The Social and Technological Incentives for Cybercriminals to Engage in Ransomware Activities

Yichao Wang*, Sophia Roscoe, Budi Arief, Lena Connolly, Hervé Borrion, Sanaa Kaddoura

*yw300@kent.ac.uk

Download the pdf of the paper using the QR Code

SocialSec 2023: 9th International Symposium on Security and Privacy in Social Networks and Big Data

Outline

- Background, Motivation and Aim
- Methodology
- Findings
- Conclusion and Future Work

Background

BBC Sign in Home News Sport

NEWS

Home | Cost of Living | War in Ukraine | Climate | UK | World | Business | Politi

Health

NHS cyber-attack: GPs and hit by ransomware

13 May 2017

NHS services across England and Scotland have been hit by a large-scale cyber-attack that has disrupted hospital and GP appointments.

The prime minister said the incident was part of an untargeted wider attack affecting organisations globally.

Some hospitals and GPs have been unable to access patient data, after their computers were locked by a ransomware program demanding a payment worth £230.

But there is no evidence patient data has been compromised, NHS Digital said.

The BBC understands about 40 NHS organisations and some GP practices have been hit. The NHS in Wales and Northern Ireland has not been affected.

There is no indication of who is behind the attack yet, but the hackers demanded their payment in the virtual currency Bitcoin, which is harder to trace.

Prime Minister Theresa May said: "This is not targeted at the NHS, it's an international attack and a number of countries and organisations have been affected."

uardian

with £5 per month

on Sport Culture Lifestyle More

Asia Australia Middle East Africa Inequality Global development

This article is more than **2 years old**

Cyber-attack forces shutdown of one of the US's largest pipelines

Colonial Pipeline said it shut down 5,500 miles of pipeline, which carries 45% of the east coast's fuel supplies

Oil storage tanks owned by the Colonial Pipeline Company in Linden, New Jersey. Photograph: Mark Lennihan/AP

One of the largest pipelines in the US has been shut down after an apparent cyber-attack, its operator has said.

Colonial Pipeline said it had shut down its 5,500 miles of pipeline, which carries 45% of the east coast's fuel supplies and travels through 14 southern

FLASHPOINT

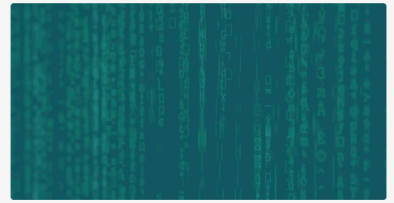
PLATFORM SOLUTIONS RESOURCES COMPANY Free trial LOG IN

Blogs

BLOG

LockBit Ransomware: Inside the World's Most Active Ransomware Group

LockBit was responsible for nearly 28 percent of known ransomware activity in the past year, and remains a major threat to organizations in the ransomware landscape



SHARE THIS: Flashpoint July 20, 2023

TABLE OF CONTENTS

- What is LockBit?
- The formation of LockBit
- The LockBit reputation
- How LockBit attacks
- Lockbit variants
- Preventing a LockBit attack
- The future of LockBit
- Identify and mitigate cyber risks with Flashpoint

In the world of ransomware, LockBit has emerged as a prominent and widespread cyber threat, posing serious challenges to organizations worldwide.

In recent times, the group has gained notoriety for its sophisticated and ruthless strain of ransomware. It infiltrates computer systems, encrypts vital data, and demands hefty ransoms, leaving victims grappling with difficult decisions.

LockBit has been the dominant strain of ransomware over approximately the past year. According to Flashpoint data, it has accounted for 27.93 percent of all known ransomware attacks from July 2022 to June 2023.

Top 10 Ransomware Groups July 2022 - June 2023

RANSOMER NAME	VICTIM POSTS
1. LockBit	1,046
2. BlackCat	389
3. Black Basta	239
4. Royal	215
5. Clop	205
6. BianLian	203
7. Play	156
8. Akira	107
9. Karakurt	102
10. Vice Society	99

FLASHPOINT

The top ten ransomware groups by number of victim posts from July 1, 2022 – June 30, 2023 (Source: Flashpoint).

Awareness, knowledge, and preparation are crucial. With a clear understanding of LockBit and the necessary preventive measures to guard against it, organizations can fortify their defenses and mitigate the risks posed by this ever-evolving cyber threat.

