Online Appendices for "An Anatomy of Crypto-Enabled Cybercrimes" by Cong, Harvey, Rabetti, and Wu (2024)

Online Appendix A: Supplementary Tables

	2018	2019	2020	2021	2022-06
Bank Transfer or Payment	154.6	179.8	320.5	762.0	703.1
	15.6%	17.0%	21.1%	24.8%	32.3%
Cash	116.7	118.4	149.2	191.8	101.4
	11.8%	11.2%	9.8%	6.2%	4.7%
Check	78.4	71.4	87.6	153.4	82.2
	7.9%	6.8%	5.8%	5.0%	3.8%
Credit Cards	140.3	121.9	152.1	181.6	110.4
	14.2%	11.5%	10.0%	5.9%	5.1%
Cryptocurrency	12.1	33.5	132.8	755.4	728.8
	1.2%	3.2%	8.7%	24.6%	33.5%
Debit Card	77.5	89.2	117.4	140.6	90.6
	7.8%	8.4%	7.7%	4.6%	4.2%
Gift Card or Reload Card	78.0	103.0	125.4	233.1	113.5
	7.9%	9.8%	8.2%	7.6%	5.2%
Money Order	20.5	22.9	26.3	38.7	18.9
	2.1%	2.2%	1.7%	1.3%	0.9%
Other	8.9	5.9	5.8		
	0.9%	0.6%	0.4%	-	-
Payment App or Service	28.5	50.2	87.9	130.9	82.2
	2.9%	4.8%	5.8%	4.3%	3.8%
Wire Transfer	272.6	259.0	315.6	482.9	147.3
	27.6%	24.6%	20.8%	15.7%	6.8%
Total	988.1	1055.1	1520.7	3070.4	2178.5

Table A1: Fraud Report
(Source: Compiled from the Federal Trade Commission)

Month	Attacks	Paid (%)	BTC	USD
Apr-2018	2	0 (0%)	0	$0
May-2018	2	0 (0%)	0	$0
Jun-2018	9	0 (0%)	0	$0
Jul-2018	10	0 (0%)	0	$0
Aug-2018	3	1 (33.3%)	5	$34,869.85
Sep-2018	11	2 (18.2%)	25	$164,498.40
Oct-2018	5	2 (40%)	40	$191,390.96
Nov-2018	20	3 (15%)	25	$130,253.90
Dec-2018	12	4 (33.3%)	88	$353,911.52
Jan-2019	28	5 (17.9%)	58	$208,339.50
Feb-2019	83	16 (19.3%)	1026.75	$3,810,643.93
Mar-2019	82	18 (22.0%)	1,611.32	$6,409,714.78
April-2019	82	14 (17.1%)	611.32	$3,170,654.26
May-2019	94	14 (14.9%)	1,146	$6,986,710.59
Jun-2019	101	11 (10.9%)	1,291.50	$10,454,868.36
Jul-2019	115	21 (18.3%)	977	$10,711,931.78
Aug-2019	17	4 (23.5%)	201	$2,255,378.88
Sep-2019	5	1 (20%)	14	$144,861.12
Total	681	116 (17%)	7,109.89	$45,028,033.83

Table A2: Ransomware gang balance sheet - subsidiary operations (Source: Proprietary)

Month	BTC	**USD**
Apr-2018	10.8	$101,801.99
May-2018	6.94	$49,498.48
Jun-2018	214.56	$1,535,261.49
Jul-2018	172.34	$1,273,163.71
Aug-2018	136.41	$863,066.08
Sep-2018	120.78	$784,149.70
Oct-2018	98.03	$629,077.39
Nov-2018	143.04	$736,753.42
Dec-2018	272.00	$1,083,045.80
Jan-2019	268.30	$967,861.19
Feb-2019	1559.70	$5,733,383.91
Mar-2019	1874.57	$7,423,461.17
Apr-2019	1311.31	$6,829,461.58
May-2019	863.59	$5,822,328.66
Jun-2019	1450.85	$11,859,023.88
Jul-2019	1877.49	$20,469,207.08
Aug-2019	726.97	$7,560,106.32
Sep-2019	857.44	$8,313,096.59
Oct-2019	1601.26	$13,499,635.78
Nov-2019	2043.75	$17,093,244.81
Dec-2019	2079.35	$15,206,475.97
Jan-2020	1963.41	$17,096,847.69
Feb-2020	1329.21	$13,469,848.97
Mar-2020	315.00	$1,684,387.30
Apr-2020	253.00	$1,671,514.46
Total	21550.17	$161,755,703.50

Table A3: Ransomware gang balance sheet - umbrella operations (Source: Proprietary)

Online Appendix B: Example of Ransomware Negotiation

(Excerpt provided by the cyber security firm FoxIT)

–victim: "We thought we have almost 6 days left. Our leadership is currently reviewing the situation and determining the best resolution."

–attacker: "Until we waiting for your reply on situation. We stopped DDoS attack to your domain, you can switch on your website. As well your blog, where hidden. Nobody will see information about that, until we will not get in deal. We stopped already other instruments which already where processed today."

–victim: "Okay, thank you. We want to cooperate with you. We just need some time during this difficult situation."

–victim: "Can you please tell us what we will receive once payment is made?"

–attacker: "You will get: 1) full decrypt of your systems and files 2) full file tree 3) we will delete files which we taken from you 4) audit of your network"

–victim: "This situation is very difficult for us, and we are worried we may get attacked again or pay and you will still post our data. What assurances or proof of file deletion can you give us?"

–attacker: "We have reputation and word, we worry about our reputation as well. After successful deal you will get: 1) full file trees of your files 2) after you will confirm we will delete all information and send you as proof video, we are not interested in to give to someone other your own data. We never work like that."

Online Appendix C

Sample of Conti Group Internal Dialogue

2021-05-07T06:51:42.746008

bentley@q3mcco35auwcstmt.onion: Скажи, у Арматы брать ботов или возврат денег?

(translated: Tell me, do we buy bots from Armata or do we return the money?)

2021-05-07T12:54:34.685218

bentley@q3mcco35auwcstmt.onion: <Pulya> $5200 отправил, все что было.

(translated: <Pulya> Sent you $5200, that's all I had)

2021-05-07T12:54:34.685860

bentley@q3mcco35auwcstmt.onion: <Pulya> с меня $7300 верно? [21:32:59] <volhvb> Да верно.

(translated: <Pulya> I owe you $7300 right? [21:32:59] <volhvb> Yes, correct)

2021-05-07T12:54:34.686854

bentley@q3mcco35auwcstmt.onion: Куда переслать?

(translated: "Where do I send it to?")

2021-05-07T12:56:45.499523

stern@q3mcco35auwcstmt.onion: ботов надо.

(translated: We need the bots)

2021-05-07T12:57:09.894275

bentley@q3mcco35auwcstmt.onion: Понял. Куда закинуть что мне пуля вчера скинул?

(translated: Got it. Where do I send what Pulya sent me yesterday?)

2021-05-07T12:57:28.860578

stern@q3mcco35auwcstmt.onion: 1AXiwETqqQoA52Jk5CmJkbAPuW8nR7VUYz

Online Appendix D

Conti leader recruiting taskforce for blockchain project

2021-06-08T12:13:14.308514

Кто нибудь из нас есть кто считает себя гуру блокчейна, и трендов. Кто может знает куда идти в этом направлении и что разрабатывать... Какие у кого идеи.
(translated: Any of us who consider himself as guru of blockchain and trends. Who might know where to go in this direction and what to develop... What ideas anyone has.")

Online Appendix E

Conti leader stern urged technical team to get blockchain storage ready

2020-08-20T16:17:47.583774

strix@q3mcco35auwcstmt.onion: Уже поднял Sia + Nextcloud на дедике. Загрузил на Sia несколько файлов для теста. Эти файлы видны через веб-интерфейс Nextcloud и через WebDAV, но, похоже, там какая-то проблема с правами доступа, что ли. При попытке скачать существующие или залить новые файлы возникает ошибка. Пока разбираюсь. Там еще, пришлось даунгрейдить Nextcloud до версии 12 (текущая версия 19), т.к. storage backend для Sia давно не обновлялся. Возможно, придется пообщаться с разработчиками для разбирательства, почему не работает.
(translated: Already got Sia + Nextcloud up on the deck. Uploaded some files to Sia for the test. These files are visible through the Nextcloud web interface and through WebDAV, but there seems to be some access rights issue or something. When trying to download existing files or upload new files an error occurs. I am still figuring it out. There also, I had to downgrade Nextcloud to version 12 (the current version is 19) because the storage backend for Sia hasn't been updated in a long time. May have to talk to the developers to figure out why it's not working.)

2020-08-20T16:18:17.212121

stern@q3mcco35auwcstmt.onion: ага поня

(translated: alright, got it)

2020-08-20T16:18:21.683602

stern@q3mcco35auwcstmt.onion: надо систему наладить эту

(translated: we need to get this system up and running)

2020-08-20T16:18:23.687287

stern@q3mcco35auwcstmt.onion: это будущее

(translated: this is the future)

Online Appendix F

Ransomware Gangs Tracked by DarkTracer, May 2019 - July 2021

AKO

Astro Team

Avaddon

AvosLocker

BABUK LOCKER

CL0P

Conti

Cuba

DarkSide

DoppelPaymer

Egregor

Everest

Grief

Haron

Hive

LOCKDATA

LV

LockBit

Lorenz

MAZE

Marketo

Mount Locker

N3tw0rm

NEMTY

Nefilim

NetWalker

Noname

Pay2Key

Payload.bin

Prometheus

Pysa

Quantum

Ragnar_Locker

Ragnarok

RansomEXX

Ranzy Locker

Sekhmet

Sodinokibi (REvil)

