

Examining Erratic Modern Ransomware Activities

Ransomware in Q3 2021

This data sheet pertains to the landscape of ransomware families, both legacy and more modern threats, in the third quarter of 2021. Our data shows the activity of the families themselves and also the types of industries and enterprises that were targeted.

	JUL	AUG	SEP
Enterprise	16,443	15,174	16,344
Consumer	5,325	4,736	3,824
SMB	1,840	1,902	2,047

Figure 1. Ransomware file detections across business segments in the third quarter of 2021

	JUL		AUG		SEP	
Enterprise	WannaCry	5,800	WannaCry	5,550	WannaCry	5,550
	REvil	2,278	GandCrab	316	Cerber	339
	Locky	376	Locky	288	Locky	327
	Gandcrab	255	Cerber	195	Gandcrab	273
	Cerber	248	REvil	162	LockBit	209
Consumer	Locky	1,009	Locky	937	Locky	871
	Cerber	234	Cerber	166	Cerber	162
	WannaCry	233	WannaCry	151	WannaCry	153
	Ako	118	Gorf	141	Gorf	82
	Gorf	107	GandCrab	93	GandCrab	48
SMB	WannaCry	285	WannaCry	285	WannaCry	311
	REvil	225	LockBit	66	LockBit	109
	Locky	54	Locky	66	Maze	22
	Gorf	23	Cerber	22	Gorf	21
	Cerber	20	Maze	21	GandCrab	19

Figure 2. The top five ransomware families detected per business segment in the third quarter of 2021 (REvil and LockBit highlighted to show activity in connection with news reports)

	JUL		AUG		SEP	
WannaCry	6,330	WannaCry	6,005	WannaCry	6,016	
REvil	2,543	Locky	1,291	Locky	1,219	
Locky	1,439	GandCrab	427	Cerber	517	
Cerber	503	Cerber	384	LockBit	364	
GandCrab	325	REvil	204	GandCrab	328	
Maze	241	LockBit	188	Maze	213	
Ako	210	Maze	177	Crypwall	193	
Crypwall	163	Mount Locker	142	Cryptesla	178	
Cryptesla	161	Shade	119	Conti	165	
Ryuk	149	Cryptesla	117	REvil	161	
Others	11,701	Others	13,608	Others	13,061	
TOTAL	23,765	TOTAL	22,122	TOTAL	22,415	

Figure 3. The top ransomware families active in the third quarter of 2021 (notable families highlighted)

JUL		AUG		SEP	
Government	1,375	Healthcare	1,445	Government	1,883
Healthcare	1,311	Government	1,435	Healthcare	780
Telecommunications	937	Manufacturing	593	Finance	751

Figure 4. The top three industries in terms of ransomware file detections in the third quarter of 2021

JUL			AUG			SEP		
Government	WannaCry	1,248	Healthcare	WannaCry	362	Government	WannaCry	5,550
	Locky	5		Maze	47		Cerber	339
	Cerber	4		Clop	20		Locky	327
Healthcare	WannaCry	1,009	Government	WannaCry	1,274	Healthcare	WannaCry	316
	GandCrab	234		GandCrab	10		Maze	20
	Lockbit	233		LockBit	6		LockBit	9
Telecommunications	REvil	285	Manufacturing	WannaCry	367	Finance	WannaCry	125
	WannaCry	225		Locky	8		Cerber	46
	GandCrab	54		GandCrab	7		Locky	34

Figure 5. The top three ransomware families affecting the top-ranking industries in the third quarter of 2021 (notable families highlighted)

JUL									
US	4,986	India	2,157	Japan	1,656	Brazil	1,474	China	1,373
REvil	1,581	WannaCry	1,546	Locky	845	WannaCry	441	WannaCry	991
Locky	170	Locky	43	Cerber	114	Cerber	44	Ako	146
Maze	123	REvil	36	LockBit	47	Phobos	37	Locky	26
Cerber	123	GandCrab	21	Encoder	41	Locky	35	GandCrab	20
WannaCry	107	Ryuk	11	Gorf	33	Crypwall	26	Gorf	19
Cryptesla	62	Mount Locker	10	Crypwall	23	GandCrab	25	Conti	5
GandCrab	58	Makop	9	Exmas	23	Maze	23	Crysis	5
Clop	42	Cerber	9	WannaCry	20	Cryptesla	22	REvil	4
Crypwall	39	Gorf	8	REvil	17	REvil	15	Stampado	4
Crilock	34	Egregor	7	GandCrab	17	Ryuk	15	Irus	4

Figure 6. The top five countries in terms of ransomware file detections and the top 10 ransomware families detected in each in July 2021 (notable families highlighted)

AUG									
US	3,122	India	2,781	Brazil	1,787	Japan	1,779	Taiwan	1,294
Maze	105	WannaCry	1,400	Locky	342	Locky	922	WannaCry	127
WannaCry	65	GandCrab	124	Cerber	50	Cerber	105	Ako	37
Locky	54	Mount Locker	76	Locky	39	Gorf	58	GandCrab	28
LockBit	36	Egregor	53	GandCrab	32	LockBit	45	Gorf	21
Clop	36	REvil	52	Cryptesla	29	GandCrab	31	Cobra	17
Crypren	34	Gorf	51	Crypwall	26	Exmas	22	Mount Locker	10
Cerber	33	Shade	40	Ryuk	23	Encoder	20	Locky	10
REvil	32	Trytocry	39	Maze	22	Crypwall	18	Cerber	7
Filecoder	32	Sekhmet	30	REvil	18	WannaCry	16	Egregor	7
Hive	29	Conti	29	Crilock	16	Reveton	15	REvil	7

Figure 7. The top five countries in terms of ransomware file detections and the top 10 ransomware families detected in each in August 2021 (notable families highlighted)

SEP									
US	2,961	Turkey	1,981	India	1,906	Brazil	1,779	Japan	1,294
Maze	104	WannaCry	315	WannaCry	1,410	WannaCry	351	Locky	764
LockBit	81	Cerber	119	Gorf	45	Cerber	55	Cerber	109
Conti	62	Locky	84	Cryptesla	17	Lockbit	44	LockBit	41
Locky	60	GandCrab	71	Ramsil	11	GandCrab	32	Gorf	40
WannaCry	47	Crypwall	70	Makop	9	Crypwall	26	GandCrab	27
Cryptesla	30	Cryptesla	38	Phobos	8	Maze	24	WannaCry	18
Cerber	27	Crilock	33	Babuk	6	Cryptesla	20	Crypwall	16
Clop	25	Spora	31	Conti	6	DarkSide	18	REvil	13
Scarab	20	Cryptlock	27	Locky	5	LockBit	15	Reveton	13
Crawl	20	LockBit	26	GandCrab	5	REvil	14	Exmas	11

Figure 8. The top five countries in terms of ransomware file detections and the top 10 ransomware families detected in each in September 2021 (notable families highlighted)

