Targeted Threats to Civil Society Dataset v1.0 (Oct 2021)

Author	Lennart Maschmeyer, Senior Researcher, ETH Zurich
Motivation	This project highlights an understudied aspect of cyber conflict, targeted digital threats to civil society. Civil Society Organizations are routinely targeted by the same advanced threat actors as states and large organizations, but rarely receive the same attention in media reports or research. Consequently, there is a lack of comprehensive data on this issue. This dataset aims to improve this situation by tracking threats to civil society in the best available source of comprehensive data: public reporting by the infosec industry.
Data	Since the aim is comprehensiveness, data is collected from all available public reporting by the infosec industry and by independent research centers. Inclusion criteria for reports are threefold: 1) they must be public, 2) they must concern targeted threats and 3) they were published by an infosec firm.
Funding	This project was made possible by a generous grant by Columbia University's School of International and Public Affairs and the Carnegie Corporation of New York.
Notes	This is a work in progress, if you notice any errors, missing reports or other issues, please let me know.
Contact	lennart.maschmeyer@sipo.gess.ethz.ch

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
184	Stuxnet Under the Microscope	ESET	2010	https://www.welivesecurity.	N					0.6897794951	
241	Aurora Botnet Command Structure	Damballa	2010	https://paper.seebug.org/pa	N					0.5775371117	
406	OPERATION AURORA DETECT, DIAGNOSE, RESPOND	HBGary	2010	https://paper.seebug.org/pa	N			China		0.341150283	
425	Cyber Attacks on Google and Others—Who Is Really at Risk?	TrendMicro	2010	https://blog.trendmicro.com	N					0.305920176	
457	Combating Operation Aurora	McAfee	2010	https://paper.seebug.org/pa	N					0.2562701372	
521	In-depth Analysis of Hydraq	CA ISBU	2010	https://paper.seebug.org/pa	Y	2	Hydraq / Aurora	China	China	0.1680269701	
532	CASE STUDY: OPERATION AURORA	Triumfant	2010	https://github.com/kbandla/	N					0.1462861292	
23	Have I Got Newsforyou: Analysis of Flamer C&C Server	Symantec	2011	https://www.symantec.com/	N					0.9389157069	
67	Trojan.Taidoor	Symantec	2011	https://www.symantec.com/	N		Taidoor	not attributed	Taiwan, United States	0.9163187415	
91	Highly Targeted Attacks and the Weakest Links	TrendMicro	2011	https://blog.trendmicro.com	N					0.8442757408	
195	W32.Stuxnet Dossier	Symantec	2011	https://www.symantec.com/	N					0.6685467134	
210	The Nitro Attacks	symantec	2011	https://www.symantec.com/	Y	2	Nitro	Not attributed	Not specified	0.6381523811	
245	**Stuxnet/Duqu: The Evolution of Drivers**	Kaspersky	2011	https://securelist.com/stuxn	N					0.5707776578	
356	Alleged APT Intrusion Set: “1.php” Group	Zscaler	2011	https://www.zscaler.com/pd	N					0.4047963831	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
359	**Duqu Trojan Questions and Answers**	SecureWorks	2011	https://www.secureworks.co	N					0.4038930401	
374	Advanced Persistent Threats: A Decade in Review	Command Five Pty Ltd	2011	https://www.commandfive.c	Y	3	Not specified	Not attributed	China	0.385476594	
408	The “Lurid” Downloader	TrendMicro	2011	http://la.trendmicro.com/m	Y	2	Covert Grove	not atributed	Russia, Tibet, China	0.336284347	
458	SK Hack by an Advanced Persistent Threat	Command Five Pty Ltd	2011	https://www.commandfive.c	N					0.2551592942	
528	HTran and the Advanced Persistent Threat	SecureWorks	2011	https://www.secureworks.co	N					0.1523111164	
538	w64 regin stage 1	F-Secure	2011	https://www.f-secure.com/d	N		not named	not attributed		0.1430886853	
566	Night Dragon	McAfee	2011	https://securingtomorrow.m	N		night Dragon	china		0.1062569046	
584	Palebot Palestinian credentials	Norman	2011	http://msdsrnd.com/wp-cor	N					0.08864190019	
14	Energy Risk	KPMG	2012	https://assets.kpmg.com/co	N					0.9153584344	
59	The Taidoor Campaign	TrendMicro	2012	https://www.trendmicro.de/	N					0.9786815545	
142	THE VOHO CAMPAIGN : AN IN DEPTH ANALYSIS	RSA	2012	http://blogsdev.rsa.com/wp-	Y	2		Not attributed	United States	0.7494715208	
143	Systematic cyber attacks against Israeli and Palestinian targets	Norman AS	2012	http://enterprise-manage.nc	N					0.7487799155	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
227	The Luckyat Hackers	Symantec	2012	http://www.symantec.com/c	N		LuckyCat			0.6110407115	
240	IXESHE An APT Campaign	TrendMicro	2012	https://www.trendmicro.de/	N		IXESHE			0.5783583717	
255	The Sin Digoo Affair	SecureWorks	2012	https://www.secureworks.cc	N					0.554191193	
312	w32 regin stage 1	F-Secure	2012	https://www.f-secure.com/d	N					0.4604059082	
328	Targeted Attacks in Syria	F-Secure	2012	https://www.f-secure.com/v	Y	1	not named	not attributed	Syria	0.4449628826	
330	Elderwood project	Symantec	2012	http://www.symantec.com/c	Y	2	Elderwood	China	States, China, Australia	0.4435802024	
352	Command and Control in the Fifth Domain	Command Five Pty Ltd	2012	https://www.commandfive.c	N					0.4097856121	
391	It's not the end of the world: DarkComet misses by a mile	ArborNetworks	2012	https://www.arbornetworks	N					0.3589473953	
