LockBit, Conti, and BlackCat Lead Pack Amid Rise in Active RaaS and Extortion Groups

Ransomware in Q1 2022

This data sheet pertains to the ransomware threat landscape of the first quarter of 2022. Sourced 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 details the activity of ransomware in general and the ransomware families that dominated the landscape in particular during the period.

	Jan 2022	Feb 2022	Mar 2022
Email threats	306,754	697,369	1,853,566
URL threats	282,534	233,301	389,761
File threats	195,376	253,196	228,046
Total	**784,664**	**1,183,866**	**2,471,373**
Total threats: 4,439,903			

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

Source: Trend Micro™ Smart Protection Network™

	Jan 2021	Feb 2021	Mar 2021
Email threats	482,614	453,065	367,979
URL threats	749,403	641,479	693,569
File threats	280,069	405,963	183,902
Total	**1,512,086**	**1,500,507**	**1,245,450**
Total threats: 4,258,043			

Table 2. The numbers of ransomware threats detected and blocked by Trend Micro across email, URL, and file layers in each month of the first quarter of 2021

Source: Trend Micro Smart Protection Network

	Q1 2021	Q1 2022
Active RaaS and extortion groups	19	31
Victim organizations	476	615

Table 3. The numbers of active RaaS and extortion groups and of victim organizations of successful ransomware attacks in the first quarter of 2021 and the first quarter of 2022

Source: RaaS and extortion groups' leak sites

Industry	Victim count
Finance	57
IT	53
Manufacturing	45
Professional services	41
Construction	39
Materials	38
Healthcare	31
Transportation	30
Academe	28
Automobile	27

Table 4. The top 10 industries affected by successful RaaS and extortion attacks in terms of victim organizations in the first quarter of 2022

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

	Jan	Feb	Mar
Enterprise	15,889	16,019	14,314
Consumer	3,834	3,340	3,522
SMB	2,699	2,919	1,540

Table 5. The numbers of ransomware file detections in machines in each business segment in each month of the first quarter of 2022

Source: Trend Micro Smart Protection Network

Country	Victim count
US	243
UK	43
Italy	37
Germany	31
Canada	24

Country	Victim count
France	24
Spain	17
Brazil	13
Switzerland	11
Australia	10

Table 6. The top 10 countries affected by successful RaaS and extortion attacks in terms of victim organizations in the first quarter of 2022

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

Ransomware family	Victim count
LockBit	220
Conti	117
BlackCat	59

Table 7. The top three ransomware families used in successful RaaS and extortion attacks in terms of victim organizations in the first quarter of 2022

Source: RaaS and extortion groups' leak sites

Organization size	LockBit	Conti	BlackCat
Small (1 to 200 employees)	144	34	34
Medium (201 to 1,000 employees)	45	49	15
Large (more than 1,000 employees)	23	34	10
Unknown	8	0	0
Total	**220**	**117**	**59**

Table 8. The distribution by organization size of LockBit, Conti, and BlackCat's successful attacks in terms of victim organizations in the first quarter of 2022

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

Ransomware family	Victim count
WannaCry	12,110
Locky	3,714
Cerber	1,510
GandCrab	1,398
LockBit	919

Ransomware family	Victim count
Maze	874
StopCrypt	768
DarkSide	767
MountLocker	724
Conti	655

Table 9. The top 10 ransomware families in terms of ransomware file detections in machines in the first quarter of 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

Jan		Feb		Mar	
WannaCry	3,997	WannaCry	3,886	WannaCry	4,227
Locky	1,121	Locky	1,236	Locky	1,357
GandCrab	555	DarkSide	604	Cerber	543
Cerber	513	Cerber	454	GandCrab	406
Maze	378	GandCrab	437	StopCrypt	295
Conti	348	Purgen	414	LockBit	290
MountLocker	285	LockBit	386	BlackCat	232
LockBit	243	Maze	326	Crysis	223
StopCrypt	237	BlackCat	273	REvil	184
REvil	198	MountLocker	255	MountLocker	184
Others	14,670	Others	14,338	Others	12,371
Total	**22,545**	**Total**	**22,609**	**Total**	**20,312**

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

Source: Trend Micro Smart Protection Network

Jan		Feb		Mar	
Manufacturing	1,294	Government	1,216	Government	1,298
Finance	1,171	Finance	999	Finance	1,075
Government	1,048	Manufacturing	868	Fast-moving consumer goods	629

Table 11. The top three industries in terms of ransomware file detections in machines in each month of the first quarter of 2022

