacks. Compared to Q2's 1755, this a 2% deviation in volume, on one of the busiest quarters in the past 18 months.



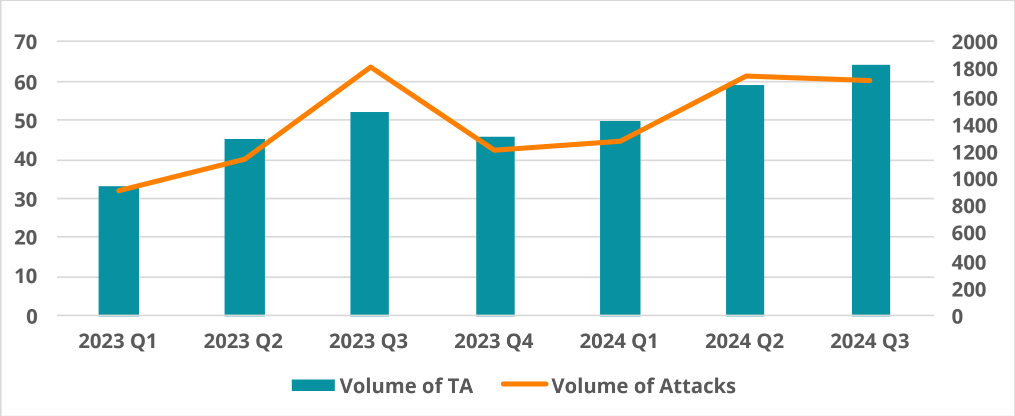
Total Number of Attacks by Threat Actor, Q3 2024



Total Ransomware Attacks by Quarter, Q1 2023 – Q3 2024

Running average this quarter is 27 successful attacks per group, (1720 attacks / 64 active identified groups), which also shows that the number of attacks is increasing as time goes on. Interestingly, the total number of active ransomware and extortion groups is also increasing in line with the increase of these types of attacks. The average number of attacks per group is staying within similar boundaries (excl. large spikes/drops) at 26-29 attacks per quarter – which tells us that this increase in attacks is not because existing groups are having more success, but rather that the total number of affiliates, threat actors and groups is growing. **Ransomware operations is a thriving industry.**

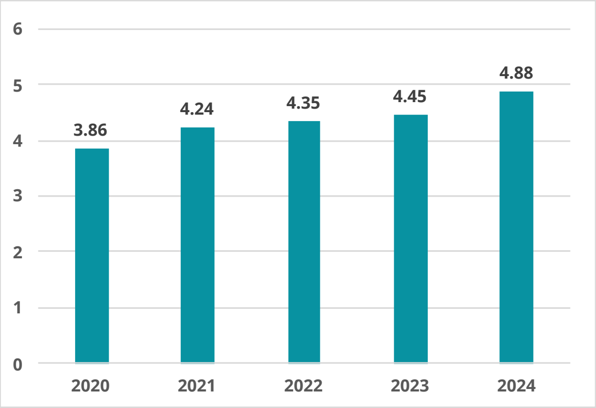
Quarter	Total Number of Successful Attacks	Total Number of Active Groups
2024 Q3	1720	64
2024 Q2	1755	59
2024 Q1	1283	50
2023 Q4	1218	46
2023 Q3	1826	52
2023 Q2	1147	45
2023 Q1	909	33



Combined: Total Ransomware Groups (left, teal) and Volume of Attacks (right, orange)

The average cost of a data breach for an organization continues to grow year over year, as measured by IBMs “Cost of a Data Breach,” through 2020 until today in 2024, rising from $3.86M to $4.88M in four years. This data shows that incidents are getting more expensive and more frequent as time goes on.

Security costs continue to go up to combat the increasing likelihood of a successful attack. The data and statistics detailed above are only the tip of the iceberg, as with cybersecurity incidents there are multiple other factors depending on industry which can impacts an organization’s bottom line.