Motivation

There is limited research focused on how potential criminals are motivated to engage in ransomware activities

Image Sources:
https://www.socinvestigation.com/what-is-surface-web-deep-web-and-dark-web/
https://www.dreamstime.com/cartoon-criminal-running-gun-vector-design-cartoon-criminal-running-gun-vector-image103171750

Research Aim

To investigate the social and technological discourse in the dark web that may foster ransomware-related criminal activities

Outline

- Background, Motivation and Aim
- Methodology
- Findings
- Conclusion and Future Work

Data Collection

- A snapshot was taken on Dread based on our selection of 16 keywords
- The initial collected posts contained a sample of 19,109 candidate posts
- Candidate posts span a period of 1,720 days (between 16 February 2018 to 1 November 2022)
- Manual filtering was done and returned the final dataset of 1,279 posts, covering a period of 1,651 days (between 25 March 2018 and 30 September 2022)

Full set of the raw data available at: https://github.com/SocialSec2023-Paper-23/SocialSec-2023-Paper-23-Additional-Information

Post Categories

- **Hacker** : The post indicates that its author has performed a ransomware attack
  - Sub-category: “group” and “individual”
- **Potential Hacker** : The post indicates that its author plans to perform a ransomware attack
  - Sub-category: “group” and “individual”
- **RaaS Provider** : The post contains a user offering RaaS for sale
  - Sub-category: “group” and “individual”
- **News**: The post refers to ransomware -related real world events (e.g., actual ransomware attacks)

Post Categories (cont'd)

- **Education** : The post contains explicit educational information about ransomware related subjects
  - Sub-category: "request" and "provider"
- **Information** : The post requests or provides general information that cannot be classified as "Education" or "News"
  - Sub-category: "request", "provider", and "moderator"
- **Debate** : The post presents an opinion, often initiating or contributing to a debate
- **Other** : Posts that do not fit any of the previous categories

Outline

- Background, Motivation and Aim
- Methodology
- Findings
- Conclusion and Future Work

Mapping Posts

Table 1. The numeric breakdown of the posts among the eight categories

	Hacker		**Potential Hacker**		**RaaS Provider**		**Education**		**Information**			**News**	**Debate**	**Other**
	Group	Individual	Group	Individual	Group	Individual	Request	Provider	Request	Provider	Moderator	\	\	\
	22	6	22	99	26	44	76	89	216	370	5	\	\	\
Total	28		121		70		165		591			161	265	63
Percentage	2.19%		9.46%		5.47%		12.90%		46.21%			12.59%	20.72%	4.93%

Mapping Posts (cont'd)

