

LockBit, BlackCat, and Clop Prevail as Top RAAS Groups: Ransomware in 1H 2023

This data sheet collates relevant information on the ransomware threat landscape for the first and second quarters of 2023, 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 three most prominent ransomware families in the threat landscape during the six-month span. It should be noted that we did not include legacy ransomware families, or those that are not visibly active in the current threat landscape, in this report. Legacy ransomware family detections are also excluded from detection counts featured in this report.

	JAN	FEB	MAR	APR	MAY	JUN
Email threats	405,914	763,641	347,163	243,916	342,515	282,417
URL threats	134,885	174,322	202,212	172,920	145,080	116,907
File threats	414,687	526,668	678,976	860,947	575,094	309,589
Total	955,486	1,464,631	1,228,351	1,277,783	1,062,689	708,913
Total quarterly	3,648,468			3,049,385		

Table 1. The numbers of ransomware threats detected and blocked by Trend across email, URL, and file layers per month in the first and second quarters of 2023

Source: Trend Micro™ Smart Protection Network™

	Q1	Q2
Total active RaaS and extortion groups	27	42
Victim organizations	836	1,163

Table 2. The numbers of active RaaS and extortion groups and victim organizations of successful ransomware attacks in the first and second quarters of 2023

Sources: RaaS and extortion groups' leak sites

Q1		Q2	
Industry	Victim count	Industry	Victim count
Finance	67	Finance	131
IT	66	IT	118
Manufacturing	59	Healthcare	102
Healthcare	57	Manufacturing	96
Academe	55	Academe	80
Transportation	54	Construction	70
Professional services	53	Professional services	69
Construction	52	Materials	56
Materials	52	Transportation	47
Legal services	34	Legal services	46

Table 3. The top 10 industries affected by successful RaaS and extortion attacks in the first and second quarters of 2023

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

Segment	JAN	FEB	MAR	TOTAL
Enterprise	7,441	8,590	10,527	26,558
Consumer	1,902	2,258	2,012	6,172
SMB	1,804	1,242	1,572	4,618

Table 4. The number of ransomware file detections in machines in each business segment per month in the first quarter of 2023

Source: Trend Micro Smart Protection Network

Segment	APR	MAY	JUN	TOTAL	Percentage of increase in Q1 vs. Q2
Enterprise	8,969	8,733	10,968	28,670	8.0% increase
Consumer	1,506	1,815	1,863	5,184	16% decrease
SMB	1,127	954	1,214	3,295	28.7% decrease

Table 5. The number of ransomware file detections in machines in each business segment per month in the second quarter of 2023

Source: Trend Micro Smart Protection Network

Q1		Q2	
Country	Victim count	Country	Victim count
United States	397	United States	552
United Kingdom	64	United Kingdom	68
Canada	34	Canada	54
France	28	Germany	41
Germany	28	France	34
India	23	Brazil	32
Italy	22	Italy	29
Australia	20	Australia	27
Brazil	13	Spain	23
Spain	12	Unknown	24

Table 6. The top 10 countries affected by successful RaaS and extortion attacks in the first and second quarters of 2023

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

Q1		Q2	
Ransomware family	Number of victim organizations	Ransomware family	Number of victim organizations
LockBit	276	LockBit	246
Clop	107	BlackCat	130
BlackCat	82	Clop	95

Table 7. The top three ransomware families used in successful RaaS and extortion attacks in terms of victim organizations in the second and third quarters of 2023

Sources: RaaS and extortion groups' leak sites

Organization size	LockBit		BlackCat		Clop	
	Q1	Q2	Q1	Q2	Q1	Q2
Small (1 to 200 employees)	154	145	44	51	37	18
Medium (201 to 1,000 employees)	56	47	16	43	18	25
Large (more than 1,001 employees)	50	41	19	34	50	51
Unknown	16	13	3	2	2	1

Table 8. The distribution by organization size of LockBit, BlackCat, and Clop's successful attacks in terms of victim organizations in the first and second quarters of 2023