427	Crouching Tiger, Hidden Dragon, Stolen Data	Context	2012	https://www.contextis.com/	Y	2	China	China	China, Taiwan, Tibet	0.3051017991	
438	The Mirage Campaign	SecureWorks	2012	https://www.secureworks.cc	N					0.2840375523	
465	**CozyDuke**	F-Secure	2012	https://www.f-secure.com/d	N		Dukes/APT29			0.2467761848	
468	Taming the RATs	Matasano	2012	http://www.matasano.com/	Y	2	Not specified	Not attributed	Not specified	0.2421634195	
493	Recovering from Shamoon	Fidelis	2012	http://threatgeek.typepad.c	N					0.2055531679	
496	The Madi Infostealers	Kaspersky	2012	https://securelist.com/the-n	N					0.2025228535	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
527	skywiper	Crysys	2012	https://www.crysys.hu/publi	N					0.1532484462	
540	Gauss: Abnormal Distribution	Kaspersky	2012	https://securelist.com/gauss	N					0.1398683547	
546	Luckycat redux	TrendMicro	2012	http://blog.trendmicro.com/	Y	3		not attributed	Japan, India, Tibet	0.1310386899	
560	Analysis of the FinFisher Lawful Interception Malware	Rapid7	2012	https://blog.rapid7.com/201	Y	1	not named	not attributed	Bahrain, United States	0.1164106486	
582	OSX SabPub	Kaspersky	2012	https://securelist.com/new-\	N					0.08903264919	
590	Revealed: Operation Shady RAT	McAfee	2012	http://www.csri.info/wp-cor	Y	2	Shady RAT	Not attributed	United States	0.07039653031	
613	MSUpdaterTrojanWhitepaper	Zscaler	2012	https://paper.seebug.org/pa	N					0.0358413331	
620	The Heartbeat Campaign	TrendMicro	2012	http://www.trendmicro.it/m	Y	3	Heartbeat	Not attributed	Tibet, China	0.02077476459	
16	Evasive Tactics: Terminator RAT	FireEye	2013	https://www.fireeye.com/bl	Y	3	multiple	Not attributed	China	0.9186709527	
36	Operation Beebus	FireEye	2013	https://www.fireeye.com/bl	N					0.9312325479	
38	Operation DeputyDog	FireEye	2013	https://www.fireeye.com/bl	N		DeputyDog	Not attributed		0.9957912777	
40	OPERATION SAFFRON ROSE	FireEye	2013	https://www.fireeye.com/co	Y	1	Ajax Security Team	Iran	Iran	0.9847458501	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
57	The Mutter Backdoor Operation	FireEye	2013	https://www.fireeye.com/bl	N					0.909973792	
66	Trojan APT BaneChant	FireEye	2013	https://www.fireeye.com/bl	N					0.9225068459	
77	Kaspersky Lab Identifies Operation “Red October,” an Advanced	Kaspersky	2013	https://usa.kaspersky.com/a	Y	3	Red October	not attributed	China	0.8740979944	
85	APT1: technical backstage	Itrust	2013	https://malware.lu/assets/fi	Y	3	APT1	China	not specified	0.8531698034	
94	APT1 Exposing One of China’s Cyber Espionage Units	Mandiant	2013	https://www.fireeye.com/co	N		APT1	China		0.8411591791	
97	Trojan APT Seinup	FireEye	2013	https://www.fireeye.com/bl	N					0.8351994825	
107	Android Trojan found in targeted attack	Kaspersky	2013	https://securelist.com/andro	Y	1	not named	not attributed	Tibet, China	0.8169189959	
110	The Maudi Surveillance Operation	Norman Shark	2013	http://cfile8.uf.tistory.com/a	Y	1	Maudi	Not attributed	China, Mongolia	0.8116042662	
130	Stuxnet 0.5: The Missing Link	Symantec	2013	https://www.symantec.com/	N		not named	not attributed		0.776083992	
146	Comment Crew: Indicators of Compromise	Symantec	2013	https://www.symantec.com/	N		Comment Crew			0.7432133993	
154	The "Kimsuky" Operation	Kaspersky	2013	https://securelist.com/the-k	N		Kimsuky	North Korea	South Korea	0.7373696503	
162	Operation EphemeralHydra	FireEye	2013	https://www.fireeye.com/bl	N					0.7268679096	
168	"njRAT" uncovered	Fidelis	2013	http://threatgeek.typepad.c	N					0.7223410151	
198	njRAT, The Saga Continues	Fidelis	2013	https://paper.seebug.org/pa	N					0.6621439381	
211	POISON IVY: Assessing Damage and Extracting Intelligence	FireEye	2013	https://www.fireeye.com/co	Y	3		not attributed	Not specified	0.6359715011	
221	The Great Bank Robbery: the Carbanak APT	Kaspersky	2013	https://securelist.com/the-g	N					0.6193184418	
238	Operation Arachnophobia	ThreatConnect	2013	https://www.threatconnect.	N			Pakistan		0.5847033527	
254	NetTraveler Is Back: The ‘Red Star’ APT Returns With New Trick	Kasperky	2013	https://securelist.com/nettra	Y	1	Nettraveler	China	china	0.5581907485	
281	The ‘TeamSpy’ Story	Kaspersky	2013	https://kasperskycontenthub	Y	2	TeamSpy	not attributed	multiple	0.5178934365	
282	Hidden Lynx – Professional Hackers for Hire	Symantec	2013	http://www.symantec.com/	N		Hidden Lynx	China		0.5164232151	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
298	Operation Molerats	FireEye	2013	https://www.fireeye.com/bl	N		Molerat			0.4805722691	
320	Hiding in Plain Sight: The FAKEM Remote Access Trojan	TrendMicro	2013	https://www.trendmicro.de/	N		not named	not attributed		0.4500409882	
326	India Pak Tranchulas	ThreatConnect	2013	https://www.threatconnect.	N					0.446202253	
378	“Red October” Diplomatic Cyber Attacks Investigation	Kaspersky	2013	https://securelist.com/red-o	N			russia		0.3830391075	
410	Mac Spyware Found at Oslo Freedom Forum	F-Secure	2013	https://www.f-secure.com/w	Y	1	not named	not attributed	not specified	0.3309193987	