Suncrypt

SynACK

Team Snatch

Vice Society

XING LOCKER

Online Appendix G

Bitcoin Abuse—Reported Addresses per Category

Panel A: Bitcoin Tumbler

Year-Month	Addresses	ReportCount	Transactions	TotalReceived (USD)	ReportCount (per address)
2018-Apr	3	6	8	1	2.0
2018-May	1	2	6	114	2.0
2018-Sep	1	2	12	1	2.0
2018-Oct	1	2	2	0	2.0
2018-Nov	1	10	0	0	10.0
2018-Dec	2	11	0	0	5.5
2019-Jan	8	21	2	0	2.6
2019-Feb	4	10	1,214	5	2.5
2019-Mar	7	27	3	0	3.9
2019-Apr	5	26	34	2	5.2
2019-May	3	21	0	0	7.0
2019-Jun	3	14	309	10	4.7
2019-Jul	1	20	0	0	20.0
2019-Aug	5	54	8	0	10.8
2019-Sep	5	10	232	263,979	2.0
2019-Oct	4	16	18	0	4.0
2019-Nov	3	59	21	0	19.7
2019-Dec	3	25	31,492	1,595	8.3
2020-Jan	3	17	323,919	575,743	5.7
2020-Feb	8	103	104,910	503,630	12.9
2020-Mar	8	22	321	20	2.7
2020-Apr	46	214	20,949	357,505	4.6
2020-May	17	54	562	3	3.2
2020-Jun	21	58	2,296	29	2.8
2020-Jul	20	57	124,769	411	2.8
2020-Aug	29	77	7,878	88,745	2.7
2020-Sep	21	178	4,800	29	8.5
2020-Oct	38	126	9,247	154	3.3
2020-Nov	29	263	4,211	86	9.1
2020-Dec	30	88	145,6176	3,884,375	2.9
2021-Jan	30	90	70,664	46,869	3.0
2021-Feb	33	108	8,632	304	3.3
2021-Mar	39	216	27,294	149,003	5.5
2021-Apr	26	81	52,979	34,841	3.1
2021-May	7	62	2,796	29,688	8.9
2021-Jun	2	9	412	279,905	4.5
2021-Jul	1	6	561	7	6.0
2022-Jan	3	45	894,519	1,101,168	15.0
2022-Feb	5	801	1,192,025	15,654,679	160.2
Grand Total	476	3,011	4,343,281	22,972,901	6.3

Table AO1: Bitcoin Abuse: Reported Addresses
(Source: Compiled from BitcoinAbuse.com—Additional information involved checking address history at Blockchain.com)

Panel B: Blackmail Scam

Year-Month	Addresses	ReportCount	Transactions	TotalReceived (USD)	ReportCount (per address)
2018-Sep	13	61	63	2	4.7
2018-Oct	143	739	258	15	5.2
2018-Nov	226	1,485	1,911	62	6.6
2018-Dec	199	2,222	376	22	11.2
2019-Jan	280	2,809	496	89	10.0
2019-Feb	241	2,608	2,006	552	10.8
2019-Mar	299	3,151	69,217	6,403	10.5
2019-Apr	298	3,926	272	24	13.2
2019-May	316	2,824	971	44,955	8.9
2019-Jun	142	2,533	429	25	17.8
2019-Jul	70	1,673	808	27	23.9
2019-Aug	107	2,811	3,657	134,371	26.3
2019-Sep	91	1,706	304	16	18.7
2019-Oct	66	924	471	13	14.0
2019-Nov	70	837	138	6	12.0
2019-Dec	48	1,325	444	11	27.6
2020-Jan	92	1,297	255	8	14.1
2020-Feb	58	516	228	7	8.9
2020-Mar	85	1,206	15,850	386,132	14.2
2020-Apr	2,326	11,496	6,563	522	5.0
2020-May	557	3,096	4,332	114	5.6
2020-Jun	94	1,286	3,293	7,041	13.7
2020-Jul	91	1,411	3,346	98	15.5
2020-Aug	84	1,245	1,715	121	14.8
2020-Sep	83	1,002	25,471	2,103	12.1
2020-Oct	116	1,058	3,010	166	9.1
2020-Nov	126	1,959	32,707	2,171	15.5
2020-Dec	79	1,712	8,595	458	21.7
2021-Jan	104	2,182	2,424	2,096	21.0
2021-Feb	128	2,010	6,068	8,678	15.7
2021-Mar	144	2,124	3,921	84	14.7
2021-Apr	118	1,493	2,606	92	12.6
2021-May	50	689	5,173	169	13.8
2021-Jun	17	524	451	8	30.8
2021-Jul	4	1,087	106	5	271.7
2021-Aug	8	461	127	3	57.6
2021-Sep	1	89	2	-	89.0
2021-Oct	2	57	9	1	28.5
2021-Dec	4	35	3,826	1,699	8.7
2022-Jan	1	5	-	-	5.0
2022-Feb	1	10	1,905	9,201	10.0
Grand Total	6,982	69,684	213,804	607,570	10.0

Table AO1: Bitcoin Abuse: Reported Addresses (Continued)

Panel C: Darknet Market

Year-Month	Addresses	ReportCount	Transactions	TotalReceived (USD)	ReportCount (per address)
2018-Sep	1	2	2	0	2.0
2018-Dec	2	8	-	-	4.0
2019-Jan	3	10	-	-	3.3
2019-Feb	6	376	54	4	62.7
2019-Apr	1	29	5	0	29.0
2019-Jun	3	16	828	35	5.3
2019-Jul	2	15	-	-	7.5
2019-Aug	3	6	15	0	2.0
2019-Sep	4	10	1,773	55	2.5
2019-Oct	2	6	37	0	3.0
2019-Nov	2	7	86	3	3.5
2019-Dec	3	9	57	13	3.0
2020-Jan	2	6	4	0	3.0
2020-Feb	6	21	1,313	21	3.5
2020-Mar	6	148	396	297,352	24.7
2020-Apr	3	32	-	-	10.7
2020-May	3	8	14	2	2.7
2020-Jun	3	6	185	1	2.0
2020-Jul	13	86	1,532	32	6.6
2020-Aug	13	48	19,210	777	3.7
2020-Sep	22	49	10,814	63	2.2
2020-Oct	10	35	111,084	68	3.5
2020-Nov	15	34	1,323	21	2.3
2020-Dec	19	55	2,573	101,651	2.9
2021-Jan	15	38	2,443	1,438	2.5
2021-Feb	11	33	3,454	11,418	3.0
2021-Mar	6	14	222	9	2.3
2021-Apr	10	81	3,491	74	8.1
2021-May	1	2	492	6	2.0
2021-Jul	1	24	4	0	24.0
2022-Jan	1	30	316	1	30.0
Grand Total	192	1,244	161,727	413,046	6.5

Table AO1: Bitcoin Abuse: Reported Addresses (Continued)

Panel D: Other

Year-Month	Addresses	ReportCount	Transactions	TotalReceived (USD)	ReportCount (per address)
2018-Aug	3	6	-	-	2.0
2018-Sep	5	14	18	1	2.8
2018-Nov	5	12	20	0	2.4
2018-Dec	7	21	21	1	3.0
2019-Jan	8	24	17	4	3.0
2019-Feb	7	19	168	4	2.7
2019-Mar	7	19	249	23	2.7
2019-Apr	8	21	365	13	2.6
2019-May	14	81	327	50,059	5.8
2019-Jun	10	34	240	18	3.4
2019-Jul	9	41	182	105	4.6
2019-Aug	9	20	499	584	2.2
2019-Sep	25	131	172,746	1,264,657	5.2
2019-Oct	8	42	230	6	5.2
2019-Nov	15	48	833	129	3.2
2019-Dec	12	35	39,066	3,397	2.9
2020-Jan	52	175	4,115	191	3.4
2020-Feb	58	186	900	94	3.2
2020-Mar	107	504	2,113	180	4.7
2020-Apr	173	872	4,173	3,743	5.0
2020-May	215	793	19,393	61,344	3.7
2020-Jun	76	245	4,023	489	3.2
2020-Jul	52	152	38,578	109,755	2.9
2020-Aug	74	275	277,464	5,106,884	3.7
2020-Sep	49	162	380,631	833,474	3.3
2020-Oct	70	206	15,194	642	2.9
2020-Nov	78	244	11,106	1,019,732	3.1
2020-Dec	46	136	57,543	1,538	3.0
2021-Jan	84	222	218,720	232,906	2.6
2021-Feb	73	225	10,179	1,104	3.1
2021-Mar	78	214	91,416	5,327,933	2.7
2021-Apr	63	199	20,818	6,530	3.2
2021-May	18	144	138,204	40,038	8.0
2021-Jun	1	10	108	35	10.0
2021-Jul	3	329	687	491	109.7
2021-Aug	2	14	30	0	7.0
2021-Sep	1	4	327	2	4.0
2021-Oct	4	25	1,176,552	37,019,698	6.2
2021-Nov	1	13	346,779	100,462,323	13.0
2022-Jan	1	7	131	1	7.0
Grand Total	1531	5,924	3,034,165	151,548,126	3.9

Table AO1: Bitcoin Abuse: Reported Addresses (Continued)

Panel E: Ransomware

Year-Month	Addresses	ReportCount	Transactions	TotalReceived (USD)	ReportCount (per address)
2017-Nov	1	2	27	1	2.0
2018-Jun	1	2	-	-	2.0
2018-Jul	2	4	-	-	2.0
2018-Aug	23	48	7	0	2.1
2018-Sep	58	265	87	11	4.6
2018-Oct	98	445	100	7	4.5
2018-Nov	147	611	49	2	4.2
2018-Dec	120	589	120	5	4.9
2019-Jan	289	2,588	629	46	8.5
2019-Feb	136	1,219	5,024	26,189	9.0
2019-Mar	142	1,476	13,935	53,437	10.4
2019-Apr	145	1,512	132	9	10.4
2019-May	140	2,066	404	27	14.8
2019-Jun	75	727	596	54	9.7
2019-Jul	48	995	163	10	20.7
2019-Aug	57	839	49	1	14.7
2019-Sep	83	1,189	4,308,846	127,108	14.3
2019-Oct	40	509	5,314	250	12.7
2019-Nov	46	581	57	2	12.6
2019-Dec	43	583	269	22	13.6
2020-Jan	46	1,479	78,159	29,460	32.1
2020-Feb	45	468	986	11	10.4
2020-Mar	57	976	864	23	17.1
2020-Apr	1979	9,702	3,491	1,950	4.9
2020-May	461	2,154	2,157	125	4.7
2020-Jun	69	840	2,217	120	12.2
2020-Jul	58	599	67,076	11,140,191	10.3
2020-Aug	69	905	3,999	575	13.1
2020-Sep	70	1,544	33,574	208,862	22.1
2020-Oct	71	522	7,423	244	7.3
2020-Nov	79	936	1,794	41	11.8
2020-Dec	53	708	11,895	1,836	13.4
2021-Jan	87	643	36,073	96,355	7.4
2021-Feb	79	710	8,588	13,724	9.0
2021-Mar	102	1,079	8,253	170	10.6
2021-Apr	71	630	3,337	68	8.9
2021-May	22	360	2,328	229	16.4
2021-Jun	6	265	7,618	118	44.2
2021-Jul	6	61	1,671	288	10.2
2021-Aug	6	81	391	5	13.5
2021-Sep	1	4	542	25	4.0
2021-Oct	2	24	17,212	150,376	12.0
2021-Nov	8	254	18,855	1,611,096	31.7
2021-Dec	15	591	1,047,264	142,579,357	39.4
2022-Jan	4	48	31,666	291,312	12.0
2022-Feb	3	86	38,477	32,472	28.7
Grand Total	5163	41,919	5,771,718	156,366,213	8.1