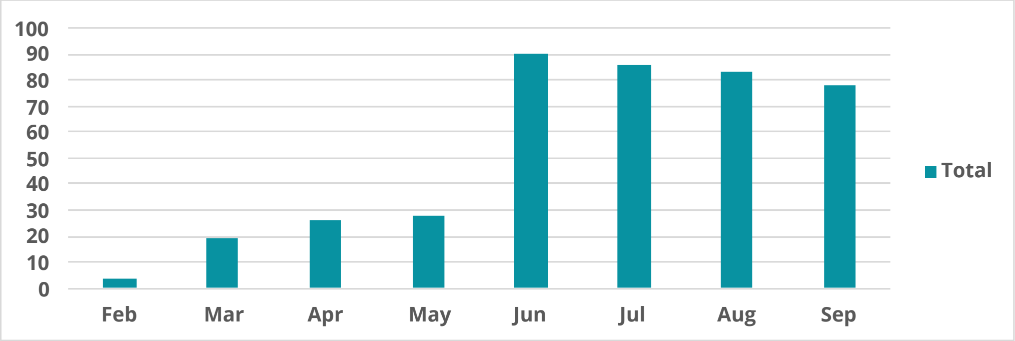
Average Cost of a Data Breach in Millions of USD, 2020-2024

Ransomware Groups

The top five groups measured by volume of attacks this quarter are:

Group	Volume
Ransomhub	247
Lockbit	92
Play	92
Qilin	80
Meow	78

Ransomhub, who we previously mentioned last quarter have risen to the top with their marketplace offering between an 80% and 90% profit split with affiliates. The unpaid AlphV affiliates who performed the ransomware attack on Change HealthCare worked with Ransomhub to extort Change a second time. It is not known if Change paid the second extortion, but this display may have led to Ransomhub gaining credibility and attracting other affiliates to their platform.



Ransomhub Lifetime Activity

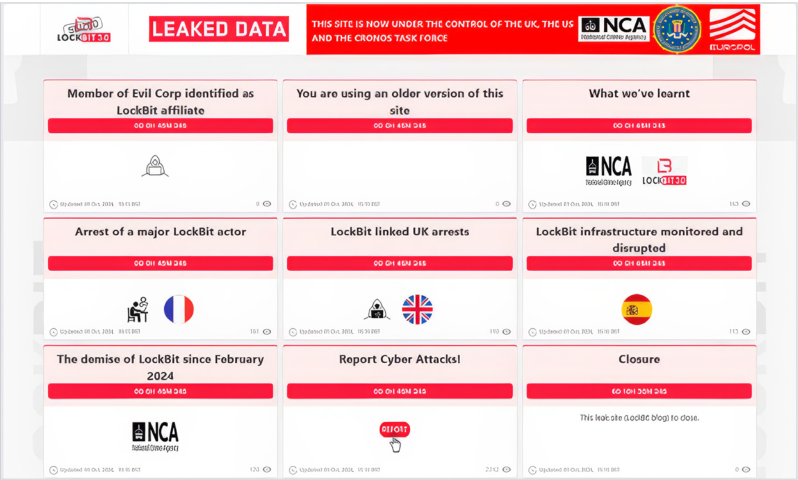
Lockbit is still going strong, coming in second again despite the disruptions by law enforcement in their operations.

Interestingly, Dispossessor has fallen from the most prolific group last quarter, down to 15th place with only 40 attacks, vs. 329 last quarter. We discussed this group last quarter, noting that many of the victims listed on their darkweb page originally appeared on other groups pages. Many have speculated that Dispossessor are not performing attacks directly and are instead taking credit for the work of others. This sudden drop lends more credibility to that claim. The CyberMaxx research team spoke with an organization in the financial sector who were listed as a victim and confirmed that this was another case of false advertising and reuse on Dispossessors side of an incident which occurred earlier in the year.