Sources: LockBit, BlackCat, and Clop's leak sites and Trend's OSINT research

JAN		FEB		MAR	
BlackCat	585	BlackCat	499	Black Basta	1,169
StopCrypt	530	StopCrypt	471	StopCrypt	494
LockBit	258	Black Basta	247	LockBit	290
Conti	139	Royal	210	BlackCat	210
Cryptesla	113	LockBit	208	Conti	152
Sodinokibi	94	Conti	125	Pentera	118
Crilock	93	Cryptesla	110	Cryptesla	111
Ryuk	76	Vicesociety	76	KlopRansom	105
Crysis	73	Sodinokibi	72	Crysis	100
Bacucrypt	71	Crilock	70	Targetcomp	91

Table 9. The top 10 ransomware families in terms of ransomware file detections in machines in the first quarter of 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

APR		MAY		JUN	
StopCrypt	466	StopCrypt	428	Playde	1,025
Black Basta	349	LockBit	422	Akirans	504
LockBit	224	Clop	244	LockBit	442
BlackCat	185	Conti	186	StopCrypt	353
Conti	127	BlackCat	160	BlackCat	203
Cryptesla	125	Sodinokibi	130	Conti	176
Mauicrypt	121	Cryptesla	125	Clop	165
Ransim	99	Alccrypt	95	Noko	137
Clop	89	Crilock	90	Sodinokibi	126
KlopRansom	84	Ryuk	88	Cryptesla	106

Table 10. The top 10 ransomware families in terms of ransomware file detections in machines in the second quarter of 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

JAN		FEB		MAR	
Industry	File detections	Industry	File detections	Industry	File detections
Fast-moving consumer goods	652	Banking	1,268	Banking	1,271
Retail	592	Retail	692	Manufacturing	1,055
Telecommunications	365	Technology	364	Retail	851

Table 11. The top three industries in terms of ransomware file detections in machines per month in the first quarter of 2023

Source: Trend Micro Smart Protection Network

APR		MAY		JUN	
Industry	File detections	Industry	File detections	Industry	File detections
Banking	1,905	Banking	1,342	Banking	1,525
Retail	764	Retail	719	Retail	600
Transportation	644	Transportation	716	Telecommunications	375

Table 12. The top three industries in terms of ransomware file detections in machines per month in the second quarter of 2023

Source: Trend Micro Smart Protection Network

JAN			FEB			MAR		
Fast-moving consumer goods	Conti	16	Banking	Cryptesla	28	Banking	Cryptesla	28
	Crilock	14		Crilock	24		StopCrypt	28
	LockBit	14		Spora	22		Crilock	24
Retail	Conti	15	Retail	Conti	16	Manufacturing	StopCrypt	10
	Cryptesla	14		Cryptesla	16		Occusa	7
	Crilock	12		Crilock	13		Roduk	6
Telecommunications	LockBit	9	Technology	Black Basta	79	Retail	Conti	27
	Scarab	7		BlackCat	13		BlackCat	20
	Clop	6		Hive	7		Cryptesla	14

Table 13. The top three industries in terms of ransomware file detections in machines in the top affected industries per month in the first quarter of 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

APR			MAY			JUN		
Banking	Cryptesla	38	Banking	LockBit	59	Banking	LockBit	35
	StopCrypt	37		Cryptesla	28		StopCrypt	31
	Crilock	35		Crilock	24		Cryptesla	28
Retail	Cryptesla	21	Retail	Conti	20	Retail	LockBit	20
	StopCrypt	17		Cryptesla	14		Conti	16
	Conti	15		Ryuk	14		Playde	13
Transportation	Conti	17	Transportation	Cryptesla	16	Telecommunication	Phobos	10
	Cryptesla	14		Conti	15		LockBit	10
	Crilock	12		Crilock	13		Scarab	7

Table 14. The top three industries in terms of ransomware file detections in machines in the top affected industries per month in the second quarter of 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