445	KeyBoy, Targeted Attacks against Vietnam and India	Rapid7	2013	https://blog.rapid7.com/201	N		KeyBoy / Tropic			0.2685790408	
459	HangOver	Norman	2013	https://paper.seebug.org/pa	N		HangOver	not attributed		0.2548615794	
463	ETSO APT Attacks Analysis	Ahnlab	2013	http://global.ahnlab.com/glo	N					0.2526437553	
471	Threat Advisory Exploit Operation Red October	McAfee	2013	https://paper.seebug.org/pa	N		Red October	not attributed		0.2356148236	
482	**Dissecting Operation Troy**	McAfee	2013	https://www.mcafee.com/ca	N			North Korea		0.2218735179	
502	miniduke indicators public	Crysys	2013	https://github.com/kbandla/	N					0.1924325767	
513	MiniDuke Paper Final	Bitdefender	2013	https://labs.bitdefender.com	N		MiniDuke, APT29	not attributed		0.1756793677	
514	Plugx Smoaler	Sophos	2013	https://sophosnews.files.wo	N					0.1742177479	
568	“Winnti” More than just a game	Kaspersky	2013	https://securelist.com/winnt	Y	3	Winnti	China	China, Tibet	0.1044101287	
573	Secrets of the Comfoo Masters	SecureWorks	2013	https://www.secureworks.co	N	3		Not attributed	not specified	0.1010786096	
579	Operation Hangover	Norman Shark	2013	http://enterprise-manage.no	N	2	Not named	India	India, Pakistan	0.0918126125	
587	Analysis Report (TLP:WHITE) Analysis of a stage 3 Miniduke sample	CIRCL	2013	https://www.circl.lu/files/tr-	N		Not identified, but linked to APT 29			0.07496486695	
610	Safe A TARGETED THREAT	TrendMicro	2013	https://www.trendmicro.de/	Y	2	Safe	not attributed	not specified	0.03936435423	
612	The 'Icefog' APT	Kaspersky	2013	https://kasperskycontenthub	N			China, South Korea, japan		0.03763575041	
615	Hikit Analysis-Final	Novetta	2013	https://www.novetta.com/w	N		not named	Not attributed		0.03134993005	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
622	**The NetTraveler (aka 'Travnet')**	Kaspersky	2013	https://kasperskycontenthub	Y	3	NetTraveler	China	China, Tibet	0.01841947468	
3	APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?	FireEye	2014	https://www.fireeye.com/co	Y	2	APT28	Russia	Not specified	0.9317531193	
9	CVE-2014-4114: Details on August BlackEnergy PowerPoint Car	ESET	2014	https://www.welivesecurity.	N			not attributed		0.984210716	
13	**Dragonfly: Western Energy Companies Under Sabotage Threa**	Symantec	2014	https://www.symantec.com/	N					0.9414052342	
27	iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in	iSight	2014	https://web.archive.org/web	N		Sandworm / BlackEnergy	Russia		0.9434848712	
32	Micro-Targeted Malvertising via Real-time Ad Bidding"	Invincea	2014	https://paper.seebug.org/pa	N					0.9198148126	
33	New Zero-Day Exploit targeting Internet Explorer Versions 9 through 11 Identified in Targeted Attacks	FireEye	2014	https://www.fireeye.com/bl	N					0.9699062229	
37	Operation CloudyOmega Ichitaro	Symantec	2014	https://www.symantec.com/	N		CloudyOmega	not attributed		0.909088479	
41	OrcaRAT	PwC	2014	http://pwc.blogs.com/cyber	N					0.958823088	
47	Sayad Flying Kitten analysis	Vinsula	2014	http://vinsula.com/2014/07/	N					0.8883381893	
52	Syrian Malware	Kaspersky	2014	https://securelist.com/files/	Y	1	Resistant Syrian Electronic Army	Not attributed	Syria	0.9351150374	
56	The little malware that could	FireEye	2014	https://www.fireeye.com/co	N					0.9139999766	
58	THE REGIN PLATFORM	Kaspersky	2014	https://securelist.com/files/	N		Not named	nation state'		0.9956571728	
60	The Uroburos case	Gdata	2014	https://www.gdatasoftware.	N					0.920096566	
86	**I am Ironman: DEEP PANDA Uses Sakula Malware to Target Organizations in Multiple Sectors**	CrowdStrike	2014	https://www.crowdstrike.co	N		DeepPanda	China		0.8522037971	
89	regin-analysis	Symantec	2014	https://www.symantec.com/	N			nation-state		0.8459190222	
92	RAT in a Jar	Fidelis	2014	https://www.fidelissecurity.c	N					0.8429901365	
106	World War C	FIreEye	2014	https://www.fireeye.com/co	Y	2	Not applicable	Not applicable	China	0.817650445	
116	Connecting the Dots: Syrian Malware Team Uses BlackWorm for	FireEye	2014	https://www.fireeye.com/bl	N		Syrian Malware Team	Syria		0.7988614428	
135	Mo' Shells Mo' Problems - Deep Panda Web Shells	CrowdStrike	2014	https://www.crowdstrike.co	N		DeepPanda	China		0.7701208871	
136	Operation Poisoned Hurricane	FireEye	2014	https://www.fireeye.com/bl	N		Poisoned Hurricane	Not attributed		0.7651602119	
138	Gathering in the Middle East, Operation STTEAM	Fidelis	2014	https://paper.seebug.org/pa	N		STTEAM	not attributed		0.7585911064	
139	Cybersecurity's Maginot Line	FireEye	2014	https://www2.fireeye.com/r	N					0.7563165171	
140	BE2 custom plugins, router abuse, and target profiles	Kaspersky	2014	https://securelist.com/be2-c	N		Sandworm / BlackEnergy / TeleBots / Quedagh			0.7556193926	
144	XtremeRAT: Nuisance or Threat?	FireEye	2014	https://www.fireeye.com/bl	N					0.7473435539	
151	Miniduke twitter	ESET	2014	https://www.welivesecurity.	N		APT29			0.7409094865	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
153	The Eye of the Tiger	Airbus	2014	http://blog.cassidiancyberse	N		Pitty Tiger			0.7393782239	
158	Threat Intelligence Brief 2014-07 Illuminating the Etumbot APT Backdoor	ASERT	2014	https://asert.arbornetworks	N		APT12	China		0.7344352215	