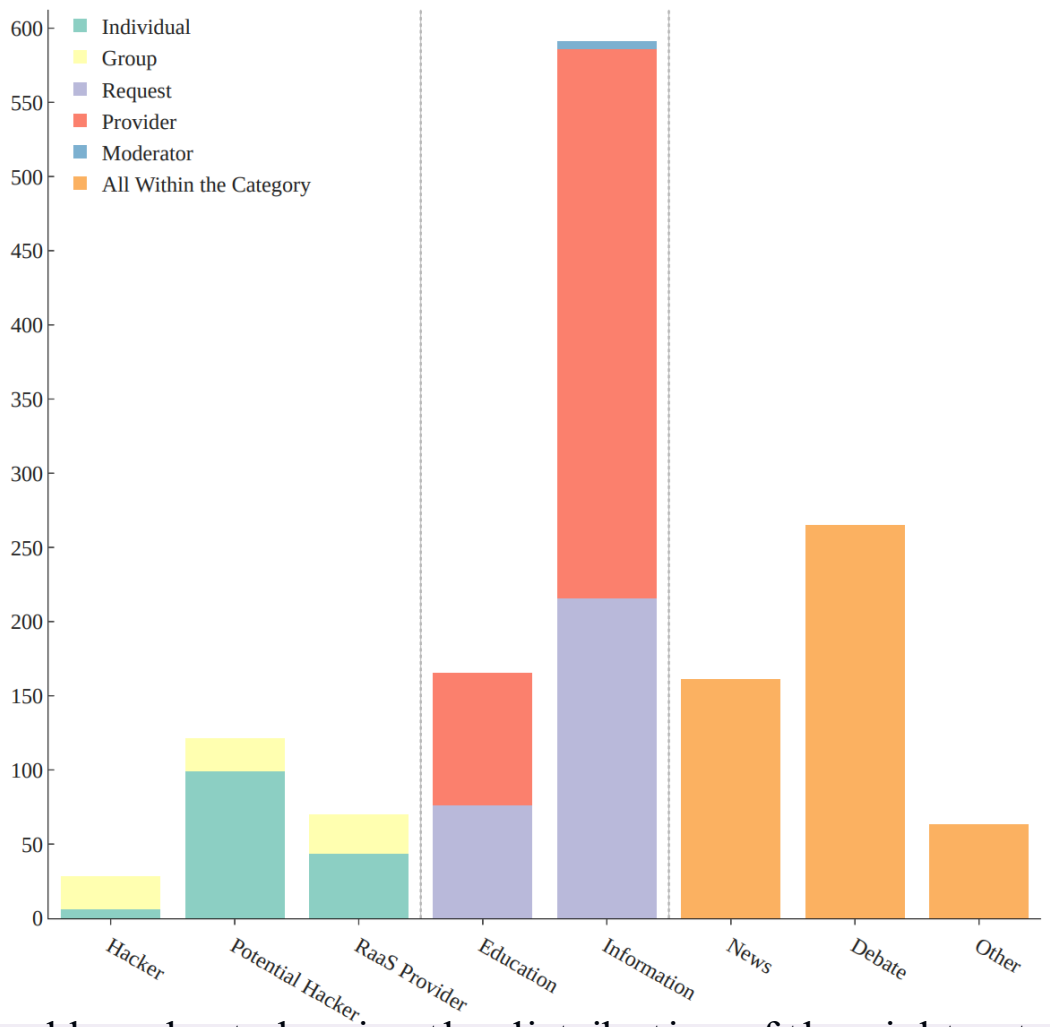


Fig. 1. A stacked bar chart showing the distribution of the eight categories of the ransomware-related posts in the Dread forum

Information & Education - Share

“anyone happen to have the onion link to the recent babuk ransomware breach?”

“can you tell me some gangs that offer raas services and how to contact them, please?”

“curious if anyone has any information on if revil was paid by kaseya or if they simply shut down to evade le. read today that kaseya was able to obtain a decryptor key from a third party, any thoughts?”

Debate - Morality

- Posts (marked as “Debate” category) often appear after an information or education request
- Many users debate the morality of using ransomware on anyone other than large companies
- During the COVID-19 pandemic, many condemned the attacks on healthcare facilities, citing the “impact of it on people's lives”
- Posts contribute to the building of trust between potential criminals and the emergence of more private criminal communities, as well as to encourage further learning

Ransomware as a Service (RaaS)

- Many conversations would be around RaaS groups, such as LockBit, DarkSide, etc.
  - *“looking for the lockbit2.0 on dread”*
- The user friendly and easy-to-set-up nature of RaaS makes it ideal for newbies to pick up, especially when there are some support communities to learn how to use RaaS

Dread – The Community

- **Horizontal Communication**
  - Due to the illegal nature of ransomware and Dread as a forum, the necessity of protecting it from law enforcement is paramount
  - Because of this "us vs. them" mentality, there is an incentive to share knowledge while trying to elude law enforcement and prevent exposure
- **Vertical Communication**
  - Was found within a small group of respected and knowledgeable individuals
  - E.g., a user who runs an extensive education course with many being *"very impressed"* with its contents

Keywords

Table 2. The frequencies and percentages of the keywords being found in ransomware-related posts

Keywords	Ransomware	RaaS	REvil	Extortion	DarkSide	LockBit	Sodinokibi	BlackCat	Hive	Avaddon	BlackMatter
Frequency	618	58	44	39	32	10	7	3	2	1	1
Percentage	75.83%	7.12%	5.40%	4.79%	3.93%	1.23%	0.86%	0.37%	0.25%	0.12%	0.12%

Outline

- Background, Motivation and Aim
- Methodology
- Findings
- Conclusion and Future Work

Conclusion

- Our dataset confirms that ransomware-related posts (1,279) exist on the Dread dark web forum
- These posts can generally be grouped into eight categories: *Hacker, Potential Hacker, RaaS Provider, Education, Information, News, Debate* and *Other*
- These posts pose a threat to cyber security, because they might provide a pathway for wannabe ransomware operators to get in on the act

Future Work

- More keywords and more variations of ransomware-related terms
- More data collection on different forums
  - Such as Russian Anonymous Marketplace (RAMP) and XSS
- Machine learning techniques can be employed
  - Classifying ransomware posts automatically
  - Automatic detection of such posts on platforms
- Considering how such posts should be handled, or how some follow-up intervention actions can be prepared

The Social and Technological Incentives for Cybercriminals to Engage in Ransomware Activities

Yichao Wang*, Sophia Roscoe, Budi Arief, Lena Connolly, Hervé Borrion, Sanaa Kaddoura

*yw300@kent.ac.uk

Download the pdf of the paper using the QR Code

SocialSec 2023: 9th International Symposium on Security and Privacy in Social Networks and Big Data