Source: Trend Micro Smart Protection Network

Jan			Feb			Mar		
Manufacturing	WannaCry	159	Government	WannaCry	1,072	Government	WannaCry	1,126
	Conti	6		WannaCrypt	7		Cerber	7
	Cerber	5		Cobra	4		Cobra	6
Finance	WannaCry	88	Finance	WannaCry	82	Finance	WannaCry	101
	GandCrab	71		GandCrab	45		BlackCat	55
	Cerber	46		Cerber	42		GandCrab	48
Government	WannaCry	929	Manufacturing	LockBit	163	Fast-moving consumer goods	Cerber	37
	Gorf	5		WannaCry	157		Locky	32
	Locky	4		Thanos	8		Crypwall	26

Table 12. The top three ransomware families in terms of ransomware file detections in machines in the top affected industries in each month of the first quarter of 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

	Jan		Feb		Mar	
Enterprise	WannaCry	3,597	WannaCry	3,463	WannaCry	3,804
	GandCrab	487	DarkSide	586	GandCrab	350
	Cerber	301	Purgen	410	Locky	315
	Locky	300	GandCrab	362	Cerber	278
	MountLocker	277	LockBit	329	LockBit	228
Consumer	Locky	769	Locky	684	Locky	402
	Cerber	190	StopCrypt	156	StopCrypt	236
	StopCrypt	166	Cerber	150	Cerber	177
	WannaCry	134	WannaCry	150	WannaCry	149
	Conti	117	Gorf	65	Gorf	62
SMB	WannaCry	256	WannaCry	273	WannaCry	272
	Maze	105	Maze	90	BlackCat	24
	LockBit	94	Locky	46	LockBit	21
	Conti	82	Cerber	45	Locky	19
	Locky	33	GandCrab	37	Macaw	17

Table 13. The top five ransomware families in terms of ransomware file detections in machines in each business segment in each month of the first quarter of 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

Jan									
US 3,964		India 2,196		Brazil 1,825		Japan 1,715		China 1,598	
Maze	261	WannaCry	898	WannaCry	165	Locky	726	WannaCry	336
Locky	157	GandCrab	92	GandCrab	83	Cerber	115	Hermes	24
Conti	99	MountLocker	65	MountLocker	55	Gorf	39	Conti	12
WannaCry	74	Egregor	42	Egregor	36	StopCrypt	37	Cobra	10
GandCrab	72	REvil	32	REvil	35	LockBit	29	Roduk	6
LockBit	71	Shade	30	Shade	30	GandCrab	28	Snatch	4
Cerber	69	Trytocry	30	Trytocry	27	Crawl	25	Cerber	3
Clop	64	Conti	28	DarkSide	27	Maze	21	GandCrab	3
Filecoder	53	StopCrypt	26	Conti	27	Fakeglobe	17	Gorf	3
Cryptesla	49	Sekhmet	24	Sekhmet	20	Nemucod	17	Ako	3

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

Source: Trend Micro Smart Protection Network

Feb									
US 4,045		India 2,218		Japan 1,976		Turkey 1,713		Malaysia 1,143	
LockBit	247	WannaCry	974	Locky	853	WannaCry	114	DarkSide	512
Maze	196	GandCrab	72	Cerber	102	Cerber	96	WannaCry	176
Babuk	121	BlackCat	71	WannaCry	30	Locky	78	Cerber	5
Locky	65	MountLocker	66	GandCrab	24	Crypwall	62	Locky	3
Cryptesla	64	Egregor	42	Gorf	24	GandCrab	54	Polyransom	2
WannaCry	60	REvil	41	LockBit	22	Cryptesla	35	StopCrypt	2
GandCrab	50	Shade	31	Maze	21	Crilock	28	REvil	2
Filecoder	45	StopCrypt	31	StopCrypt	18	Cryptlock	23	Winlock	1
Cerber	45	Trytocry	30	Crypwall	17	Cryphydra	23	Cryak	1
Clop	45	Conti	25	Reveton	13	Spora	23	Shade	1

Table 15. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in February 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

Mar									
US 2,458		Japan 2,011		India 1,777		Turkey 1,748		Taiwan 1,152	
Crysis	130	Locky	921	WannaCry	1,137	WannaCry	167	WannaCry	69
Locky	93	Cerber	129	StopCrypt	26	Cerber	109	BlackCat	43
Maze	82	Crawl	39	Lokilocker	23	Locky	74	Encoder	28
Cerber	62	LockBit	30	GandCrab	20	GandCrab	67	Roduk	26
LockBit	57	GandCrab	29	Gorf	19	Crypwall	63	Ako	18
BlackCat	64	Gorf	23	Polar	16	Cryptesla	34	GandCrab	15
Cryptlock	38	StopCrypt	21	Egregor	13	Spora	30	Cobra	14
Lokilocker	32	REvil	19	Cerber	13	Crilock	29	MountLocker	11
GandCrab	31	Crypwall	17	Wanna	13	Crypctb	26	Gorf	10
WannaCry	30	Agent	17	MountLocker	11	Cryptlock	26	Crysis	9