166	Gholee - a “protective edge” themed spear phishing campaign	ClearSky	2014	http://www.clearskysec.com	N					0.7244919866	
189	The Monju Incident	Context	2014	https://www.contextis.com/	N					0.678174862	
194	LeoUncia and OrcaRat	Airbus	2014	http://blog.airbuscybersecu	N		not named	not attributed		0.672409133	
209	Democracy in Hong Kong Under Attack	Volexity	2014	https://www.volexity.com/b	Y	1	Not specified	Not attributed	China	0.6393969547	
212	Sednit espionage group now using custom exploit kit	ESET	2014	https://www.welivesecurity.	N		APT28 / Sofacy	russia		0.6344240687	
220	HACKING THE STREET? FIN4 LIKELY PLAYING THE MARKET	FireEye	2014	https://www.fireeye.com/co	N		FIN4	not attributed		0.6202708652	
229	Bots, Machines, and the Matrix	Fidelis	2014	https://www.fidelissecurity.c	N					0.6085269842	
236	korea power plant wiper	?	2014	https://paper.seebug.org/pa	N					0.5898128128	
237	Threat Spotlight: Group 72	Cisco	2014	https://blogs.cisco.com/secu	N		Group 72			0.5878454591	
249	Operation Quantum Entanglement	FireEye	2014	https://www.fireeye.com/co	N		Moafee, DragonOK	China		0.56499289	
250	Reimagining security	FIreEye	2014	https://www.avantec.ch/ass	N		n/a	n/a		0.5645906283	
263	**NetTraveler APT Gets a Makeover for 10th Birthday**	Kaspersky	2014	https://securelist.com/nettra	Y	1	NetTraveler	China	China, Tibet	0.5436922424	
270	Turla 2 Penquin	Kaspersky	2014	https://securelist.com/the-p	N					0.5337577382	
272	Recent Watering Hole Attacks Attributed to APT Group “th3bug	PaloAlto Networks	2014	https://researchcenter.paloa	N					0.5299598614	
277	SUPPLY CHAIN ANALYSIS: From Quartermaster to SunshopFireEye	FIreEye	2014	https://www.fireeye.com/co	N		Sunshop	China		0.5256258451	
289	Snake In The Grass: Python-based Malware Used For Targeted A	BlueCoat	2014	https://www.bluecoat.com/	N			Pakistan		0.5028085626	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
291	Operation Snowman	FireEye	2014	https://www.fireeye.com/bl	Y	3	DeputyDog	Not attributed	Not specified	0.4986172645	
295	Intruder File Report- Sneakernet Trojan	Fidelis	2014	https://paper.seebug.org/pa	N					0.4908343339	
299	APT28: Sofacy? So Funny.	PwC	2014	https://pwc.blogs.com/cybe	N		APT28	Not attributed		0.4798743118	
304	**Uroburos - highly complex espionage software with Russian r**	G Data	2014	https://public.gdatasoftware	N					0.4687687557	
305	**BlackEnergy Quedagh**	F-Secure	2014	https://www.f-secure.com/d	N		Quedagh / BlackEnergy /	Russia		0.4686672461	
311	Operation Poisoned Handover	FireEye	2014	https://www.fireeye.com/bl	Y	1	Poisoned Handover	China	China	0.4629714857	
327	Operation Pawn Storm Using Decoys to Evade Detection	TrendMicro	2014	https://www.trendmicro.de/	Y	2	APT28	not attributed	Russia	0.446184205	
336	TR-25 Analysis - Turla / Pfinet / Snake/ Uroburos	CIRCL	2014	http://www.circl.lu/pub/tr-2	N		Turla			0.4297574387	
340	TrapX ZOMBIE Report Final	TrapX	2014	https://trapx.com/trapx-labs	N					0.4256519651	
353	Aided Frame, Aided Direction	FireEye	2014	https://www.fireeye.com/bl	Y	1	Sunshop	China	China	0.4083273383	
355	THE CASE OF THE MODIFIED BINARIES	Leviathan	2014	http://www.leviathansecurit	N					0.4073399093	
361	OperationCleaver The Notepad Files	Cylance	2014	https://threatvector.cylance.	N		Cleaver	Not attributed		0.4032812368	
362	The Black Vine cyberespionage group	Symantec	2014	http://www.symantec.com/	N		BlackVine			0.3995147442	
366	**OPERATION "KE3CHANG": Targeted Attacks Against Ministries of Foreign Affairs**	FireEye	2014	https://www.fireeye.com/co	N		Ke3chang	China		0.3954556038	
372	**The Snake Campaign**	BAE Systems	2014	http://www.baesystems.com	N		Turla / snake / uroburos			0.3861310276	
373	Operation Pawn Storm: The Red in SEDNIT	TrendMicro	2014	https://blog.trendmicro.com	Y	3	APT28	not attributed		0.3855725325	
376	**COSMICDUKE** **Cosmu with a twist of MiniDuke**	F-Secure	2014	https://www.f-secure.com/d	N		Dukes/APT29			0.3844985978	
377	Scan Box Framework	PWC	2014	http://pwc.blogs.com/cyber	N	3		Not attributed	United States	0.3837478316	
381	Korplug Afghanistan Tajikistan	ESET	2014	https://www.welivesecurity.	N					0.3800605538	
384	**"El Machete"**	Kaspersky	2014	https://securelist.com/el-ma	N					0.3732594836	
388	Unveiling "Careto" - The Masked APT	Kaspersky	2014	https://kasperskycontenthub	Y	3	Careto	Not attributed	not specified	0.3658614663	
395	OperationDoubleTap	FireEye	2014	www.fireeye.com/blog/threa	N					0.3575757196	
397	Energetic Bear – Crouching Yeti	Kaspersky	2014	https://securelist.com/energ	N					0.352975613	
402	Shell Crew	RSA	2014	https://www.emc.com/colla	N		DeepPanda	not attributed		0.3499171268	
404	OnionDuke Tor	F-Secure	2014	https://www.f-secure.com/w	N		OnionDuke	not attributed		0.3454080934	
405	New CDTO: A Sneakernet Trojan Solution	Fidelis	2014	https://paper.seebug.org/pa	N					0.342879565	
415	The Darkhotel APT A Story of Unusual Hospitality	Kaspersky	2014	https://securelist.com/files/	Y	2	DarkHotel	Not attributed	a, Russia, South Korea	0.3163246884	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