	JAN		FEB		MAR	
Enterprise	BlackCat	571	BlackCat	442	Black Basta	1,028
	LockBit	196	Royal	206	LockBit	221
	StopCrypt	190	StopCrypt	173	StopCrypt	198
	Conti	111	LockBit	156	BlackCat	184
	Cryptesla	91	Black Basta	113	Conti	136
Consumer	StopCrypt	261	StopCrypt	226	StopCrypt	225
	LockBit	41	LockBit	47	LockBit	62
	Magniber	34	Magniber	41	Magniber	48
	Crawl	20	Crawl	27	Crawl	25
	Polyransom	17	Conti	21	Ako	21
SMB	StopCrypt	49	Black Basta	134	Black Basta	141
	Ryuk	24	BlackCat	52	StopCrypt	51
	Sodinokibi	21	StopCrypt	38	BlackCat	22
	Crilock	20	Convagent	15	Vice Society	15
	Cryptesla	20	Makop	7	Convagent	15

Table 15. The top five ransomware families in terms of ransomware file detections in machines per business segment and per month in the first quarter of 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

	APR		MAY		JUN	
Enterprise	StopCrypt	302	LockBit	331	Playde	1,005
	Black Basta	265	StopCrypt	242	Akirans	466
	BlackCat	181	Clop	241	LockBit	275
	LockBit	164	Conti	167	StopCrypt	188
	Cryptesla	122	BlackCat	147	Clop	162
Consumer	StopCrypt	128	StopCrypt	143	StopCrypt	135
	LockBit	51	LockBit	70	LockBit	64
	Magniber	45	Magniber	39	ContiCrypt	40
	Crawl	19	PolyRansom	27	Encoder	29
	Polyransom	16	Conti	17	PolyRansom	29
SMB	Black Basta	82	StopCrypt	32	LockBit	102
	StopCrypt	27	Phobos	9	BlackCat	52
	Convagent	25	BlackCat	9	Akirans	36
	Ransim	21	Convagent	7	Avaddon	23
	Targetcomp	9	Sodinokibi	6		

Table 16. The top five ransomware families in terms of ransomware file detections in machines per business segment and per month in the second quarter of 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

JAN									
Turkey		Japan		United States		Brazil		Taiwan	
Conti	60	LockBit	46	LockBit	57	BlackCat	465	StopCrypt	66
Cryptesla	51	StopCrypt	32	StopCrypt	31	StopCrypt	24	Magniber	39
Crilock	44	Cryptesla	21	Ryuk	16	LockBit	8	Roduk	21
StopCrypt	42	Crilock	21	Convagent	11	Conti	5	Ako	12
Sodinokibi	40	Cryptoload	20	Crawl	10	Cryptesla	4	Encoder	8
LockBit	40	Spora	19	Royal	9	Azvo	4	Makop	7
Spora	36	Crypctb	17	Clop	8	Crysis	4	Crysis	6
BlackCat	34	Cryakl	16	BlackCat	8	Scarab	4	Clop	6
Crypmic	34	Sodinokibi	16	Virlock	7	Roadsweep	4	Cryptesla	6
Cryptlock	29	Cryptlock	16	Conti	7	Blackmagic	4	Phobos	6

Table 17. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in January 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

FEB									
Taiwan		United States		Italy		Turkey		Japan	
StopCrypt	48	Royal	196	BlackCat	20	StopCrypt	24	LockBit	34
Magniber	46	Black Basta	144	Crypctb	14	Conti	22	Cryptoload	23
Roduk	19	StopCrypt	38	Cryptesla	14	Cryptesla	18	StopCrypt	18
LockBit	19	Convagent	17	Crilock	12	LockBit	16	Inject	14
Cryptesla	17	Crawl	14	Spora	11	Crilock	14	Small	11
Conti	16	LockBit	13	Stopcrypt	11	Sodinokibi	13	Crawl	9
Encoder	15	Vicesociety	11	Cryptlock	10	Spora	13	Cryakl	8
Sodinokibi	13	Conti	11	Cryphydra	9	BlackCat	12	Reveton	7
Clop	13	Sodinokibi	10	LockBit	9	Lockergoga	12	Crypjaff	5
Phobos	11	BlackCat	9	Sodinokibi	8	Cryptlock	12	Nemucod	5

Table 18. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in February 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