Table AO1: Bitcoin Abuse: Reported Addresses (Continued)

Panel F: Sextortion

Year-Month	Addresses	ReportCount	Transactions	TotalReceived (USD)	ReportCount (per address)
2019-Feb	6	29	2	-	4.8
2019-Mar	247	1,556	171	15	6.3
2019-Apr	239	2,365	211	17	9.9
2019-May	334	3,240	376	31	9.7
2019-Jun	102	1,335	147	9	13.1
2019-Jul	68	1,721	124	7	25.3
2019-Aug	105	926	31,511	33,804	8.8
2019-Sep	155	1,535	192	11	9.9
2019-Oct	62	927	111	4	14.9
2019-Nov	86	1,841	270	19	21.4
2019-Dec	68	1,038	199	13	15.3
2020-Jan	90	1,246	261	12	13.8
2020-Feb	55	1,008	354	9	18.3
2020-Mar	74	890	73	3	12.0
2020-Apr	4097	19,454	389	26	4.7
2020-May	602	2,898	311	11	4.8
2020-Jun	69	1,075	6,234	92	15.6
2020-Jul	42	1,248	100	5	29.7
2020-Aug	52	726	122	4	14.0
2020-Sep	51	909	475	10	17.8
2020-Oct	64	876	151	6	13.7
2020-Nov	105	1,863	422	15	17.7
2020-Dec	57	1,242	566	13	21.8
2021-Jan	77	1,373	110	3	17.8
2021-Feb	80	1,495	142	4	18.7
2021-Mar	125	2,227	228	3	17.8
2021-Apr	105	1,147	127	2	10.9
2021-May	40	959	683	8	24.0
2021-Jun	25	724	107	2	29.0
2021-Jul	5	236	11	0	47.2
2021-Aug	5	1,219	25	1	243.8
2021-Sep	1	137	7	1	137.0
2021-Oct	3	44	2	0	14.7
2021-Nov	2	202	6	0	101.0
2021-Dec	2	8	-	-	4.0
2022-Jan	4	177	16	2	44.2
2022-Feb	2	10	-	-	5.0
Grand Total	7306	59,906	44,236	34,163	8.2

Table AO1: Bitcoin Abuse: Reported Addresses (Continued)

Online Appendix H

Bitcoin Addresses Extracted from Conti Leaks

112qJRWfQCAqKzSk3ZcQnq1A1YwqyfLbgp
12KHi1L1KUNDjSvkG5j56FRNbFrud3ZjUU
12V63PHiX8FvEgyewX5W1D2QrdJJSawqQM
12YQDqmq3t6bCKPKMRWFmqrju4UMXbcqvF
12bsh5bc7wkVSRv25Qw6x3JYzuQDpZZ4zi
1347fBtFzZCrPq29yjRpct5f6Kq5uHZHHy
14HnaQfsQdtgVSNR91jLcbcKtdyddDfP6D
15QULY9y2HJj1i85LiJGMYWChhAqnGkCSx
15gjb8F5Zd8XRKBCgVxsr8ZuVzr7yBtnCN
169J9MvXSjJZUjarG7JXDD8qiQXZS4jj6A
16evvEiZ6HKkV9WAbysJfJG1Qa7DzJGUFp
172KVKhMqL5CU1HN884RbArzu5DDL5hwE3
17mc4Qm7ka9jhQEUB5LTxP3gW3tsDYUJGQ
1AXiwETqqQoA52Jk5CmJkbAPuW8nR7VUYz
1B8sFxkPtMqR86dkfd3rFT38A5tncCDZD8
1CwbkiHug1yw7HGdYxEtXk9nQFUc6GKxzj
1DF9qtzbja79o3yBAmgoX5wdsSSpaPD2mE
1DS9DVVD4K86ppQhg8ta9XFVEaaW7NXZfA
1DSp4woswZECAL9zdmmGeu1s7k1sGExFDh
1FWWRT88WjYbZp4NoRNEBgTGjRxhi2J9YM
1G5LWXMN42ueD2eWvm4zMrhXGihghHDgMq
1G5wLGHbsMmbRT7CdfmBA4aeR7RNwiG8FY
1GXrHar42EHxHNXM2nFkXQ5gpTMxdR5q5j
1GoAiu7jLbjNoVBvKX8Dba45G4J3BFL3tM
1H4JUerGtbh74dP2e4N2ogmATd5SR47iXN
1HFqLt3fbuewZe5ncJautgncS6hN1ZzX5r
1HtyXyCrshiJmLYNru7atpDMJrzG9mzwzf
1K4NVpT26qwtLp2yReFkgecPkqqQHVrVJd
1KBuDgmq8umdoAkdUQLp9YApeHuuKFeUWF
1KMRTrRYZABPnCnpqhzECMhjaF5sKCyeQK
1KQ5tkv7NWjG2a67fP6UzTc7egE6HWAXux
1KfDPgc6CiWb6Fnin1bLWi2moX1ViXANxW
1KkwkfQCB5VuwF8PnDHhw38EVGdCHK5fMk
1LCEGFc6Cwe194B6gavMcZ56o2pbftXqWk
1LLRL4vZajTtpjuBh5VpBD8zUg73CHUsq3
1LYiEgq9k3xSAddbqMZcsVTayJVoKbTFub
1MxtwUpH4cWAz4en4kqVNzAdx5gpk9etUC
1NVHhVjcPEWdUNpUjb3RaBWPw2WdvZ7JEk
1NqxPMSjDxEfJ2ozbFnGEoumDpL4Z8frKh
1PemRXvQ5nbDs6q19pCUzfd4kXVGovVoe3
1Q6SsW88b94a4P3Rxtfr4pRxvhqqJAWvEc
1QAprZhPZ3QkAFbo59YyxjAuHcLKduFsFn
1hLvH27BxAPbqx3R2fMCuuMPfS2gGDBJL
31inPQPChryvSPEnaXrBc6kmYH4NAqYnTR
32Bg4EsuNjxVJ9ZP2RWHv66ybZRHQotQS4
32zW4tVTk3SvWVvgFJUx8AYe4wGJQH6SGi
3351LRF9NrFH5v2CMZWsCv66tv5UAjX5Gn
33hiG13GTHTV2G8aZxzBJHBPBpDNevcK2B
33i6BL4HGNL7YSdPWDP9x2swdJinNLs5zu
35Z4UipuER5ZGprGUugcoxPWwZ43RXchPX
35aWyVRkYme3aKeezp6wsJVGeoYsCTH44Z
36M8QiR4tiT2HyqUocRParhzEf7q8smXBV
36UqDj8hGfZTVjpURvSnKtpJnJKjhYcvuY
36dmB68ZpeZZThy9SnCHoMvfqCKgZS1Grf
37JcnKmYGBT7H5fyWuthHnrJsQjcHrewDB
385weBHnfNpr4EhKCaLZTN6zGcczt4Fben
38ZcBm8BBEpVn4y7CkGL7yyyYPKMSsEvhP
393FUUZgie8iv8RxLKDuiyXx6TRCV9pmz7
395hQDyiBT16yt8jVVNj7WuZoQ4ouuFJcZ
396PgCGZf7FAK5Sxmxa9NhGRZECddT2mMv
39ApJGgEiLAV23rPbcma5Kn2yqFfzWWNnW
3A8xNfeK2dXdDHi5PtKjZFa48HFixTqdAv
3Abc4kZoDruwVZu6jERirKypok1EFmZZKt
3B7AmkZ8VVhKAAqCp4ZLNVbmGJQoZcaBc9
3C4MVjmXVu1vjJFfg4phf55L1LAscKa8dr
3C5MYb2bZvQMSGTnDhtvJnt72ByZeFLgtN
3CPbvktjKPiWcYu4PM4oVrQhvSQjCKnR59
3CvVwhowFkgoqEw2cZE5DmMYvsqRgtQVaH
3Cxt179UhfF4xkNQsytDmoJVWEJs1ERbZh
3E6GJ8Cmk7dBQE2maUisJfJNRdxB4ih1sN
3ESoHHu87mTrFNSNUaMVEfT3vYwRYGfSHQ
3FHwdzaSjv2trZZHkLCrXMKypCK4BwEcuy
3HKn3KR4FG5LBwPtB48axLRohpNnykyHAb
3HVdGfBobqwYH4SmMtVRcKXeSwdQjF3Khv