417	Cat Scratch Fever: CrowdStrike Tracks Newly Reported Iranian A	CrowdStrike	2014	https://www.crowdstrike.co	Y	3	FlyingKitten/Saffron Rose	Iran	Iran	0.3152326152	
421	The Siesta Campaign	TrendMicro	2014	http://blog.trendmicro.com/	N					0.3096211605	
424	PAN Nitro	PaloAlto Networks	2014	https://unit42.paloaltonetw	N		Nitro	not attributed		0.306105384	
433	Cloud Atlas: RedOctober APT is back in style	Kaspersky	2014	https://securelist.com/cloud	N		CloudAtlas/RedOctober			0.2973475961	
464	Darwin's Favorite APT Group	FireEye	2014	https://www.fireeye.com/bl	N			China		0.247425271	
466	Operation Poisoned Helmand	ThreatConnect	2014	https://threatconnect.com/b	N		Not named	China		0.2434320167	
472	Sandworm to Blacken	TrendMicro	2014	https://blog.trendmicro.com	N		BlackEnergy / Sandworm			0.235112306	
474	CrowdStrike Global Threat Intel Report	CrowdStrike	2014	https://www.crowdstrike.co	Y	2	Flying Kitten	Iran	Iran, multiple	0.2340794221	
483	Darkhotel Indicators of Compromise	Kaspersky	2014	https://securelist.com/files/2	N		DarkHotel			0.22113613	
485	Threat Spotlight: Group 72, Opening the ZxShell	Cisco	2014	https://blogs.cisco.com/secu	N					0.2157845258	
490	Profiling an enigma: The mystery of North Korea's cyber threat landscape	HP Security	2014	https://community.hpe.com	N	3	Kimsukyang	North Korea	South Korea	0.2102732547	
510	Forced to Adapt: XSLCmd Backdoor Now on OS X	FireEye	2014	https://www.fireeye.com/bl	Y	3	not named	not attributed	Tibet, China	0.1773100456	
516	Derusbi (Server Variant) Analysis	Novetta	2014	http://www.novetta.com/wp	N					0.1724092659	
520	The Rotten Tomato Campaign	Sophos	2014	https://www.sophos.com/en	N			china		0.1682333161	
545	Back in BlackEnergy *: 2014 Targeted Attacks in Ukraine and Po	ESET	2014	https://www.welivesecurity.	N		BlackEnergy	Not attributed		0.1316502706	
549	Putter Panda	CrowdStrike	2014	https://cdn0.vox-cdn.com/as	N			China		0.1301957431	
555	Roaming Tiger	ESET	2014	http://2014.zeronights.org/a	N		Roaming Tiger	Not attributed		0.1226733302	
562	Wiper Malware	Talos	2014	https://blogs.cisco.com/secu	N					0.1152713101	
564	Sofacy Phishing	PwC	2014	https://pwc.blogs.com/files/	N		APT28/Sofacy	Russia		0.113752425	
592	Analysis of MITM on Google	Netresec	2014	https://www.netresec.com/?	N					0.06573062895	
596	Operation GreedyWonk	FireEye	2014	https://www.fireeye.com/bl	Y	1	GreedyWonk	not attributed	Egypt, USA	0.06130232926	
597	**Inception Report**	BlueCoat	2014	http://dc.bluecoat.com/Ince	N		Inception	Not attributed		0.06018251119	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
602	The French Connection	CrowdStrike	2014	https://www.crowdstrike.co	N		AuroraPanda + X			0.05194011911	
605	Targeted Attacks Against the Energy Sector	Symantec	2014	http://www.symantec.com/	N					0.04256644375	
611	The Epic Turla Operation	Kaspersky	2014	https://securelist.com/the-e	N		Turla / Uroburos			0.03781999042	
621	Operation "TooHash": how targeted attacks work	G Data	2014	https://secure.gd/dl-en-tool	N					0.01986104132	
4	Behind the Syrian Conflict's Digital Front Lines	FireEye	2015	https://www.fireeye.com/co	Y	1	not named	Lebanon	Syria	0.9007811491	
7	China Hacks the Peace Palace: All Your EEZ's Are Belong to Us	ThreatConnect	2015	https://www.threatconnect.	N		Not named	China		0.9742148014	
11	Dissecting Linux/Moose	ESET	2015	https://www.welivesecurity.	N					0.9950652223	
24	Inception APT Analysis Bluecoat	BlueCoat	2015	https://www.bluecoat.com/	N					0.9826690236	
29	Latest Flash Exploit Used in Pawn Storm Circumvents Mitigatio	TrendMicro	2015	https://blog.trendmicro.com	N		APT28	not attributed		0.9745489664	
45	RSA Incident Response: An APT Case Study	RSA	2015	https://autoblog.postblue.in	N					0.9923990927	
51	SOUTHEAST ASIA: AN EVOLVING CYBER THREAT LANDSCAPE	FireEye	2015	https://www.fireeye.com/co	N					0.8922843061	
54	THE DESERT FALCONS TARGETED ATTACKS	Kaspersky	2015	https://securelist.com/files/	Y	2	Desert Falcons	Not attributed	alestine, Jordan, Israel	0.9129644237	
63	Tracking MiniDionis	PaloAlto Networks	2015	https://unit42.paloaltonetw	N		APT29	Not attributed		0.8986838354	
75	CVE-2015-2545: overview of current threats	Kaspersky	2015	https://securelist.com/cve-2	N					0.8796209908	
76	Peering-Into-GlassRAT-final(Nov-23-15)	RSA	2015		N					0.876103335	
79	Tactical Intelligence Bulletin: Scanbox II	PwC	2015	http://pwc.blogs.com/files/c	Y	3	Several actors using same malware	Not attributed	Jnited States, Vietnam	0.8702997224	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
81	Iran-based-attackers-use-back-door-threats-to-spy-on-Middle-E	Symantec	2015	https://www.symantec.com/	Y	2	Cadelle, Chafer	Iran	multiple	0.8645569856	
90	Project Cobra Analysis	Gdata	2015	https://www.gdatasoftware.	N					0.8443395114	
99	Dissecting the Malware Involved in the INOCNATION Campaign	Fidelis	2015	https://www.fidelissecurity.c	N					0.8252792494	
101	The Naikon APT Tracking Down Geo-Political Intelligence Across APAC, One Nation at a Time	Kaspersky	2015	https://securelist.com/the-n	N					0.8246827511	
104	**APT30**	FireEye	2015	https://www2.fireeye.com/r	Y	2	APT30	China	multiple	0.8212986358	
