

LockBit, BlackCat, and Royal Dominate the Ransomware Scene in Q4 2022

Ransomware in Q4 2022

This data sheet collates relevant information on the ransomware threat landscape for the fourth quarter of 2022, obtained from ransomware-as-a-service (RaaS) and extortion groups' leak sites, Trend Micro's open-source intelligence (OSINT) research, and the Trend Micro™ Smart Protection Network™. The data presented here describes ransomware activity in general and the four most prominent ransomware families in the threat landscape during the three-month span.

Layer	OCT	NOV	DEC	TOTAL
Email threats	458,379	456,879	292,060	1,026,613
URL threats	123,997	122,433	122,352	835,848
File threats	444,237	256,536	535,952	950,364
Total threats				2,812,825

Table 1. The numbers of ransomware threats detected and blocked by Trend Micro across email, URL, and file layers per month in the fourth quarter of 2022

Source: Trend Micro™ Smart Protection Network™

Q4 2022	
Total active RaaS and extortion groups	32
Victim organizations	664

Table 2. The numbers of active RaaS and extortion groups and victim organizations of successful ransomware attacks in the fourth quarter of 2022

Source: RaaS and extortion groups' leak sites

Industry	Victim count
IT	79
Healthcare	57
Manufacturing	51
Academe	43
Finance	43
Materials	40
Professional services	40
Construction	39
Automobile	30
Transportation	27

Table 3. The top 10 industries affected by successful RaaS and extortion attacks in terms of victim organizations in the fourth quarter of 2022

Source: RaaS and extortion groups' leak sites and Trend Micro's OSINT research

Segment	OCT	NOV	DEC	TOTAL
Enterprise	8,861	14,057	9,294	32,212
Consumer	2,818	2,131	2,302	7,251
SMB	1,312	1,414	2,220	4,946

Table 4. The numbers of ransomware file detections in machines in each business segment per month in the fourth quarter of 2022

Source: Trend Micro Smart Protection Network

Country	Victim count
United States	279
United Kingdom	38
Canada	34
Germany	24
Australia	22
Brazil	21
France	17
Spain	17
India	13
Taiwan	11
Others	188
Total	664

Table 5. The top 10 countries affected by successful RaaS and extortion attacks in terms of victim organizations in the fourth quarter of 2022

Source: RaaS and extortion groups' leak sites and Trend Micro's OSINT research

Ransomware family	No. of victim organizations
Lockbit	147
BlackCat	77
Royal	71

Table 6. The top three ransomware families used in successful RaaS and extortion attacks in terms of victim organizations in the fourth quarter of 2022

Source: RaaS and extortion groups' leak sites

Organization size	Lockbit	BlackCat	Royal
Small (1 to 200 employees)	76	30	40
Medium (201 to 1,000 employees)	32	22	19
Large (more than 1,001 employees)	23	20	8
Unknown	16	5	4
Total	147	77	71

Table 7. The distribution by organization size of LockBit, BlackCat, and Royal's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: LockBit, BlackCat, and Royal's leak sites and Trend Micro's OSINT research

OCT		NOV		DEC	
Locky	753	Wannaren	2,507	Locky	677
Cerber	379	Locky	718	Gorf	548
GandCrab	265	Hive	485	BlackCat	457
Hive	249	Cerber	348	Cerber	365
LockBit	194	Cryptophp	324	GandCrab	237
StopCrypt	160	GandCrab	247	Cobra	228
Magniber	157	BlackCat	194	LockBit	201
Crypwall	148	LockBit	185	Crypwall	146
Cobra	140	StopCrypt	182	Conti	111
Maze	123	Zeppelin	177	Cryptesla	101

Table 8. The top 10 ransomware families in terms of ransomware file detections in machines in the fourth quarter of 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