MAR									
Turkey		United States		Taiwan		Kuwait		Canada	
BlackCat	110	Black Basta	247	Magniber	59	Cryptesla	28	Black Basta	701
Conti	67	StopCrypt	46	StopCrypt	48	Crilock	24	StopCrypt	3
LockBit	41	Royal	27	Roduk	15	Spora	22	Royal	3
Crilock	38	BlackCat	24	Ako	15	Conti	21	PolyRansom	3
Cryptesla	36	Convagent	19	Zeppelin	7	LockBit	20	Ako	3
StopCrypt	35	KlopRansom	15	Scarab	6	Cryptlock	20	Cryptoload	1
Sodinokibi	33	Vicesociety	15	Encoder	6	Cryphydra	18	Crysis	1
Spora	32	Trigona	14	Conti	6	Crypctb	16	LockBit	1
Cryptlock	28	Crawl	12	Paradise	6	Sodinokibi	16	Redniev	1
Cryphydra	28	LockBit	11	Blackmatter	5	Crypmic	16	HiddenTear	1

Table 19. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in March 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

APR									
United States		Turkey		Kuwait		Taiwan		Italy	
Black Basta	151	Conti	39	Cryptesla	28	Magniber	45	Crypctb	16
BlackCat	112	Cryptesla	33	Crilock	24	StopCrypt	37	Cryptesla	12
Ransim	41	LockBit	27	Spora	22	Ako	8	Crilock	11
Convagent	34	Crilock	26	Conti	21	Roduk	6	Spora	11
StopCrypt	31	BlackCat	25	Cryptlock	20	Encoder	3	LockBit	10
Royal	15	Spora	24	LockBit	20	LockBit	3	StopCrypt	10
LockBit	10	StopCrypt	24	Cryphydra	18	FakeGlobe	2	Cryphydra	9
Petya	9	Sodinokibi	21	Sodinokibi	16	Cryptolocker	2	Cryptlock	9
Conti	9	Cryphydra	20	Crypmic	16	Emper	2	Sodinokibi	8
Sodinokibi	8	Cryptlock	20	Crypctb	16	Derialock	2	Crypmic	8

Table 20. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in April 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

MAY									
Turkey		Kuwait		United States		Taiwan		Qatar	
Conti	68	Cryptesla	28	BlackCat	33	Magniber	40	Cryptesla	14
BlackCat	51	Crilock	24	LockBit	32	StopCrypt	39	Conti	14
LockBit	49	Conti	23	Stopcrypt	19	Ako	10	BlackCat	11
Sodinokibi	47	Spora	22	Convagent	16	LockBit	7	Spora	11
Cryptesla	43	Cryptlock	20	Black Basta	15	Roduk	7	LockBit	11
Crilock	35	LockBit	20	Conti	13	Phobos	5	Crilock	11
Cryptlock	30	Cryphydra	18	Polyransom	12	Clop	5	Cryptlock	10
Spora	30	Sodinokibi	17	Sodinokibi	12	Encoder	4	Cryphydra	9
Cryphydra	26	Crypmic	16	Clop	12	Cryptesla	4	Sodinokibi	8
Crypctb	26	Crypctb	16	Ransim	9	Conti	4	Ryuk	8

Table 21. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in May 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

JUN									
Turkey		Kuwait		Spain		United States		Japan	
Conti	76	Cryptesla	28	Playde	987	LockBit	113	LockBit	55
LockBit	73	LockBit	26	StopCrypt	6	Akirans	64	Inject	15
Sodinokibi	50	Crilock	24	Moneymess	4	StopCrypt	25	Cryptoload	14
Cryptesla	48	Spora	22	Ponyfinal	3	BlackCat	17	Petya	8
Crilock	43	Conti	22	Trigona	2	PolyRansom	15	Reveton	6
Blackbyte	40	Cryptlock	20	Noko	2	Encoder	13	StopCrypt	6
BlackCat	38	Cryphydra	18	Crosslock	2	Sodinokibi	12	DwnLdr	5
Clop	36	Sodinokibi	16	Avaddon	2	Crawl	11	Jaff	5
Cryphydra	33	Ishtar	16	Mimic	1	Echoraix	8	Small	5
Cryptlock	33	Crypmic	16	Alien	1	Esxiargs	8	Targetcomp	4

Table 22. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in June 2023, with notable ransomware families highlighted