105	ThreatGroup-3390	SecureWorks	2015	https://www.secureworks.co	N					0.8180900706	
114	Operation Tropic Trooper	TrendMicro	2015	http://blog.trendmicro.com/	N		Keyboy / Tropic Trooper	Not attributed		0.8022724137	
118	ZoxPNG Full Analysis-Final	Novetta	2015	http://www.novetta.com/wp	N					0.7943080783	
119	Skeleton Key Analysis	SecureWorks	2015		N					0.7934626313	
128	**Equation Group: questions and answers**	Kaspersky	2015	https://securelist.com/files/2	N			Not attributed		0.7768925249	
160	Hacktivist Group CyberBerkut Behind Attacks on German Offici	TrendMicro	2015	https://blog.trendmicro.com	N		CyberBerkut	not attributed		0.7318394664	
171	The MiniDuke Mystery: PDF 0-day Government Spy Assembler	Kaspersky	2015	https://securelist.com/the-n	N	3		Not attributed	United States	0.7131732053	
175	Dissecting the “Kraken”	G Data	2015	https://www.gdatasoftware.	N					0.7097435706	
178	Kaspersky Security Bulletin 2015. Evolution of cyber threats in t	Kaspersky	2015	https://securelist.com/kaspe	N		N/A			0.7068169076	
181	Duke APT group's latest tools: cloud services and Linux support - FSecure Weblog	F-Secure	2015	https://labsblog.f-secure.cor	N					0.6939390392	
182	STRONTIUM: A profile of a persistent and motivated adversary	rosoft Security Intelligence	2015	http://download.microsoft.c	Y	3	APT28	Russia	multiple	0.6910832327	
187	Carbanak gang is back and packing new guns	ESET	2015	https://www.welivesecurity.	N		Carbanak			0.6834927129	
199	New Headaches: How The Pawn Storm Zero-Day Evaded Java’s	TrendMicro	2015	https://blog.trendmicro.com	N		APT28	not attributed		0.6598520507	
200	New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targ	TrendMicro	2015	https://blog.trendmicro.com	N		APT28	not attributed		0.6575582324	
215	Panda Security Uncovers Ongoing Attack Against Oil Tankers	Panda	2015	https://www.pandasecurity.	N		Phantom Menace	rivate individual		0.6310733725	
216	**APT28 targets financial markets**	Root9b	2015	https://www.root9b.com/sit	N		APT28 / Sofacy			0.6294070718	
224	Operation-Potao-Express final v2	ESET	2015	https://www.welivesecurity.	N					0.6158083321	
225	**Duqu 2.0:**	CrySyS	2015	http://www.crysys.hu/duqu2	N					0.6154955419	
230	Operation Potao Express: Analysis of a cyber-espionage toolkit	ESET	2015	https://www.welivesecurity.	N			Not attributed		0.607292489	
244	Pawn Storm’s Domestic Spying Campaign Revealed; Ukraine an	TrendMicro	2015	https://blog.trendmicro.com	Y	1	APT28	Russia	Russia	0.5723847329	
258	**The Dukes**	F-Secure	2015	https://www.f-secure.com/d	N		The Dukes / APT29	Russia	United States	0.5524919343	
268	**"Forkmeiamfamous": Seaduke, latest weapon in**	symantec	2015	https://www.symantec.com/	N		The Dukes / APT29			0.5389105539	
287	PlugX goes to the registry	Sophos	2015	https://www.sophos.com/er	N					0.503537003	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
293	winnti pharmaceutical	Kaspersky	2015	https://securelist.com/game	N					0.4961536055	
302	ROCKET KITTEN: A CAMPAIGN WITH 9 LIVES	Check Point	2015	https://blog.checkpoint.com	N			Iran	ers in Iran, plus others	0.4748789083	
313	Operation WOOLEN-GOLDFISH	TrendMicro	2015	www.trendmicro.de%2Fmed	N					0.4603852659	
314	The MnsMM campaigns	Kaspersky	2015	https://securelist.com/files/:	N					0.4598690635	
318	Sofacy APT hits high profile targets with updated toolset	Kaspersky	2015	https://securelist.com/sofac	N		APT28	Russia		0.4546111933	
324	TERRACOTTA VPN	RSA	2015		N					0.448500924	
329	Thamar Reservoir	ClearSky	2015	http://www.clearskysec.com	Y	3	Thamar Reservoir	Iran	multiple	0.4438546229	
331	Inside EquationDrug Espionage Platform	Kaspersky	2015	https://securelist.com/inside	N		Equation Group	Not attributed		0.4423532058	
333	PWC ELISE-Security-Through-Obesity(Dec-23-15)	PwC	2015		N					0.4364613391	
339	https://www.symantec.com/connect/blogs/duqu-20-reemerge	Symantec	2015	https://www.symantec.com/	N			Not attributed		0.4262374279	
344	Vinself steganography	Airbus	2015	http://blog.airbuscybersecu	N		not named	not attributed		0.4223832595	
349	APT28 MacOS	BitDefender	2015	https://download.bitdefend	N		APT28			0.4140361966	
351	BBSRAT-Attacks-Targeting-Russian-Organizations-Linked-to-Roa	PaloAlto Networks	2015	https://researchcenter.paloa	N					0.4099754479	
357	PlugX Threat Activity in Myanmar	ArborNetworks	2015	http://pages.arbornetworks.	N					0.4045797198	
370	The Chronicles of the Hellsing APT: the Empire Strikes Back - Securelist	Kaspersky	2015	https://securelist.com/the-c	N					0.3881855171	
379	Sofacy II	PwC	2015	http://pwc.blogs.com/files/c	N		APT28/Sofacy			0.3824411703	
394	Butterfly: Corporate spies out for financial gain	symantec	2015	https://www.symantec.com/	N		Butterfly	non-state actor		0.357589285	
398	Operation Arid Viper	TrendMicro	2015	https://www.trendmicro.cor	N					0.3524711195	
399	The Mystery of Duqu 2.0	Kaspersky	2015	https://securelist.com/the-m	N					0.3519640592	
403	OperationClandestineWolf	FireEye	2015	https://www.fireeye.com/bl	N					0.3454651499	
430	Cylance SPEAR Team: A Threat Actor Resurfaces	Cylance	2015	https://www.cylance.com/cc	N		Not mentined by name, but sounds	China		0.2995458645	