OCT		NOV		DEC	
Industry	File detections	Industry	File detections	Industry	File detections
Fast-moving consumer goods	1,213	Fast-moving consumer goods	1,657	Manufacturing	824
Manufacturing	793	Manufacturing	309	Fast-moving consumer goods	793
Government	260	Government	200	Retail	275

Table 9. The top three industries in terms of ransomware file detections in machines in each month of the fourth quarter of 2022

Source: Trend Micro Smart Protection Network

OCT			NOV			DEC		
Fast-moving consumer goods	Cerber	71	Fast-moving consumer goods	Cerber	98	Manufacturing	Cerber	39
	Locky	62		Locky	76		Locky	37
	Crypwall	50		GandCrab	62		GandCrab	27
Manufacturing	Cerber	36	Manufacturing	Vice Society	28	Fast-moving consumer goods	Cerber	46
	Locky	32		Gorf	7		Locky	37
	Crypwall	26		Roduk	7		Crypwall	27
Government	Cerber	11	Government	Cerber	6	Retail	Cerber	13
	Locky	7		Crilock	6		GandCrab	10
	Crilock	6		Babuk	5		Locky	8

Table 10. The top three industries in terms of ransomware file detections in machines in the top affected industries in each month of the fourth quarter of 2022

Source: Trend Micro Smart Protection Network

	OCT		NOV		DEC	
Enterprise	Locky	372	Wannaren	2,507	Gorf	515
	Cerber	283	Locky	364	BlackCat	441
	GandCrab	224	Hive	349	Locky	236
	Lockbit	133	Cryptophp	323	Cerber	220
	Crypwall	131	Cerber	270	Cobra	200
Consumer	Magniber	113	Locky	97	Locky	151
	Locky	105	StopCrypt	77	Cerber	58
	StopCrypt	95	Cerber	52	Lockbit	35
	Cerber	68	Magniber	45	Magniber	34
	Gorf	52	Gorf	33	Crawl	31
SMB	Hive	197	Hive	124	Cerber	71
	Black Basta	36	BlackCat	64	Locky	59
	BlackOat	36	Gorf	15	GandCrab	43
	LockBit	14	StopCrypt	13	Crypwall	35
	StopCrypt	8	Ransom	12	LockBit	26

Table 11. The top five ransomware families in terms of ransomware file detections in machines in each business segment in each month of the fourth quarter of 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

		OCT							
United States		Japan		Taiwan		Turkey		Brazil	
Total 1,860		Total 1,677		Total 1,478		Total 1,360		Total 955	
Locky	80	Locky	362	Magniber	135	Cerber	70	Maze	52
Black Basta	40	Cerber	72	StopCrypt	35	Locky	56	Zeppelin	16
BlackOat	40	LockBit	44	Roduk	26	Crypwall	48	GandCrab	15
Maze	32	GandCrab	42	Ako	21	GandCrab	48	Clop	11
Cerber	30	Crypwall	38	Cobra	17	Cryptesla	24	Filecoder	11
Babuk	18	DrodZp	38	BlackCat	12	Crilock	21	LockBit	11
Crawl	15	StopCrypt	21	Convagent	11	Sodinokibi	20	Scarab	10
GandCrab	13	Cryptoload	20	Gorf	8	BlackCat	20	Phobos	9
LockBit	13	Gorf	18	CryFile	8	LockBit	20	Babuk	8
Prestige	13	Cryptesla	14	LVRansomware	7	Cryptlock	19	Ransom	8

Table 12. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in October 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