Major Events

Operation Cronos Update

Law Enforcement updated Lockbit's release pages on the dark web with a countdown timer, replacing posts that were previously made during the disruption operation earlier this year. The posts were titled "Lockbit Linked UK Arrest" and "Lockbit Disruption" amongst others. A screenshot of this can be seen below:


LOCKBIT 3.0
LEAKED DATA
THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE
NCA
EUROPOL

Member of Evil Corp identified as LockBit affiliate
00 0H 45M 34S

You are using an older version of this site
00 0H 45M 34S

What we've learnt
00 0H 45M 34S

Arrest of a major LockBit actor
00 0H 45M 34S

LockBit linked UK arrests
00 0H 45M 34S

LockBit infrastructure monitored and disrupted
00 0H 45M 34S

The demise of LockBit since February 2024
00 0H 45M 34S

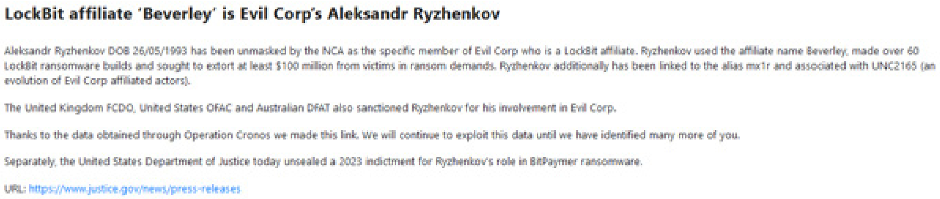
Report Cyber Attacks!
00 0H 45M 34S

Closure
60 10H 30M 34S

This leak site (LockBit blog) to close.

Once the timer reached zero, the posts were released, related to the arrest of multiple individuals worldwide who were related to the Lockbit operation, including developers and the owner of the bullet-proof hosting site used by Lockbit's infrastructure.

Images from the released posts are below:



LockBit affiliate 'Beverley' is Evil Corp's Aleksandr Ryzhenkov

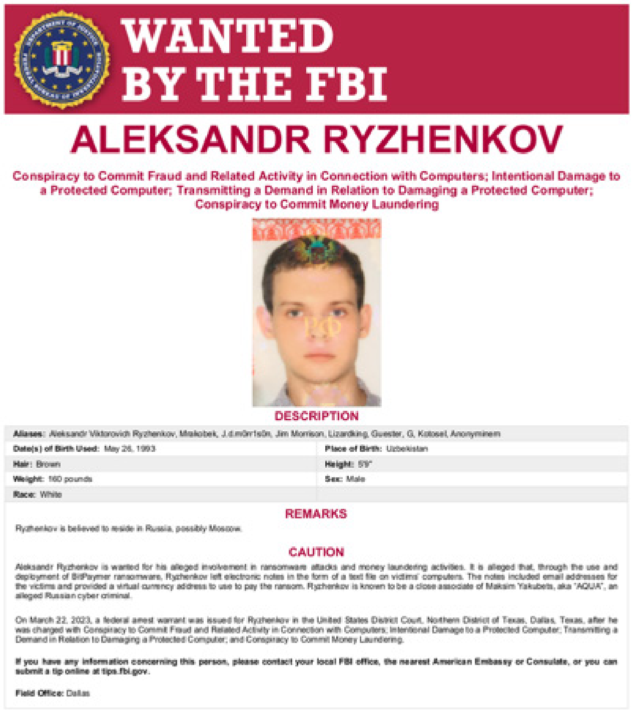
Aleksandr Ryzhenkov DOB 26/05/1993 has been unmasked by the NCA as the specific member of Evil Corp who is a LockBit affiliate. Ryzhenkov used the affiliate name Beverley, made over 60 LockBit ransomware builds and sought to extort at least $100 million from victims in ransom demands. Ryzhenkov additionally has been linked to the alias mx1r and associated with UNC2165 (an evolution of Evil Corp affiliated actors).

The United Kingdom FCDO, United States OFAC and Australian DFAT also sanctioned Ryzhenkov for his involvement in Evil Corp.

Thanks to the data obtained through Operation Cronos we made this link. We will continue to exploit this data until we have identified many more of you.

Separately, the United States Department of Justice today unsealed a 2023 indictment for Ryzhenkov's role in BitPaymer ransomware.