436	WateringHole Aerospace CVE-2015-5122 IsSpace	PaloAlto Networks	2015	https://researchcenter.paloa	N					0.285758539	
437	HackerGroup-Creates-Network-Fake-LinkedIn-Profiles(10-07-20	SecureWorks	2015	https://www.secureworks.cc	N					0.2854989041	
451	An In-Depth Look at How Pawn Storm's Java Zero-Day Was Use	TrendMicro	2015	https://blog.trendmicro.com	N		APT28	not attributed		0.2644682838	
452	Pawn Storm Targets MH17 Investigation Team	TrendMicro	2015	https://blog.trendmicro.com	Y	2	APT28	not attributed	not specified	0.2622373676	
462	Pawn Storm Update: Trend Micro Discovers New Java Zero-Day	TrendMicro	2015	https://blog.trendmicro.com	N		APT28	not attributed		0.2530333269	
475	The Anthem Hack: All Roads Lead to China	ThreatConnect	2015	https://threatconnect.com/b	N		Unknown	China		0.2338491371	
488	HAMMERTOSS	FireEye	2015	https://www2.fireeye.com/r	N		APT29	Russia		0.2145975494	
491	Grabit and the RATs	Kaspersky	2015	https://securelist.com/grabit	N					0.2095260355	
494	UnFIN4ished Business pwd	PwC	2015	http://pwc.blogs.com/cyber	N					0.2049975326	
497	An analysis of Regin's Hopscotch and Legspin	Kaspersky	2015	https://securelist.com/an-an	N					0.2021883954	
498	unit42-operation-lotus-blossom	PaloAlto Networks	2015	https://www.paloaltonetwo	N					0.2020908259	
500	Attacks against Israeli & Palestinian interests	PwC	2015	http://pwc.blogs.com/cyber	N			Not attributed		0.194356626	
501	Wild Neutron – Economic espionage threat actor returns with	Kaspersky	2015	https://securelist.com/wild-i	N					0.1943145957	
515	Scarab Russian	Symantec	2015	https://www.symantec.com/	N					0.1740778363	
524	MiniDionis CozyCar Seaduke	PaloAlto Networks	2015	https://researchcenter.paloa	N					0.1611116511	
525	volatile-cedar-technical-report	Check Point	2015	https://www.checkpoint.cor	N					0.1560686407	
534	Dino – the latest spying malware from an allegedly French espionage group analyzed	ESET	2015	https://www.welivesecurity.	N		Animal Farm	France		0.1457168492	
543	Operation Pawn Storm Ramps Up its Activities; Targets NATO, V	TrendMicro	2015	https://blog.trendmicro.com	Y	3	APT28	not attributed	Russia, Ukraine	0.1365439872	
544	Angler and Nuclear Exploit Kits Integrate Pawn Storm Flash Exp	TrendMicro	2015	https://blog.trendmicro.com	N		APT28	not attributed		0.13380818	
556	Operation Armageddon	Looking Glass	2015	https://www.lookingglasscyb	N			Russia		0.1225294185	
577	Operation Russian Doll	FireEye	2015	https://www.fireeye.com/bl	N		APT28	Russia		0.09738626304	
606	The CozyDuke APT	Kaspersky	2015	https://securelist.com/the-c	N		APT29	not attributed		0.04245568709	
608	ASERT Threat Intelligence Report 2015-08 Uncovering the Seven Pointed Dagger	ASERT	2015	https://asert.arbornetworks	Y	2	Group 27/Seven Pointed Dagger	Not attributed	Myanmar	0.04075721837	
618	Cmstar Downloader: Lurid and Enfal's New Cousin	PaloAlto networks	2015	https://researchcenter.paloa	N					0.0247776374	
625	Pawn Storm Update: iOS Espionage App Found	TrendMicro	2015	http://blog.trendmicro.com/	N		APT28			0.01078579024	
1	'DealersChoice' is Sofacy's Flash Player Exploit Platform	PaloAlto Networks	2016	https://unit42.paloaltonetw	N		APT28 / Sofacy	Russia		0.9851269609	
5	Can a BEAR Fit Down a Rabbit Hole?	ThreatConnect	2016	https://threatconnect.com/b	N		not named	Not attributed		0.8922009662	
12	Does a BEAR Leak in the Woods?	ThreatConnect	2016	https://threatconnect.com/b	N		APT28	Russia		0.9292593993	
39	Operation Dust Storm	Cylance	2016	https://www.cylance.com/cc	N		Might have been APT1 (activity	Not attributed		0.8922480311	
44	Tropic Trooper Targets Taiwanese Government and Fossil Fuel F	PaloAlto Networks	2016	https://unit42.paloaltonetw	N		KeyBoy / Tropic	not attributed		0.3375435564	
53	T9000-Advanced-Modular-Backdoor-Uses-Complex-Anti-Analys	PaloAlto Networks	2016	https://researchcenter.paloa	N			Not attributed		0.9793465616	
55	The Dukes R&D finds a new Anti-Analysis technique	PaloAlto Networks	2016	https://unit42.paloaltonetw	N		APT29	Not attributed		0.9878100969	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
61	The-ProjectSauron-APT research KL(08-08-2016)	Kaspersky	2016	https://securelist.com/files/	N					0.9699632761	
71	ropic Trooper Targets Taiwanese Government and Fossil Fuel Pr	PaloAlto Networks	2016	https://unit42.paloaltonetw	N					0.9717021112	
78	PowerDuke: Widespread Post-Election Spear Phishing Campaig	Volexity	2016	https://www.volexity.com/b	Y	1	APT29	Russia	United States	0.8722475238	
80	Operation Dusty Sky	ClearSky	2016	http://www.clearskysec.com	Y	3	Molerat	not attributed	mirates, United States.	0.8662004309	
93	MONSOON –	Forecepoint	2016	https://blogs.forcepoint.com	N		Same one as			0.8428097305	
96	IXESHE Derivative IHEATE Targets Users in America	TrendMicro	2016	https://blog.trendmicro.com	N		IXESHE			0.8355010164	
141	BITTER: A Targeted Attack Against Pakistan	Forecepoint	2016	https://blogs.forcepoint.com	N					0.7556012068	
145	Patchwork cyberespionage group expands tar	Symantec	2016	https://www.symantec.com/	Y	2	Patchwork	not attributed	apan, United Kingdom	0.7440012288	