Source: Trend Micro Smart Protection Network

LockBit

Q1		Q2	
Industry	Victim count	Industry	Victim count
IT	25	Manufacturing	29
Manufacturing	23	Finance	24
Finance	22	Construction	21
Professional services	22	Academe	19
Materials	21	IT	19
Others	163	Others	134
Total	276	Total	246

Table 23. The distribution by industry of LockBit's successful attacks in terms of victim organizations in the first and second quarters of 2023

Source: LockBit's leak site

Q1		Q2	
Region	Victim count	Region	Victim count
North America	113	North America	100
Europe	74	Europe	62
Asia-Pacific	47	Asia-Pacific	40
Latin America and the Caribbean	24	Latin America and the Caribbean	22
Middle East	10	Africa	8
Eastern Europe	5	Eastern Europe	7
Africa	3	Middle East	7
Total	276	Total	246

Table 24. The distribution by region of LockBit's successful attacks in terms of victim organizations in the first and second quarters of 2023

Source: LockBit's leak site

Q1		Q2	
Country	Victim count	Country	Victim count
United States	104	United States	90
France	16	France	11
United Kingdom	15	United Kingdom	11
India	12	Canada	10
Germany	11	Italy	9
Others	118	Others	115
Total	276	Total	246

Table 25. The distribution by country of LockBit's successful attacks in terms of victim organizations in the first and second quarters of 2023

Source: LockBit's leak site

BlackCat

Q1		Q2	
Industry	Victim count	Industry	Victim count
Legal services	8	Finance	18
Finance	7	IT	16
Healthcare	7	Professional services	12

Q1		Q2	
Industry	Victim count	Industry	Victim count
Academe	6	Healthcare	11
Food and staples	6	Manufacturing	10
Others	48	Others	63
Total	82	Total	130

Table 26. The distribution by industry of BlackCat's successful attacks in terms of victim organizations in the first and second quarters of 2023

Source: BlackCat's leak site

Q1		Q2	
Region	Victim count	Region	Victim count
North America	46	North America	75
Europe	16	Asia-Pacific	18
Asia-Pacific	11	Europe	16
Latin America and the Caribbean	4	Latin America and the Caribbean	10
Middle East	3	Africa	9
Africa	2	Middle East	2
Total	82	Total	130

Table 27. The distribution by region of BlackCat's successful attacks in terms of victim organizations in the first and second quarters of 2023

Source: BlackCat's leak site

Q1		Q2	
Country	Victim count	Country	Victim count
United States	42	United States	70
United Kingdom	6	Canada	5
Canada	4	Brazil	3
Australia	3	France	3
Italy	3	India	3
Others	24	Others	46
Total	82	Total	130

Table 28. The distribution by country of BlackCat's successful attacks in terms of victim organizations in the first and second quarters of 2023

Source: BlackCat's leak site

Clop

Q1		Q2	
Industry	Victim count	Industry	Victim count
Healthcare	14	Finance	35
IT	14	IT	15
Finance	13	Academe	10
Media and entertainment	6	Healthcare	8
Professional services	6	Manufacturing	4
Others	54	Others	23
Total	107	Total	95

Table 29. The distribution by industry of Clop's successful attacks in terms of victim organizations in the first and second quarters of 2023

Source: Clop's leak site

Q1		Q2	
Region	Victim count	Region	Victim count
North America	61	North America	68
Europe	16	Europe	22
Asia-Pacific	12	Asia-Pacific	3
Latin America and the Caribbean	10	Africa	1
Middle East	6	Middle East	1
Africa	2		
Total	107	Total	95

Table 30. The distribution by region of Clop's successful attacks in terms of victim organizations in the first and second quarters of 2023

Source: Clop's leak site

Q1		Q2	
Country	Victim count	Country	Victim count
United States	53	United States	62
United Kingdom	9	United Kingdom	6
Canada	8	Canada	5
Australia	4	Germany	5
Colombia	3	France	3
Others	30	Others	14
Total	107	Total	95

Table 31. The distribution by country of Clop's successful attacks in terms of victim organizations in the first and second quarters of 2023

Source: Clop'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

Trend Micro
Research 