URL: https://www.justice.gov/news/press-releases



WANTED BY THE FBI

ALEKSANDR RYZHENKOV

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer; Conspiracy to Commit Money Laundering

DESCRIPTION

Aliases: Aleksandr Viktorovich Ryzhenkov, Mrakobek, J.d.m0rr1s0n, Jim Morrison, Lizardking, Guester, G, Kotosel, Anonyminem	
Date(s) of Birth Used: May 26, 1993	**Place of Birth:** Uzbekistan
Hair: Brown	**Height:** 5'9"
Weight: 160 pounds	**Sex:** Male
Race: White	

REMARKS

Ryzhenkov is believed to reside in Russia, possibly Moscow.

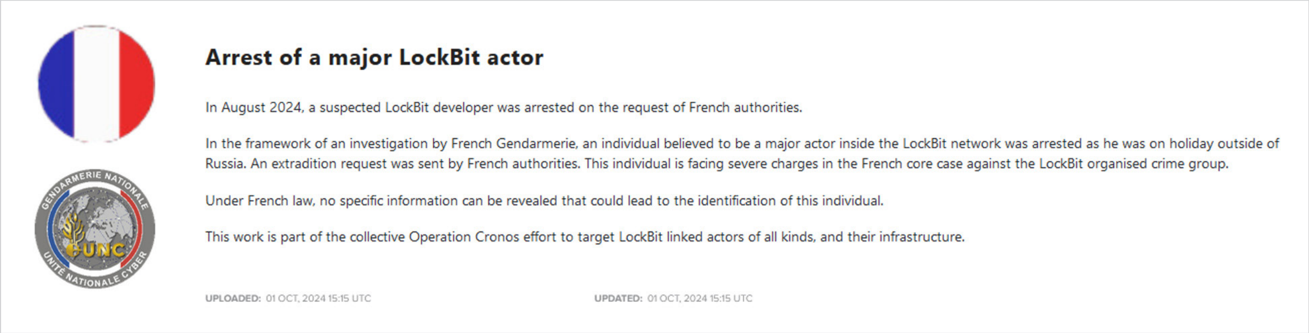
CAUTION

Aleksandr Ryzhenkov is wanted for his alleged involvement in ransomware attacks and money laundering activities. It is alleged that, through the use and deployment of BitPaymer ransomware, Ryzhenkov left electronic notes in the form of a text file on victims' computers. The notes included email addresses for the victims and provided a virtual currency address to use to pay the ransom. Ryzhenkov is known to be a close associate of Maksim Yakubets, aka "AQUA", an alleged Russian cyber criminal.

On March 22, 2023, a federal arrest warrant was issued for Ryzhenkov in the United States District Court, Northern District of Texas, Dallas, Texas, after he was charged with Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer; and Conspiracy to Commit Money Laundering.

If you have any information concerning this person, please contact your local FBI office, the nearest American Embassy or Consulate, or you can submit a tip online at tips.fbi.gov.

Field Office: Dallas



Arrest of a major LockBit actor

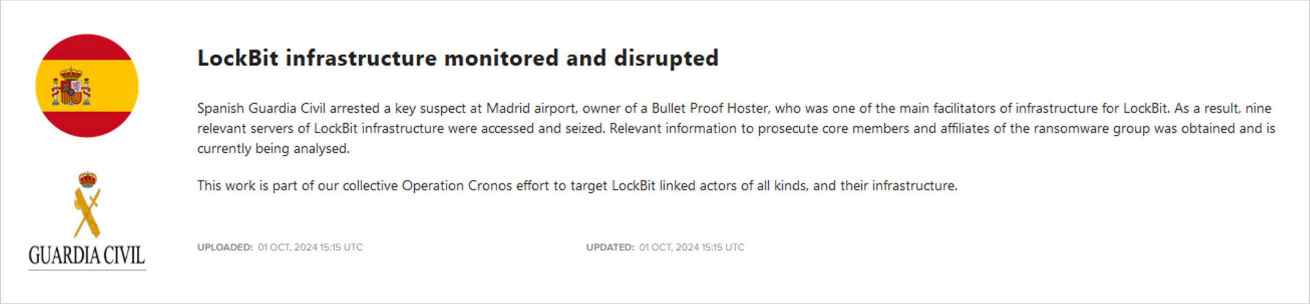
In August 2024, a suspected LockBit developer was arrested on the request of French authorities.