NOV									
India		United States		Turkey		Japan		Taiwan	
Total 3,862		Total 3,289		Total 2,343		Total 1,177		Total 1,011	
Wannaren	2,507	Hive	348	Cerber	122	Locky	259	Magniber	50
Cobra	50	Cryptophp	276	Locky	101	Cerber	43	Ako	22
Locky	28	Locky	99	Crypwall	79	LockBit	29	StopCrypt	21
GandCrab	16	Maze	94	GandCrab	76	Cryptoload	20	Roduk	21
StopCrypt	8	BlackCat	35	Cryptesla	42	Gorf	18	Ransom	11
Holyghost	6	BlackBasta	32	LockBit	39	StopCrypt	17	Cobra	11
Zeppelin	6	Cerber	30	Crilock	38	DrodZp	16	Gorf	8
Wanna	5	LockBit	27	Conti	35	Crawl	11	CryFile	8
Efil	5	Clop	25	Spora	34	GandCrab	11	Crypmod	4
Bacucrypt	5	Filecorder	22	BlackCat	31	Small	10	Beuiran	4

Table 13. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in November 2022 (with notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

DEC									
Japan		Turkey		Colombia		United States		Taiwan	
Total 3,061		Total 2,137		Total 1,434		Total 1,103		Total 899	
Locky	410	Cerber	112	BlackCat	343	PLAYDE	32	Magniber	37
Cerber	156	Locky	89	Crypmo	1	Locky	30	Roduk	20
GandCrab	94	GandCrab	70	StopCrypt	1	BlackBasta	21	Ako	19
Crypwall	76	Crypwall	61			Cerber	20	Encoder	8
LockBit	55	Conti	40			Crawl	12	Cobra	8
Cryptesla	42	Spora	35			Royal	11	Gorf	7
Crilock	39	LockBit	35			BlackCat	8	LockBit	6
CRYPCTB	32	Cryptesla	35			GandCrab	7	Conti	6
Spora	31	Sodinokibi	33			NetWalker	6	Convagent	6
Sodinokibi	30	Crilock	33			Hive	6	Phobos	5

Table 14. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in December 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

LockBit

Industry	Victim count
Finance	14
IT	14
Healthcare	13
Manufacturing	13
Professional services	13
Others	80
Total	664

Table 15. The distribution by industry of LockBit's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: LockBit's leak site

Region	Victim count
North America	44
Asia-Pacific	42
Europe	34
Latin America and the Caribbean South	18
Middle East	4
Eastern Europe	4
Africa	1
Total	147

Table 16. The distribution by region of LockBit's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: LockBit's leak site

Country	Victim count
United States	35
United Kingdom	10
Canada	9
Australia	8
Brazil	7
Others	78
Total	147

Table 17. The distribution by country of LockBit's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: LockBit's leak site

BlackCat

Industry	Victim count
IT	11
Manufacturing	8
Healthcare	6
Media and entertainment	5
Legal services	5
Others	42
Total	77

Table 18. The distribution by industry of BlackCat's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: LockBit's leak site

Region	Victim count
North America	40
Europe	14
Asia-Pacific	12
Latin America and the Caribbean South	7
Africa	3
Others	1
Total	77

Table 19. The distribution by region of BlackCat's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: BlackCat's leak site

Country	Victim count
United States	37
Germany	4
Australia	3
Brazil	3
Canada	3
Others	27
Total	77

Table 20. The distribution by country of BlackCat's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: BlackCat's leak site

Royal

Industry	Victim count
IT	9
Finance	8
Materials	6
Healthcare	5
Food and staples	5
Others	38
Total	71

Table 21. The distribution by industry of Royal's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: Royal's leak site

Region	Victim count
North America	53
Europe	10
Latin America and the Caribbean South	4
Asia-Pacific	2
Africa	1
Middle East	1
Total	71

Table 22. The distribution by region of Royal's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: Royal's leak site

Country	Victim count
United States	45
Canada	8
Brazil	3
Germany	3
Australia	2
Others	10
Total	71

Table 23. The distribution by country of Royal's successful attacks in terms of victim organizations in the fourth quarter of 2022

Source: Royal's leak site



Trend Micro, a global cybersecurity leader, leverages decades of security expertise, research, and innovation to help make the world safe for exchanging digital information.

[TrendMicro.com](https://www.trendmicro.com)

Trend Micro
Research 