3HqUAxCJ3yv2WNQE3MQSjRKGLAQqGRA4rq
3HrDFf1Yj95PFeSR58kCthga3p9hcz9Nmw
3JDKxEidX2JhmusBDB3BRaCahucEiHcK8n
3JGbpCKLyNhWatqZWD2RC6Vs4kzmqtPLPW
3Jc3mTyYuRpP7hynPaStpDBPNNd8FYydzS
3KXtQMqQqNRx37a5A5JTSSnZwzqoTvmxJE
3LaDs8DLJCSiJDV8RYHGyk4EVjbVRvxC9A
3M9tAMuamLcCpifaCQPSH3Th5F4VwjmyWz
3MqifVVoWvgAq6L8opqHbk9jJw6vmgtN2n
3N4oho2uXfkFBfUAPtoPGLUXjHXqXV4vrJ
3NAn1bJ49deFB9MmKw1gfBVr5Vwu5KsVzr
3PC7zJHCuTUh8oNyJud9u72J2rGH7SZwaK
3PNoZtKdNxnCEzdSQegBMbZiUufrL6RtL1
3PsVm4PDNhrhwnVf8rsL72mH1CcyCP3etD
3PyFQL2UNfzBVwCi9GYqn2vYpMeamcoQqv
3QdNiLEpxKWQ6SoxULAo4xc48d5otumivR
3QsBgNCy4UwKkYXPLSucytEY4LyddZSSN9
bc1q0q5gsymkvp7vfpuexz0eq5csufxs60npza3ct5
bc1q0wxas9pmy86gk2ptm3gprxcp5mdx92sed3tjhr
bc1q2ca6jfml0fvnke43dm5ade3hzagjyjfmyqw2p8
bc1q2cjna87ayslzn63aqntt263etzxgdth55fdzjd
bc1q2pnhvfkx0x9cqh8q4z96aa50rqxxcutp65ymx8
bc1q2vtrs0tt52knglpc7qv9sydvzvmz8qegxyxaak
bc1q33uvkjlvyks7d2p3v5fz5xl3j0sazrsdh7qdn5
bc1q3efl4m2jcr6gk32usxnfyrxh294sr8plmpe3ye
bc1q3hefqfvzfdnagwr9dkxphlz2xs6zem5r87hygh
bc1q3j4rq3k5d7ru85pecqtahcndkgx530e3g54633
bc1q3stptj0pv6swqcyu6m5n74jamzmadsukn5ce7t
bc1q3ts2gkcfcx8a007gclltdcc47f9j4sx68cf7zn
bc1q47tlstrwpqf8uhwwzp30483upe6havrfqv0ecj
bc1q4cjrllm405ktv2rm0jsh4ja5k8q9r7vmxfdcne
bc1q4hxu7x9jjlx9wqx8sr6pq2gajr786gffgpw3ey
bc1q4qvnjchr3y9wpm78qlnr6659qrtnnt5pfgn6p5
bc1q546cv2zm9vc6mfy47t6ud98m9h058mvd6e6z8a
bc1q59g25qrrqnyvcl2jdmxh9y5c0tvnxzk4c4xrl6
bc1q5aqs5hrlt3wj5xrnj0craykgsq6h8mse3cftf8
bc1q69k8ll0jmxs4d29wztrdpn4dhyus5uh6pxqrfz
bc1q6gj8ymnjh863gmuvh2nc3462trrvzlxf2atzxn
bc1q70rw85x8m795nvkee56krg5t6nlwuh6wjl6ycg
bc1q7cd8rxvwuqgeh2ya9vk2ekr9qutthyklzkamf8
bc1q7mp0j2vq2xgt7mzha0kh8rqsp5ev3927hum30h
bc1q8m55q8gvsluzfqxqz9wfgkpcwgl9zxvsqv63ua
bc1q8qfesjc2slfwe8xv3l0rxwdexms006swf7gcur
bc1q93uacqvu2d2hv9zga7srv3jvqwjump26fcj23t
bc1q9klek9z8lwdnfka6f7ltsewm44a7ulcgkunvwg
bc1q9l9zx5ct4apdweyxfdwq8tdza93gefvl7v766r
bc1q9p5yyxsfwr987296yl5zselkczmp90uwzh95zl
bc1qa0klunvxhwwhxp0kced63250sczjdzltvr06tu
bc1qa273a36dgnrdqevnx0lftn99t2we306eu7gm2k
bc1qa2t2qweze4y545y3j5xlaqdwwjetsq082t0gqh
bc1qa68vp26dapzt09xc2fd99qg9uyt90k7n6h0xmg
bc1qa6kcfywen34duq6msagpdv9fffcu4d2ljh5pgq
bc1qah9yltjk556w375sdqqt2d4lltg49vkprgnsw7
bc1qaljhrp7md4j4ceua7q89q40p6qxwp0fk35ztwr
bc1qam9e2ux49ur53hqxlraxjjtspxv88gk0ncwja9
bc1qasgfdqnd4rxfw4m0wdjyqc3008amxvw8q2z6z4
bc1qc2gtz9eadvr9mf2xcptyatajakx93schz35aq7
bc1qc39qwc3nl2eyh2cu4ct6tyh9zqzp9ye993c0y2
bc1qc5sn0myjvc8lj7n5xs3qdq6k9t07xn6vtew2ze
bc1qc6fpzh8jkuy7l8nk44yx3dztz36ejwgkq8p5vf
bc1qc8nxs5uxh3vx4xpuxlkhkfysllg5tw9nr00spj
bc1qclzlkq8j3ckmulye0k5xpzfymsxxha735mlauf
bc1qd7f5t5vtadrlz0ms09qw4qqcgypgj7pnpastdd
bc1qdehfl7kjwy0tez8eugjwmgt8m4l6jv5hfgqk3t
bc1qdshsymz4u243ku66ysdqunu4d6wamhquxc386g
bc1qdsp0axxxdcm595jq3wfap33ewmunxy33qp03cv
bc1qdstkdj3m3cdckdmva7x5pk0qxz3ylaplun4kd4
bc1qdvmlyvaq46e53r8y6e4cyj4pq8cdf8fukj82x0
bc1qdxrwlru9hr0frts6sxjkeeevc9za5k32r3zsgx
bc1qed8hy4c2hz5m2dpyv7sf3q9p97lah4x5q5d28k
bc1qedxzh30gvh7l6lrp2nf59zf9efckka2rt2r9z4
bc1qf2lmqzwkvh6r82j7p4nx4negk3m59drj0wg6w0
bc1qfamjhlyec63dz3gvcum7s9guu3cp5n8v3hz7ud
bc1qfrmrz7nx6c62qdf6gqk65yajn2k89hfy9cum44
bc1qfx2mxw2shaek42zdgctzljp498ur8lqvvqzyxz
bc1qfyxsgmc5axdd09xfv0y2j7jl0ztpj735pj8dah
bc1qg285up24wyrfd9dwrnucwnpj247g70wxz48kg9
bc1qgd5ke95svytzhfkvjp2zhnlhhv42w0wqm0uhpx
bc1qgdnyyhjpsvlkyr7lwyxzpflzptzwwpjhswxdpa
bc1qggg5yarwhqde03f7qnltyyzt7gnqh66xsvrmcf
bc1qgqwavrqna87kqvr9tn8lk0w4uhudhp0avd5g3f
bc1qh7k79thm9lxwtrgxlxgdqun9lsvycp5gv0yucs
bc1qh83mkj8um9y7n5tqkfuyglyw9xnf55wdvn8j9q
bc1qhcfpza3zfd28g03ew485qrrsvy9jae5xvr9ydz
bc1qj320zssr8lp62ruuwfp0nj56007a36n0wa63ml
bc1qj6nnpnnn9a0zquvpd35azeruseqnxfs3jtmwcv