In the framework of an investigation by French Gendarmerie, an individual believed to be a major actor inside the LockBit network was arrested as he was on holiday outside of Russia. An extradition request was sent by French authorities. This individual is facing severe charges in the French core case against the LockBit organised crime group.

Under French law, no specific information can be revealed that could lead to the identification of this individual.

This work is part of the collective Operation Cronos effort to target LockBit linked actors of all kinds, and their infrastructure.

UPLOADED: 01 OCT, 2024 15:15 UTC **UPDATED:** 01 OCT, 2024 15:15 UTC

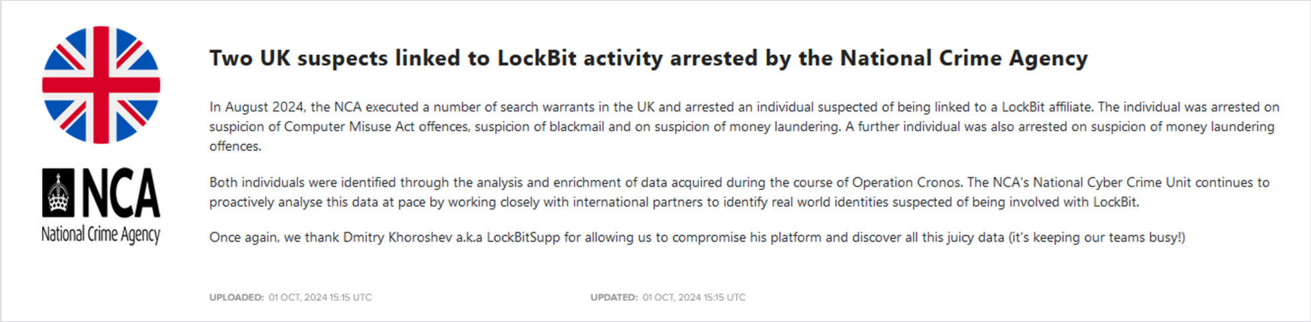


LockBit infrastructure monitored and disrupted

Spanish Guardia Civil arrested a key suspect at Madrid airport, owner of a Bullet Proof Hoster, who was one of the main facilitators of infrastructure for LockBit. As a result, nine relevant servers of LockBit infrastructure were accessed and seized. Relevant information to prosecute core members and affiliates of the ransomware group was obtained and is currently being analysed.

This work is part of our collective Operation Cronos effort to target LockBit linked actors of all kinds, and their infrastructure.

UPLOADED: 01 OCT, 2024 15:15 UTC **UPDATED:** 01 OCT, 2024 15:15 UTC



Two UK suspects linked to LockBit activity arrested by the National Crime Agency

In August 2024, the NCA executed a number of search warrants in the UK and arrested an individual suspected of being linked to a LockBit affiliate. The individual was arrested on suspicion of Computer Misuse Act offences, suspicion of blackmail and on suspicion of money laundering. A further individual was also arrested on suspicion of money laundering offences.

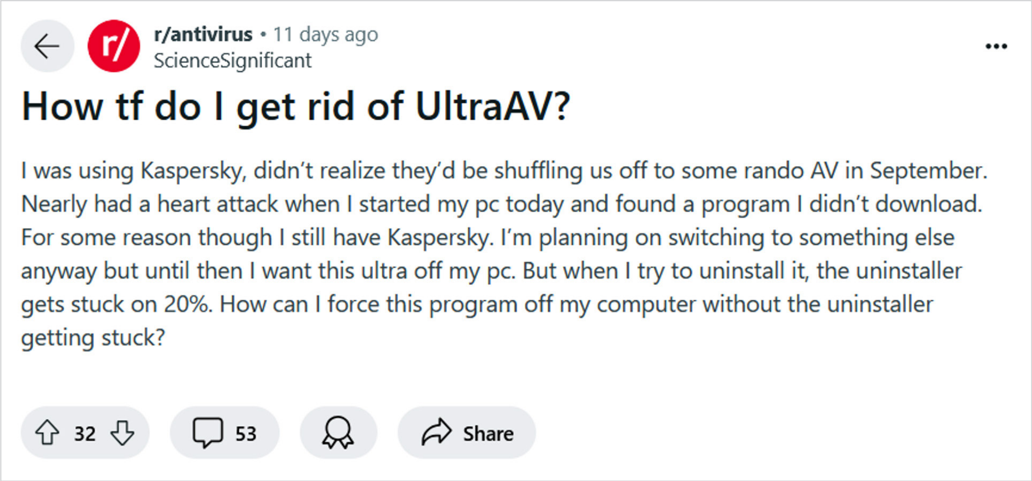
Both individuals were identified through the analysis and enrichment of data acquired during the course of Operation Cronos. The NCA's National Cyber Crime Unit continues to proactively analyse this data at pace by working closely with international partners to identify real world identities suspected of being involved with LockBit.