Table 16. The top 10 ransomware families in the top five countries in terms of ransomware file detections in machines in March 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

LockBit

Industry	Victim count
Finance	28
Construction	21
Manufacturing	21
IT	16
Professional services	16
Transportation	11
Academe	10
Hospitality	10
Real estate	10
Legal services	9
Materials	8
Foods and staples	7
Government	7
Healthcare	7
Retail	7
Apparel and fashion	6
Automobile	6
Media and entertainment	6
Community	5
Consumer goods and services	4

Industry	Victim count
Energy and utilities	2
Telecommunications	2
Trade	1
Total	**220**

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

Source: LockBit's leak site

Region	Victim count
Europe	89
North America	75
Asia-Pacific	24
Latin America and the Caribbean	16
Middle East	10
Africa	5
Unknown	1
Total	**220**

Table 18. The distribution by region of LockBit's successful attacks in terms of victim organizations in the first quarter of 2022

Source: LockBit's leak site

Country or region	Victim count
US	69
Italy	22
France	14
UK	13
Germany	8
Spain	8
Canada	6
India	6
Mexico	5
Brazil	4
China	4
Hong Kong	4
Singapore	4
Belgium	3
Czech Republic	3

Country or region	Victim count
Netherlands	3
Switzerland	3
Turkey	3
Australia	2
Argentina	2
Denmark	2
Lebanon	2
New Zealand	2
Poland	2
Portugal	2
Thailand	2
Austria	1
Bahrain	1
Bosnia and Herzegovina	1
Botswana	1
Cayman Islands	1
Chile	1
Colombia	1
Ecuador	1
Finland	1
Hungary	1
Isle of Man	1
Kuwait	1
Puerto Rico	1
Qatar	1
Republic of the Congo	1
Romania	1
Saudi Arabia	1
Senegal	1
South Africa	1
Tanzania	1
UAE	1
Unknown	1
Total	**220**

Table 19. The distribution by country or region of LockBit’s successful attacks in terms of victim organizations in the first quarter of 2022

Source: LockBit’s leak site

Conti

Industry	Victim count
Manufacturing	15
Materials	12
Professional services	12
Construction	9
Automobile	8
Finance	8
IT	8
Foods and staples	7
Media and entertainment	6
Retail	6
Transportation	6
Healthcare	5
Legal services	4
Apparel and fashion	3
Academe	2
Aerospace and defense	2
Energy and utilities	2
Hospitality	2
Real estate	2
Total	**117**

Table 20. The distribution by industry of Conti's successful attacks in terms of victim organizations in the first quarter of 2022

Source: Conti's leak site

Region	Victim count
North America	58
Europe	49
Asia-Pacific	7
Africa	1
Latin America and the Caribbean	1
Middle East	1
Total	**117**

Table 21. The distribution by region of Conti's successful attacks in terms of victim organizations in the first quarter of 2022

Source: Conti's leak site

Country	Victim count
US	52
Germany	16
UK	10
Italy	7
Canada	6
Australia	3
Netherlands	3
Sweden	3
Switzerland	3
Austria	2
New Zealand	2
Norway	2
Belgium	1
Brazil	1
Brunei	1
Denmark	1
Indonesia	1
Saudi Arabia	1
Serbia	1
Tunisia	1
Total	**117**

Table 22. The distribution by country of Conti's successful attacks in terms of victim organizations in the first quarter of 2022

Source: Conti's leak site

BlackCat

Industry	Victim count
Professional services	8
Finance	6
Legal services	6
Apparel and fashion	5
Materials	5
IT	4
Construction	3
Energy and utilities	3
Healthcare	3
Manufacturing	3
Academe	2

Industry	Victim count
Automobile	2
Foods and staples	2
Media and entertainment	2
Transportation	2
Real estate	1
Retail	1
Trade	1
Total	**59**

Table 23. The distribution by industry of BlackCat’s successful attacks in terms of victim organizations in the first quarter of 2022

Source: BlackCat’s leak site

Region	Victim count
North America	30
Europe	15
Asia-Pacific	11
Latin America and the Caribbean	2
Middle East	1
Total	**59**

Table 24. The distribution by region of BlackCat’s successful attacks in terms of victim organizations in the first quarter of 2022

Source: BlackCat’s leak site

Country or region	Victim count
US	27
Italy	4
Australia	3
Canada	3
China	3
France	3
Hong Kong	3
Spain	3
Bahamas	1
Brazil	1
Hungary	1
India	1
Indonesia	1

Country or region	Victim count
Netherlands	1
Romania	1
Switzerland	1
UAE	1
UK	1
Total	**59**

Table 25. The distribution by country or region of BlackCat's successful attacks in terms of victim organizations in the first quarter of 2022

Source: BlackCat's leak site

TREND MICRO™ | research

www.trendmicro.com