bc1qjez2nzlhntkmqzhnwr7nk784pvfn6srw3fncq6
bc1qk0nnkkk3sga4pjcvfx77l66etaz67m44ejahwx
bc1qkfuf2cd87w2u2frrlgatuhvuwj6clr8zyxlrum
bc1qkmyv5860pe24h9ytadkzgqltkjuuk9z9s027df
bc1qkqztlxw4uwfdn2xsymu3pk3p2pltw4w7helfhk
bc1qktkx0jynsfgmvlnern4zpnk8hy6u9h2zdtgtfz
bc1ql4myqe20sd0dpk5f407045qksj0gdcm278cfp5
bc1qlafd7lsrwrgfnszh5pl7tzsptcnm7jwz9zvh6a
bc1qlc0sla88psaxs9wyr0ef6zn30meff9zd72pncz
bc1qlhhgzzll4uqvd60teqn92y467kc04mj74jqudv
bc1qlkvs2jweujlms5jnrsllaxuq6zly4wvmxysty9
bc1qlms20gsjnmtkv25kp5r3jvglq5c8yzy45s6ejs
bc1qlrzkzc6nkpn9kj9krzen2rq8yfc3hc4yhcrz3h
bc1qlwef5kpsu6awedge9k3qsmthfwfq0d43kphdct
bc1qmdjxd98fnk83l5k8cpvc77f9rljr7942cq0sfz
bc1qmxdamtwnwts779k2jhqea4nd4ucqhnqh8tadmc
bc1qmy0vr0dgwk8m46mxl4pucgay3k0xv03772mn59
bc1qn3dv97k9ks7jl9764vy5s30t9vxhvmqg3ka0jv
bc1qnf6drcfl786d70wlhfytyr5xg3qqgknlsh8dc3
bc1qnm79vhfq5ss9qrsfgfgcztd58w3s7hwn24lc9u
bc1qnzg5lf5syvkldfnvxl6umstn6xk2czrstt3sk8
bc1qp04ykljcchpuufsmly6dutvjd8qtg3f563xxdw
bc1qp0ncqsk5hu0d3kwq2erypdqur2yjzypdc40du8
bc1qp80m6ljlvqd7rvp8nrlfq93el0nvzdhelnkqqj
bc1qp8kjvuqpy5u5rzrfc5jalqczvulknxek6zfdyw
bc1qpaz0c4d7m0xx7xfflyf4cuk2xsuxev5vtlmvhs
bc1qpelsktvc6d8tuuafqzkeuyddgdsck480s8t4th
bc1qphgsh952kqwcyvqexjfsmguv28dxlgd56ccnrn
bc1qptn5qsllcxmrndmwucelazjt0z68zkrgrlumy0
bc1qpwcdpjcvn4xll4jewpc8lqcfjr8tn5cj4hl23l
bc1qq6mq20rx2h7u77hp5azyqn9qrr2009quqvdld3
bc1qqefvkkldvz4t732rajkp53j82j073s6m5cku93
bc1qqkc9220l6dqh8jlslfsc4xf6wxgkga5uv02vm5
bc1qqp7nt7m7m9fju2uflds93u9n5du78q3mhx6qss
bc1qqtvk2hth8sjwwd7wfqhg9mav7x7ca9rccnnemf
bc1qr3w2ntxztyznys7mjmvl6wv5ywpgvj9c7nz0xe
bc1qr5wpxnxvqz7fy5a7a0l2qnklahdl64fqsnc49f
bc1qr8fw0xj28emurqhu8k7gj4llzgnxf4dejhl04h
bc1qrjdl409wyucrwnmveq50m63dvyy7d5ws6m50gg
bc1qrkusavjestgd6lud0rjpr47x4vs2udpqesjsn8
bc1qrqj988a305sgg2t4xcqqqlgqfzt87k5fk7a8f8
bc1qrr9v7txnjxxrqvpajan5ssmcntp5mwdn065jks
bc1qsm35q5gu8awj5cu2r3hrzecvcvs7sn8lxn2pfx
bc1qsnhfuxzprt9tdrwcp8uk0x504ye7uecf6a4aee
bc1qst63rewj2vmnnmftuhwg6hvy5rsce2dzlhk44n
bc1qstc4wgx4e2aqm4rtch0sxftr4g7gfq3fg8nwe7
bc1qt24rgc8gk3xmx6fzzdwxc2c92cmp7xa8lju4za
bc1qtdyul6azg4lfecpkyaq3gdvpypxgz2ap8cgd5f
bc1qteth4dl689n0cuh3n63r6azcagmj4wj2m9yvht
bc1qtjvs79cm5zghe95hr04e5cl9h2fh7x9chfmc6t
bc1qtk37tmu9s6556zg6d97v79hfl9xsz20ppyj4nm
bc1qtn42kyjuz0lc9w9gue72xr9m2a7jgsf3rk2vul
bc1qtnqw53pxxp3j0a7ttuurqzuzxnn66su8svwv6k
bc1qtqr3n2pa5h43c6pulqvr56c4gz4cw96sywdplf
bc1qtqtau58ej7gedrgg32u0r3vt5twnkmqkfk63l5
bc1qtsks6vals5hqdvk28gsumvsxlucypnlee9x72p
bc1qu2k6w8gf4k7e3hgwpml6vymjv93czlc7etzuy6
bc1qv4eevjn6va749j2ydepgahptpg5wmp2gculvgr
bc1qv4smajyuhyzzh0kj3r42js73qljykn4g7jmcaw
bc1qvahawe2w84mgqgspcgx4uyu0vgw6r9y96srcj2
bc1qve3zp5w6x858wz6v0ydxxyyktgjm4vyfja5ehz
bc1qvq60dqug0q9l6najzg4xtd6uxkym05tu49here
bc1qvr4p72n76sckcr69h88pazd6n76neyn93vvtpr
bc1qvyp2gg6heau0whkxvzvevwantg2rcchlrumfn0
bc1qw29f7cx035xaujcnhs6yjv70433cx078n923wh
bc1qwjg3qcugy8n6778783a4rrxvn4nvx58yjg07dt
bc1qwjz9p3qurgf5qnmmprhdhn8gg0d808knr9q825
bc1qxrnwauy7dunkm3jryv3x7mun5c3c4t0s59r9e8
bc1qxt3gt86tpyn87e8398l97m9kx3f3wrwlejdlal
bc1qxxe0uz8dp820mnl7q5w3a2z9y4zgq9cr6smlf6
bc1qy0gz9dhhck0nwg2nm5feeufczjms7m0vyvsmss
bc1qy2083z665ux68zda3tfuh5xed2493uaj8whdwv
bc1qy9s0z859gcvt62ydp9r4sy3cl83za36tjsnqpa
bc1qymfku42ak463uequgw3wqct0qk4jtlj2p250ck
bc1qyx35tjvwz5hepzefy8gsetcgaavrejgfpzuzrk
bc1qyz0mpmjewkjmmd6sc5s7j2zvce3ufg04d803sv
bc1qz8g58ym9lrln4kk87g4kks3hg82hr8hc858nd3
bc1qzgmx2k26pqcce03qf73c2j7072qp46zku4uuu6
bc1qzss3vt428z0kr6pm6sae5wtcxrfgn4edt8eetn

Online Appendix I

Ryuk Addresses Extract from Ransomwhere.re

12vsQry1XrPjPCaH8gWzDJeYT7dhTmpcjL

14aJo5L9PTZhv8XX6qRPncbTXecb8Qohqb

14dpmsn9rmdcS4dKD4GeqY2dYY6pwu4nVV

14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

15FC73BdkpDMUWmxo7e7gtLRtM8gQgXyb4

15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

162DVnddxsbXeVgdCy66RxEPADPETBGVBR

1C8n86EEttnDjNKM9Tjm7QNVgwGBncQhDs

1CN2iQbBikFK9jM34Nb3WLx5DCenQLnbXp

1CW4kTqeoedinSmZiPYH7kvn4qP3mDJQVa

1CbP3cgi1Bcjuz6g2Fwvk4tVhqohqAVpDQ

1ChnbV4Rt7nsb5acw5YfYyvBFDj1RXcVQu

1Cyh35KqhhDewmXy63yp9ZMqBnAWe4oJRr

1FRNVupsCyTjUvF36GxHZrvLaPtY6hgkTm

1K6MBjz79QqfLBN7XBnwxCJb8DYUmmDWAt

1KURvApbe1yC7qYxkkkvtdZ7hrNjdp18sQ

1Kx9TT76PHwk8sw7Ur6PsMWyEtaogX7wWY

1L9fYHJJxeLMD2yyhh1cMFU2EWF5ihgAmJ

1LKULheYnNtJXgQNWMo24MeLrBBCouECH7

1NuMXQMUxCngJ7MNQ276KdaXQgGjpjFPhK

3LE4u2csMS9y1MdfgBZ3pDmnDg7VCtX322

Online Appendix J

Conti Members' Email Addresses

0x00lord@q3mcco35auwcstmt.onion
8383@q3mcco35auwcstmt.onion
Hash@q3mcco35auwcstmt.onion
Stern@q3mcco35auwcstmt.onion
admin@q3mcco35auwcstmt.onion
admintest@q3mcco35auwcstmt.onion
admu@q3mcco35auwcstmt.onion
ahtung@q3mcco35auwcstmt.onion
ahtyng@q3mcco35auwcstmt.onion
air@q3mcco35auwcstmt.onion
airbnb1@q3mcco35auwcstmt.onion
alarm2@q3mcco35auwcstmt.onion
alarm@q3mcco35auwcstmt.onion
alaska@q3mcco35auwcstmt.onion
alert@q3mcco35auwcstmt.onion
ali@q3mcco35auwcstmt.onion
aloxa@q3mcco35auwcstmt.onion
alter@q3mcco35auwcstmt.onion
alto@q3mcco35auwcstmt.onion
andy@q3mcco35auwcstmt.onion
answer@q3mcco35auwcstmt.onion
atlant@q3mcco35auwcstmt.onion
atlas@q3mcco35auwcstmt.onion
axel@q3mcco35auwcstmt.onion
azot@q3mcco35auwcstmt.onion
badboy@q3mcco35auwcstmt.onion
baget@q3mcco35auwcstmt.onion
baly@q3mcco35auwcstmt.onion
balzak@q3mcco35auwcstmt.onion
band@q3mcco35auwcstmt.onion
baraka@q3mcco35auwcstmt.onion
barmen@q3mcco35auwcstmt.onion
baron@q3mcco35auwcstmt.onion
bash@q3mcco35auwcstmt.onion
batka@q3mcco35auwcstmt.onion
baxter@q3mcco35auwcstmt.onion
begemot@q3mcco35auwcstmt.onion
bekeeper@q3mcco35auwcstmt.onion
bentley@q3mcco35auwcstmt.onion
beny@q3mcco35auwcstmt.onion
best@q3mcco35auwcstmt.onion
bestofthebest@q3mcco35auwcstmt.onion
beta@q3mcco35auwcstmt.onion
bezdar@q3mcco35auwcstmt.onion
bill@q3mcco35auwcstmt.onion
billgeizh@q3mcco35auwcstmt.onion
bio@q3mcco35auwcstmt.onion
black@q3mcco35auwcstmt.onion
blackjob@q3mcco35auwcstmt.onion
blood@q3mcco35auwcstmt.onion
bloodrush@q3mcco35auwcstmt.onion
bob@q3mcco35auwcstmt.onion
boba@q3mcco35auwcstmt.onion
boby@q3mcco35auwcstmt.onion
bonen@q3mcco35auwcstmt.onion
booker@q3mcco35auwcstmt.onion
born@q3mcco35auwcstmt.onion
bourbon@q3mcco35auwcstmt.onion
bra@q3mcco35auwcstmt.onion
braun@q3mcco35auwcstmt.onion
brom@q3mcco35auwcstmt.onion
buggati@q3mcco35auwcstmt.onion
buh@q3mcco35auwcstmt.onion
bullet@q3mcco35auwcstmt.onion
bumer@q3mcco35auwcstmt.onion
buran@q3mcco35auwcstmt.onion
buri@q3mcco35auwcstmt.onion
buza@q3mcco35auwcstmt.onion
calmar@q3mcco35auwcstmt.onion
cameron@q3mcco35auwcstmt.onion
cany@q3mcco35auwcstmt.onion
carter@q3mcco35auwcstmt.onion
casper@q3mcco35auwcstmt.onion
caution@q3mcco35auwcstmt.onion
ceram@q3mcco35auwcstmt.onion
cert@q3mcco35auwcstmt.onion
cesar@q3mcco35auwcstmt.onion
chain@q3mcco35auwcstmt.onion
chaos@q3mcco35auwcstmt.onion
cheesecake@q3mcco35auwcstmt.onion
cherry@q3mcco35auwcstmt.onion
child@q3mcco35auwcstmt.onion
chip@q3mcco35auwcstmt.onion
chrom@q3mcco35auwcstmt.onion
cicada@q3mcco35auwcstmt.onion
clickclack@q3mcco35auwcstmt.onion
clipper@q3mcco35auwcstmt.onion
cnn@q3mcco35auwcstmt.onion
cobdoctor@q3mcco35auwcstmt.onion
Contisupport@q3mcco35auwcstmt.onion
cooler@q3mcco35auwcstmt.onion
cosmos@q3mcco35auwcstmt.onion
craft@q3mcco35auwcstmt.onion
creamsod@q3mcco35auwcstmt.onion
cruz@q3mcco35auwcstmt.onion
cuba@q3mcco35auwcstmt.onion
cybergangster@q3mcco35auwcstmt.onion
da@q3mcco35auwcstmt.onion
dallas@q3mcco35auwcstmt.onion
dandis@q3mcco35auwcstmt.onion
dandmen@q3mcco35auwcstmt.onion
dantis@q3mcco35auwcstmt.onion
darc@q3mcco35auwcstmt.onion
david@q3mcco35auwcstmt.onion
def@q3mcco35auwcstmt.onion