Once again, we thank Dmitry Khoroshev a.k.a LockBitSupp for allowing us to compromise his platform and discover all this juicy data (it's keeping our teams busy!)

UPLOADED: 01 OCT, 2024 15:15 UTC **UPDATED:** 01 OCT, 2024 15:15 UTC

Kaspersky

Kaspersky succumb to US sanctions and sell off the US arm of the company, replacing itself with Ultra AV. Users were supposed to get advance warning of this but that seems to have been missed by several users. u/ScienceSignificant on Reddit had this to say on the AntiVirus sub:



r/antivirus • 11 days ago
ScienceSignificant

How tf do I get rid of UltraAV?

I was using Kaspersky, didn't realize they'd be shuffling us off to some rando AV in September. Nearly had a heart attack when I started my pc today and found a program I didn't download. For some reason though I still have Kaspersky. I'm planning on switching to something else anyway but until then I want this ultra off my pc. But when I try to uninstall it, the uninstaller gets stuck on 20%. How can I force this program off my computer without the uninstaller getting stuck?

It has been an interesting few years for Kaspersky, with many government agencies deciding to ban the software. A brief timeline is available below:

- LT (banned from critical infrastructure, govt. agencies can run if not sensitive): 2017
- US (prohibits Kaspersky products in federal networks): 2017
- UK (banned Kaspersky products in depts. Responsible for national security)
- NL (Banned from government systems. Justice Minister Ferdinand Grapperhaus said: “Russia has an offensive cyber program that targets among others the Netherlands and Dutch interests”): 2018
- DE (Issued a warning against Kaspersky and advised to switch to other solutions): 2022
- IT (banned in public sector over “great concern” with Kaspersky products. Occurred less than a month after RU invaded UA): 2022
- RO (Banned Kaspersky and other RU security products from public institutions and private IT institutions with classified info): 2022
- CA (Banned from Government mobile device: 2023)

Other Notable Events

- CrowdStrike outage on 19th July 2024. Lead to Microsoft holding a summit to discuss the future of security in the Microsoft kernel. Currently awaiting this outline
- Health Infrastructure Security and Accountability Act proposed in the US, September 26th 2024. If passed, it would set clearer cyber security standards for the healthcare industry and hold corporation executives accountable

Sources Used Throughout This Report

- Operation Cronos updates: Sourced directly from dark web by CyberMaxx Security Research team
- Cost of a databreach: HTTPS://WWW.IBM.COM/REPORTS/DATA-BREACH
- Kaspersky
  - HTTPS://PROTON.ME/BLOG/KASPERSKY-BAN
  - HTTPS://CYBERSCOOP.COM/DUTCH-KASPERSKY-BAN/

CyberMaxx

About

CyberMaxx, founded in 2002, is the leading provider of managed detection and response (MDR) services. We help customers reduce risk by tightly integrating MDR with offensive security, threat hunting, security research, digital forensics and incident response (DFIR) to continually adapt to new and evolving threats. Our modern MDR approach is tailored to the unique characteristics and risk factors of each customer, enabling us to take full ownership of the response process and, optionally, manage key security controls. By thinking like an adversary and defending like a guardian, we help our customers stay a step ahead of threat actors.

Learn More, Today!

To learn more about CyberMaxx’s solutions please visit, CYBERMAXX.COM to get started.