defender@q3mcco35auwcstmt.onion
delta@q3mcco35auwcstmt.onion
demetrius@q3mcco35auwcstmt.onion
demon@q3mcco35auwcstmt.onion
deploy@q3mcco35auwcstmt.onion
derek@q3mcco35auwcstmt.onion
derekson@q3mcco35auwcstmt.onion
dereksupp@q3mcco35auwcstmt.onion
dick@q3mcco35auwcstmt.onion
dino@q3mcco35auwcstmt.onion
doctor@q3mcco35auwcstmt.onion
dollar@q3mcco35auwcstmt.onion
doloto@q3mcco35auwcstmt.onion
dominik@q3mcco35auwcstmt.onion
domovoy@q3mcco35auwcstmt.onion
doomsday@q3mcco35auwcstmt.onion
dorirus@q3mcco35auwcstmt.onion
dove@q3mcco35auwcstmt.onion
driver@q3mcco35auwcstmt.onion
duke@q3mcco35auwcstmt.onion
duna@q3mcco35auwcstmt.onion
dylan@q3mcco35auwcstmt.onion
dylon@q3mcco35auwcstmt.onion
ed@q3mcco35auwcstmt.onion
efrain@q3mcco35auwcstmt.onion
electronic@q3mcco35auwcstmt.onion
elon@q3mcco35auwcstmt.onion
elvira@q3mcco35auwcstmt.onion
elvis@q3mcco35auwcstmt.onion
fasker@q3mcco35auwcstmt.onion
fast@q3mcco35auwcstmt.onion
fatboy@q3mcco35auwcstmt.onion
fergus@q3mcco35auwcstmt.onion
fff@q3mcco35auwcstmt.onion
finn@q3mcco35auwcstmt.onion
fire@q3mcco35auwcstmt.onion
fischer@q3mcco35auwcstmt.onion
flint@q3mcco35auwcstmt.onion
flip@q3mcco35auwcstmt.onion
fly@q3mcco35auwcstmt.onion
focus@q3mcco35auwcstmt.onion
fog@q3mcco35auwcstmt.onion
food@q3mcco35auwcstmt.onion
forbes@q3mcco35auwcstmt.onion
ford@q3mcco35auwcstmt.onion
forest@q3mcco35auwcstmt.onion
forum@q3mcco35auwcstmt.onion
forus@q3mcco35auwcstmt.onion
fox@q3mcco35auwcstmt.onion
frank@q3mcco35auwcstmt.onion
freebeer@q3mcco35auwcstmt.onion
frog@q3mcco35auwcstmt.onion
front@q3mcco35auwcstmt.onion
frost@q3mcco35auwcstmt.onion
fury@q3mcco35auwcstmt.onion
ganesh@q3mcco35auwcstmt.onion
gentleman@q3mcco35auwcstmt.onion
germes@q3mcco35auwcstmt.onion
ghost@q3mcco35auwcstmt.onion
gideon777@q3mcco35auwcstmt.onion
git@q3mcco35auwcstmt.onion
glad@q3mcco35auwcstmt.onion
globus@q3mcco35auwcstmt.onion
gm@q3mcco35auwcstmt.onion
goga@q3mcco35auwcstmt.onion
gold@q3mcco35auwcstmt.onion
golova@q3mcco35auwcstmt.onion
good@q3mcco35auwcstmt.onion
goodwin@q3mcco35auwcstmt.onion
gorec@q3mcco35auwcstmt.onion
graf@q3mcco35auwcstmt.onion
grafin@q3mcco35auwcstmt.onion
grajdanin@q3mcco35auwcstmt.onion
gram@q3mcco35auwcstmt.onion
grand@q3mcco35auwcstmt.onion
grant@q3mcco35auwcstmt.onion
green@q3mcco35auwcstmt.onion
gringo@q3mcco35auwcstmt.onion
grom@q3mcco35auwcstmt.onion
grossman@q3mcco35auwcstmt.onion
grover@q3mcco35auwcstmt.onion
guava@q3mcco35auwcstmt.onion
gucci@q3mcco35auwcstmt.onion
gus@q3mcco35auwcstmt.onion
hash@q3mcco35auwcstmt.onion
hitech@q3mcco35auwcstmt.onion
hlor@q3mcco35auwcstmt.onion
hod@q3mcco35auwcstmt.onion
hof@q3mcco35auwcstmt.onion
hopkins@q3mcco35auwcstmt.onion
hors@q3mcco35auwcstmt.onion
horse@q3mcco35auwcstmt.onion
host@q3mcco35auwcstmt.onion
huanivan@q3mcco35auwcstmt.onion
idgo@q3mcco35auwcstmt.onion
ilon@q3mcco35auwcstmt.onion
impact@q3mcco35auwcstmt.onion
inat@q3mcco35auwcstmt.onion
info@q3mcco35auwcstmt.onion
inkognito@q3mcco35auwcstmt.onion
ivanalert@q3mcco35auwcstmt.onion
jafar@q3mcco35auwcstmt.onion
jax@q3mcco35auwcstmt.onion
johnyboy77@q3mcco35auwcstmt.onion
jumbo@q3mcco35auwcstmt.onion
kagas@q3mcco35auwcstmt.onion
kaktus@q3mcco35auwcstmt.onion
kent@q3mcco35auwcstmt.onion
kerasid@q3mcco35auwcstmt.onion
kerberos@q3mcco35auwcstmt.onion
kevin@q3mcco35auwcstmt.onion
keykey@q3mcco35auwcstmt.onion
killer@q3mcco35auwcstmt.onion
kingston@q3mcco35auwcstmt.onion
kintaro@q3mcco35auwcstmt.onion
klaus@q3mcco35auwcstmt.onion
kolbasa@q3mcco35auwcstmt.onion
kolin@q3mcco35auwcstmt.onion
koncord@q3mcco35auwcstmt.onion
kramer@q3mcco35auwcstmt.onion

kran@q3mcco35auwcstmt.onion
kurt@q3mcco35auwcstmt.onion
larry@q3mcco35auwcstmt.onion
lemur@q3mcco35auwcstmt.onion
leo@q3mcco35auwcstmt.onion
licor@q3mcco35auwcstmt.onion
loadsupport1@q3mcco35auwcstmt.onion
loadsupport2@q3mcco35auwcstmt.onion
loft@q3mcco35auwcstmt.onion
log@q3mcco35auwcstmt.onion
logan@q3mcco35auwcstmt.onion
lom@q3mcco35auwcstmt.onion
longer@q3mcco35auwcstmt.onion
love@q3mcco35auwcstmt.onion
lucas@q3mcco35auwcstmt.onion
macallan@q3mcco35auwcstmt.onion
macros@q3mcco35auwcstmt.onion
mango@q3mcco35auwcstmt.onion
many@q3mcco35auwcstmt.onion
marcus@q3mcco35auwcstmt.onion
mario@q3mcco35auwcstmt.onion
mark@q3mcco35auwcstmt.onion
marsel@q3mcco35auwcstmt.onion
mashroom@q3mcco35auwcstmt.onion
master@q3mcco35auwcstmt.onion
matiz@q3mcco35auwcstmt.onion
mavalek@q3mcco35auwcstmt.onion
mavelak@q3mcco35auwcstmt.onion
mavelek@q3mcco35auwcstmt.onion
mavemat@q3mcco35auwcstmt.onion
max17@q3mcco35auwcstmt.onion
max@q3mcco35auwcstmt.onion
meatball@q3mcco35auwcstmt.onion
mentos@q3mcco35auwcstmt.onion
merch@q3mcco35auwcstmt.onion
merlin@q3mcco35auwcstmt.onion
miguel@q3mcco35auwcstmt.onion
miner@q3mcco35auwcstmt.onion
modar@q3mcco35auwcstmt.onion
modnik@q3mcco35auwcstmt.onion
moms@q3mcco35auwcstmt.onion
mont@q3mcco35auwcstmt.onion
moon@q3mcco35auwcstmt.onion
mops@q3mcco35auwcstmt.onion
morgan@q3mcco35auwcstmt.onion
morisson@q3mcco35auwcstmt.onion
mors@q3mcco35auwcstmt.onion
mozart@q3mcco35auwcstmt.onion
muchacho@q3mcco35auwcstmt.onion
muhoboi@q3mcco35auwcstmt.onion
mult@q3mcco35auwcstmt.onion
mushroom@q3mcco35auwcstmt.onion
n@q3mcco35auwcstmt.onion
naned@q3mcco35auwcstmt.onion
nanswer@q3mcco35auwcstmt.onion
nbaraka@q3mcco35auwcstmt.onion
ncany@q3mcco35auwcstmt.onion
ncheesecake@q3mcco35auwcstmt.onion
nContisupport@q3mcco35auwcstmt.onion
ndandis@q3mcco35auwcstmt.onion
ndriver@q3mcco35auwcstmt.onion
nek@q3mcco35auwcstmt.onion
nelon@q3mcco35auwcstmt.onion
neo@q3mcco35auwcstmt.onion
netman@q3mcco35auwcstmt.onion
netwalker@q3mcco35auwcstmt.onion
nevada@q3mcco35auwcstmt.onion
nick@q3mcco35auwcstmt.onion
nidgo@q3mcco35auwcstmt.onion
njax@q3mcco35auwcstmt.onion
njumbo@q3mcco35auwcstmt.onion
nkaktus@q3mcco35auwcstmt.onion
nkintaro@q3mcco35auwcstmt.onion
nmarsel@q3mcco35auwcstmt.onion
nmavemat@q3mcco35auwcstmt.onion
nmeatball@q3mcco35auwcstmt.onion
noman@q3mcco35auwcstmt.onion
nponetre@q3mcco35auwcstmt.onion
nprizrak@q3mcco35auwcstmt.onion
nprofessor@q3mcco35auwcstmt.onion
nrevers@q3mcco35auwcstmt.onion
nsubzero@q3mcco35auwcstmt.onion
ntramp@q3mcco35auwcstmt.onion
nuggets@q3mcco35auwcstmt.onion
oldtimes@q3mcco35auwcstmt.onion
oliver@q3mcco35auwcstmt.onion
olsen@q3mcco35auwcstmt.onion
oscar@q3mcco35auwcstmt.onion
page@q3mcco35auwcstmt.onion
painkiller@q3mcco35auwcstmt.onion
panda@q3mcco35auwcstmt.onion
paranoik@q3mcco35auwcstmt.onion
parker@q3mcco35auwcstmt.onion
perry@q3mcco35auwcstmt.onion
phantom@q3mcco35auwcstmt.onion
pin2@q3mcco35auwcstmt.onion
pin@q3mcco35auwcstmt.onion
pincus@q3mcco35auwcstmt.onion
pineapple@q3mcco35auwcstmt.onion
poll@q3mcco35auwcstmt.onion
ponetre@q3mcco35auwcstmt.onion
porovoz@q3mcco35auwcstmt.onion
price@q3mcco35auwcstmt.onion
private@q3mcco35auwcstmt.onion
prizrak@q3mcco35auwcstmt.onion
professor@q3mcco35auwcstmt.onion
proffjeck@q3mcco35auwcstmt.onion
pumba@q3mcco35auwcstmt.onion
quite@q3mcco35auwcstmt.onion
qwerqwerqwerqwer@q3mcco35auwcstmt.onion
qwerty@q3mcco35auwcstmt.onion
qwertycatt@q3mcco35auwcstmt.onion
ramon@q3mcco35auwcstmt.onion
rand@q3mcco35auwcstmt.onion
redmond@q3mcco35auwcstmt.onion
redroom@q3mcco35auwcstmt.onion
reshaev@q3mcco35auwcstmt.onion
revan@q3mcco35auwcstmt.onion
revers@q3mcco35auwcstmt.onion
romanov@q3mcco35auwcstmt.onion

romanov_2@q3mcco35auwcstmt.onion
rooty@q3mcco35auwcstmt.onion
rox@q3mcco35auwcstmt.onion
rozetka@q3mcco35auwcstmt.onion
salamandra@q3mcco35auwcstmt.onion
sand@q3mcco35auwcstmt.onion
sandy@q3mcco35auwcstmt.onion
santi@q3mcco35auwcstmt.onion
savage@q3mcco35auwcstmt.onion
sega@q3mcco35auwcstmt.onion
sentinel@q3mcco35auwcstmt.onion
sepvilk@q3mcco35auwcstmt.onion
serp@q3mcco35auwcstmt.onion
seven300@q3mcco35auwcstmt.onion
shamm@q3mcco35auwcstmt.onion
shaper@q3mcco35auwcstmt.onion
shark@q3mcco35auwcstmt.onion
sharn@q3mcco35auwcstmt.onion
shell@q3mcco35auwcstmt.onion
sirafim@q3mcco35auwcstmt.onion
skippy@q3mcco35auwcstmt.onion
skywalker@q3mcco35auwcstmt.onion
slojno@q3mcco35auwcstmt.onion
slon@q3mcco35auwcstmt.onion
snow@q3mcco35auwcstmt.onion
sonar@q3mcco35auwcstmt.onion
song@q3mcco35auwcstmt.onion
soul@q3mcco35auwcstmt.onion
specter@q3mcco35auwcstmt.onion
spider@q3mcco35auwcstmt.onion
spoon@q3mcco35auwcstmt.onion
staff@q3mcco35auwcstmt.onion
stakan@q3mcco35auwcstmt.onion
star@q3mcco35auwcstmt.onion
starfall@q3mcco35auwcstmt.onion
stefan@q3mcco35auwcstmt.onion
steller@q3mcco35auwcstmt.onion
stern@q3mcco35auwcstmt.onion
steve@q3mcco35auwcstmt.onion
sticks@q3mcco35auwcstmt.onion
stigg@q3mcco35auwcstmt.onion
strix@q3mcco35auwcstmt.onion
subzero@q3mcco35auwcstmt.onion
summit@q3mcco35auwcstmt.onion
sunday@q3mcco35auwcstmt.onion
swift@q3mcco35auwcstmt.onion
taker@q3mcco35auwcstmt.onion
talar@q3mcco35auwcstmt.onion
taobao@q3mcco35auwcstmt.onion
target@q3mcco35auwcstmt.onion
tatarin@q3mcco35auwcstmt.onion
taur@q3mcco35auwcstmt.onion
terry@q3mcco35auwcstmt.onion
test@q3mcco35auwcstmt.onion
tibone@q3mcco35auwcstmt.onion
tiktak@q3mcco35auwcstmt.onion
tilar@q3mcco35auwcstmt.onion
tiniles@q3mcco35auwcstmt.onion
tnt@q3mcco35auwcstmt.onion
tom@q3mcco35auwcstmt.onion
toris@q3mcco35auwcstmt.onion
tort@q3mcco35auwcstmt.onion
total@q3mcco35auwcstmt.onion
tramp@q3mcco35auwcstmt.onion
troy@q3mcco35auwcstmt.onion
trumen@q3mcco35auwcstmt.onion
trump@q3mcco35auwcstmt.onion
tunotif@q3mcco35auwcstmt.onion
tunri@q3mcco35auwcstmt.onion
twin@q3mcco35auwcstmt.onion
twister@q3mcco35auwcstmt.onion
urban@q3mcco35auwcstmt.onion
urbanone@q3mcco35auwcstmt.onion
v1cev1@q3mcco35auwcstmt.onion
valemy@q3mcco35auwcstmt.onion
vampire@q3mcco35auwcstmt.onion
van@q3mcco35auwcstmt.onion
vang@q3mcco35auwcstmt.onion
veron@q3mcco35auwcstmt.onion
vertu@q3mcco35auwcstmt.onion
victor@q3mcco35auwcstmt.onion
viper@q3mcco35auwcstmt.onion
void@q3mcco35auwcstmt.onion
voron@q3mcco35auwcstmt.onion
watson@q3mcco35auwcstmt.onion
weav@q3mcco35auwcstmt.onion
wertu@q3mcco35auwcstmt.onion
wind@q3mcco35auwcstmt.onion
winston@q3mcco35auwcstmt.onion
workman1@q3mcco35auwcstmt.onion
workman2@q3mcco35auwcstmt.onion
wowddoz@q3mcco35auwcstmt.onion
xargs@q3mcco35auwcstmt.onion
xenkee@q3mcco35auwcstmt.onion
xenon@q3mcco35auwcstmt.onion
xmoney@q3mcco35auwcstmt.onion
xnull@q3mcco35auwcstmt.onion
xoc@q3mcco35auwcstmt.onion
xxx@q3mcco35auwcstmt.onion
zevs@q3mcco35auwcstmt.onion
zloysobaka@q3mcco35auwcstmt.onion
zolotoy@q3mcco35auwcstmt.onion
zulas@q3mcco35auwcstmt.onion

Online Appendix K:

Top Ransomware Variants

The success of ransomware has prompted many different cybercrime groups to develop their own variants. Some of the most prolific and famous ransomware variants include:

- REvil: REvil, also known as Sodinokibi, was famous for being one of the ransomware variants with the highest demands. REvil suddenly ceased operations in July 2021 after a famous attack on Kaseya.
- LockBit: LockBit ransomware is a RaaS variant that first emerged in September 2019, when it was called the ABCD ransomware (due to its .abcd file extension). In July 2021, LockBit infected Accenture, stealing internal data and encrypting servers that were later restored from backups.
- WannaCry: WannaCry is the ransomware variant that started the recent surge in ransomware attacks. The original variant of WannaCry used EternalBlue, an NSA-developed exploit leaked by the ShadowBrokers, to spread via vulnerable versions of Windows' SMB.
- Conti: Conti is a ransomware-as-a-service (RaaS) group, which allows affiliates to rent access to its infrastructure to launch attacks. Industry experts have said Conti is based in Russia and may have ties to Russian intelligence.
- Ryuk: Ryuk is a very targeted ransomware variant that demands high ransoms from its victims. In July 2021, the average Ryuk ransom payment was $691,800.
- CryptoLocker: CryptoLocker is an early ransomware variant that mainly operated from September 2013 to May 2014. Operation Tovar, which took down the Gameover ZeuS botnet, largely killed this ransomware variant.
- Petya: Petya is a family of ransomware variants. Unlike most ransomware, these variants encrypt the Master Boot Record (MBR) rather than individual files.
- Locky: Locky is a ransomware variant that first began spreading in 2016. It was used by multiple different cybercrime gangs and inspired other ransomware variants.
- Bad Rabbit: Bad Rabbit was a short-lived ransomware variant that is attributed to BlackEnergy, the makers of NotPetya. Unlike NotPetya, which was a wiper masquerading as ransomware, paying the Bad Rabbit ransom enabled recovery of the encrypted files.
- DarkSide: DarkSide is a now-defunct ransomware group most famous for its attack on Colonial Pipeline in May 2021. The group is now believed to operate under the name BlackMatter.
- DearCry: DearCry is a ransomware variant developed by the HAFNIUM group to exploit the Microsoft Exchange vulnerabilities reported in March 2021.

WannaCry

The widespread malware and the damage it caused meant that the three-day attack carried an estimated global cost in the billions. Organizations like the UK's National Health Service (NHS), which ran many vulnerable machines, were hit hard. The cost of Wannacry to the NHS alone is estimated to be US$100 million. The 2017 outbreak was only stopped by the discovery of a "kill switch" within the WannaCry code, which, when triggered, stopped the malware from spreading further or encrypting the data stored on any additional machines.

Unlike many other ransomware variants, WannaCry spreads independently rather than being carried by malicious emails or installed via malware droppers. WannaCry's worm functionality comes from its use of the EternalBlue exploit, which takes advantage of a vulnerability in Windows' Server Message Block (SMB) protocol. After this vulnerability came out to the public, Microsoft released an updated version of SMB that corrected the issue in April 2017. However, the patch came just a month before WannaCry's outbreak, spreading out fastly and infecting several organizations across the globe that did not yet patch their Windows. WannaCry spread rapidly because infected machines searched on the internet for other machines running a vulnerable version of SMB. Then, the infected machine used EternalBlue to send and run a copy of WannaCry on the targeted computer. At this point, the malware would then encrypt the computer's files. However, first, it checks for the existence of a particular website. If the website exists, then the malware does nothing (this "kill switch" could have been coded on WannaCry as a way to stop the spread of the malware). If the requested website is not found, WannaCry proceeds to the encryption stage.

The WannaCry malware demanded a ransom of US$300 from its victims to be paid in Bitcoins. As a cryptocurrency, Bitcoin is less traceable than traditional types of currency, which is helpful for ransomware operators since it allows them to embed a payment address (similar to a bank account number) in a ransom message without it immediately alerting the authorities to their identity. If a victim of a WannaCry attack pays the ransom, they should be provided with a decryption key for their computer. This enables a decryption program provided by cybercriminals to reverse the transformation performed on the user's files and return access to the original data.

DarkSide

First discovered in August 2020, the group is supposedly made up of experienced cybercriminals from various ransomware groups. DarkSide is a recent entrant to the Ransomware as a Service (RaaS) space, where they develop Ransomware and sell it to other cybercriminals. This makes it possible for cybercriminals to specialize in certain areas. The DarkSide group focuses on developing and improving their malware, while their customers specialize in gaining access to target networks and delivering the malware to critical or valuable systems within them. The DarkSide group made headlines for a ransomware attack against Colonial Pipeline, which transports about half of the fuel to the East Coast of the United States. This attack crippled the pipeline's operations, causing

a complete shutdown for multiple days and causing the US government to announce a state of emergency due to the attack posing a potential national security threat.

The DarkSide ransomware group performs highly-targeted attacks. The group claims to be apolitical and is focused on making money but does not want to cause societal problems. As part of this, the group has published a list of what it considers "acceptable targets" for an attack. Once the DarkSide ransomware gains access to a target environment, it begins by collecting and exfiltrating sensitive and valuable data from the business. This is because DarkSide performs "double extortion" attacks, where victims that do not pay the ransom to decrypt their files are threatened with the exposure of their data unless the demand is met. The DarkSide group maintains a website called DarkSide Leaks, where they publish the data of those targets that refuse to pay the ransom.

After stealing the data and encrypting infected computers, the DarkSide group sends a ransom demand tailored to the particular target. Based on the size and resources of the target company, ransom demands can vary from $200,000 to 20$ million. To increase their chance of a payoff, the DarkSide group performs in-depth research on a company to identify key decision-makers and maximize the demanded ransom while ensuring it is within the target organization's ability to pay. As a RaaS vendor, the DarkSide group focuses on improving its malware to make it more effective and difficult to detect and block. The group has recently released version 2.0 of the malware, which has already been implemented in recent campaigns.

Maze

Maze became popular among ransomware gangs by pioneering the "double extortion" ransom method back in 2019. In the past, ransomware operated on a simple business model: encrypt peoples' files and then demand a ransom if they want to regain access. However, this approach only works if the target pays the ransom. Some ransomware victims could restore from backups, while others just accepted the data loss. The Maze ransomware group modified its strategy by combining a traditional ransomware attack and a data breach within a single campaign. They would gain access to an organization's network, steal sensitive information, then encrypt everything. Maze typically gains access via phishing emails, then uses various techniques to move laterally through the network, enabling it to infect more machines. If the target refused to pay the ransom, the Maze group would publicly threaten to expose their stolen data or sell it to the highest bidder. This approach increased Maze's probability of success because the publication of stolen data may cause an organization to lose competitive advantage (if intellectual property and trade secrets are revealed to a competitor) and potentially run afoul of data protection regulations (due to the loss of customer data protected by the GDPR, CCPA, etc.). ncrypt the data.

Ryuk

The operators behind the Ryuk ransomware take a targeted approach to select and infect their victims. Rather than attempting to infect computers and asking for a relatively small ransom, Ryuk ransomware campaigns focus

on a single organization. They have an extremely high asking price for data recovery. For this reason, Ryuk is commonly spread via very targeted means. These include using tailored spear phishing emails and exploiting compromised credentials to remotely access systems via the Remote Desktop Protocol (RDP). With RDP, a cybercriminal can install and execute Ryuk directly on the target machine or leverage their access to reach and infect other, more valuable systems on the network. A spear-phishing email may carry Ryuk directly or be the first in a series of malware infections.

Ryuk uses a combination of encryption algorithms, including a symmetric algorithm (AES-256) and an asymmetric one (RSA 4096). The ransomware encrypts a file with the symmetric algorithm and includes a copy of the symmetric encryption key encrypted with the RSA public key. Upon payment of the ransom, the Ryuk operator provides a copy of the corresponding RSA private key, enabling decryption of the symmetric encryption key and, using it, the encrypted files. Ransomware poses a severe threat to the stability of an infected system if it encrypts the wrong files. For this reason, Ryuk deliberately avoids encrypting certain file types (including .exe and .dll) and files in specific folders on the system. While not a foolproof system, this decreases the probability that Ryuk will break an infected computer, making file retrieval more difficult or impossible even if a ransom is paid.

Ryuk is one of the most expensive ransomware variants, with average ransom demands reaching more than US$100,000 in the first quarter of 2020. Although paying a ransom should result in the cybercriminal sending a decryption key and software capable of decrypting the victim's files, in some cases, the provided key did not work. One version of the Ryuk ransomware decryptor had an error in the code that dropped the last byte when decrypting a large file. While this last byte is just padding in some file formats, in others, it is critical to interpreting the file. As a result, some of Ryuk's victims did not regain all their encrypted files even after paying the ransom.

Online Appendix L: Chain Abuse

Category	Total	Total (%)	Bitcoin	Ethereum	Other Chains
Other Blackmail	89,274	31.76%	89,000	206	68
Sextortion	68,026	24.20%	68,000	15	11
Ransomware	54,016	19.22%	54,000	7	9
Phishing	24,014	8.54%	511	23,000	503
Impersonation	5,305	1.89%	1,457	3,586	262
Fake Returns	928	0.33%	495	273	160
Romance	332	0.12%	203	84	45
Hack - Other	681	0.24%	187	317	177
Donation Impersonation	207	0.07%	128	61	18
Fake Project	322	0.11%	104	133	85
Pigbutchering	276	0.10%	85	143	48
Rug Pull	305	0.11%	79	144	82
NFT Airdrop	488	0.17%	22	187	279
Contract Exploit	354	0.13%	17	215	122
SIM Swap	26	0.01%	9	13	4
Other Investment	4	0.00%	2	1	1
Other	36,504	12.99%	36,000	383	121
Total	281,062	100%	250,299	28,768	1,995

Table L1: Chain Abuse reports. The category Others includes BSC, Tron, Polygon, Solana, Litecoin, Arbitrum, Avalanche, Cardano, Hedera, MultiversX, and Algorand. (Source: Compiled from chainabuse.com in January 2024).

Username	**Upvotes**	Reports	Joined
0xSaiyanGod	10,000	10,000	Dec-22
CryptoScamDB	9,829	9,828	Nov-22
AustrianSimon	7,254	7,253	Apr-23
BlockMageSec	678	678	Dec-22
BeatsPerHour	474	467	Apr-23
WeaveSec	526	420	Sep-22
phillipscagney	390	388	Sep-23
iamdeadlyz	354	346	Jun-22
noscam	265	264	Apr-23
OKHotshot	232	232	Feb-23
CivicMe	233	202	Sep-22
Datalytics	585	198	Oct-22
rpolysec	182	181	Jun-22
ZachXBT	172	167	Jun-22
scamreportin8	148	143	Jun-22

Table L2: User Ranking. (Source: Compiled from chainabuse.com in January 2024).

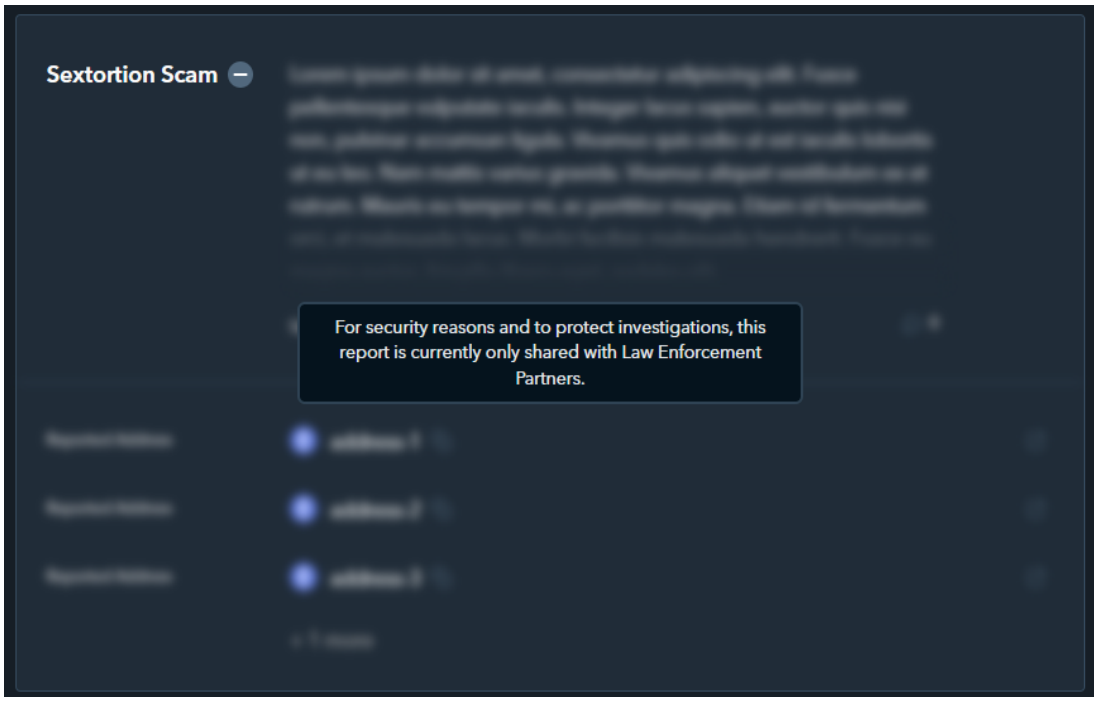

Figure L1: Example of Partial Observability due to Law Enforcement.