148	What's in a Name Server?	ThreatConnect	2016	https://threatconnect.com/b	N		APT28	Russia		0.7429909721	
149	DroppingElephant(07-08-2016)	Kaspersky	2016		N		Patchwork /	not attributed		0.7416646341	
155	Poseidon Group: a Targeted Attack Boutique specializing in glob	Kaspersky	2016	https://securelist.com/posei	N			Not attributed		0.7371883951	
157	Targeted Attacks against Banks in the Middle East	FireEye	2016	https://www.fireeye.com/bl	N					0.7351756581	
167	Turbo Twist: Two 64-bit	Fidelis	2016	https://www.fidelissecurity.c	N		Sunshop	China		0.7236461347	
169	New wave of cyberattacks against Ukrainian power industry	ESET	2016	https://www.welivesecurity.	N		not specified	not attributed		0.7162637936	
174	Pawn Storm Campaign Adds Turkey To Its List of Targets	TrendMicro	2016	https://blog.trendmicro.com	N		APT28	not attributed		0.710057828	
183	Follow the Money	FireEye	2016	https://www.fireeye.com/so	N		FIN6			0.689958766	
185	APT Group Sends Spear Phishing Emails to Indian Government	FireEye	2016	https://www.fireeye.com/bl	N					0.6893148977	
188	Rebooting Watergate: Tapping into the Democratic National Co	ThreatConnect	2016	https://threatconnect.com/b	N		Apt28, APT29	Russia		0.6804343816	
192	FROM SEOUL TO SONY: THE HISTORY OF THE DARKSEOUL GROU	BlueCoat	2016	https://github.com/kbandla/	N		DarkSeoul	North Korea		0.6744784366	
193	**ThreatGroup-4127-Targets-Clinton-Campaign**	SecureWorks	2016	https://www.secureworks.co	Y	2	TG-4127 / APT28	Russia	United States	0.6726531924	
196	PrinceofPersiaGameOver(06-28-2016)	PaloAlto Networks	2016		N					0.6661220114	
205	Hunting Libyan Scorpions	Cyberkov	2016	https://cyberkov.com/huntin	N		Libyan Scorpions	Libya		0.6472544195	
206	**Redline Drawn**	FireEye	2016	https://www.fireeye.com/co	Y	3	Not applicable	China	China	0.6429594611	
207	Buckeye cyberespionage group shifts gaze from US to Hong Kong	Symantec	2016	https://www.symantec.com/	N		Buckeye	Not attributed		0.6420940334	
208	Visiting The Bear Den	ESET	2016	https://www.welivesecurity.	N		APT28			0.6408958604	
235	En Route with Sednit Part III	ESET	2016	https://www.welivesecurity.	N		APT28/Sednit			0.5911535578	
251	Belling the BEAR	ThreatConnect	2016	https://www.threatconnect.	Y	1	APT28, CyberBerkut	Russia	Ukraine	0.5607816481	
252	Espionage toolkit targeting Central and Eastern Europe uncover	ESET	2016	https://www.welivesecurity.	N					0.5600795709	
259	BlackEnergy by the SSHBearDoor	ESET	2016	https://www.welivesecurity.	N					0.5515556487	
264	Guccifer 2.0: The Man, the Myth, the Legend?	ThreatConnect	2016	https://threatconnect.com/b	N		not named	Russia		0.5430880235	
265	The rise of TeleBots	ESET	2016	https://www.welivesecurity.	N		TeleBots /			0.5428953367	
266	Emissary-Trojan-Changelog-Did-Operation-Lotus-Blossom-Caus	PaloAlto Networks	2016		N					0.5407862258	
269	Buckeye HongKong(09-06-2016)	Symantec	2016		N					0.5343051552	
275	Microsoft DUBNIUM(06-09-2016)	Microsoft	2016		N					0.5274759969	
278	USE OF FANCY BEAR	CrowdStrike	2016	https://www.crowdstrike.co	N		APT28	Russia		0.524510205	
285	BlackEnergy-APT-Attacks-in-Ukraine-employ-spearphishing-with	Kaspersky	2016		N		BlackEnergy /			0.5066534968	
294	**Findings from Analysis of DNC Intrusion Malware**	Fidelis	2016	https://www.fidelissecurity.c	N					0.4959472902	
296	ke3chang tidepool(5-23-2016)	PaloAlto Networks	2016		N					0.4869953419	
315	Suckfly-Revealing-the secret-life-of-your-code-signing-certificat	Symantec	2016		N					0.4584874724	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
316	The Waterbug attack group	Symantec	2016	https://www.symantec.com/	N		Turla / snake / uroburos			0.4572611066	
317	Houdini's Magic Reappearance	PaloAlto Networks	2016	https://unit42.paloaltonetw	N		not named	not attributed		0.4563439256	
321	New Carbanak / Anunak Attack Methodology	TrustWave	2016	https://www.trustwave.com	N					0.449926936	
322	ScarCruft-OpDaybreak(06-17-2016)	Kaspersky	2016		N					0.4490608182	
325	A Look Into Fysbis: Sofacy's Linux Backdoor	PaloAlto Networks	2016	https://unit42.paloaltonetw	N		APT28 / Sofacy	Russia		0.446812624	
334	Operation Dusty Sky - Part 2	ClearSky	2016	http://www.clearskysec.com	N		Molerat			0.4325923621	
337	PwC Exploring CVE-2015-2545(05-06-2016)	PwC	2016		N					0.4288402688	
341	BlackEnergy trojan strikes again: Attacks Ukrainian electric pow	ESET	2016	https://www.welivesecurity.	Y	3	BlackEnergy	not attributed	Ukraine	0.4250720615	
342	MALWARE ACTORS USING NIC CYBER SECURITY THEMED SPEAF	Cysinfo	2016	https://cysinfo.com/malware	N			Pakistan		0.4240907763	
346	Strider: Cyberespionage group turns eye of Sauron on targets	Symantec	2016	https://www.symantec.com/	N		Strider	nation-state		0.4192944195	
347	Targeted-attacks-in-South-and-Southeast-Asia(Apr-26-16)	Microsoft	2016		N					0.4176955571	
360	**Operation Blockbuster**	Novetta	2016	https://www.operationblock	N		Lazarus	North Korea		0.4033199881	
363	En Route with Sednit Part I	ESET	2016	https://www.welivesecurity.	Y	2	APT28/Sednit	Russia	ıultiple Eastern Europe	0.3981066328	
367	Taiwan Presidential Election	PWC	2016	http://pwc.blogs.com/cyber_	Y	3		China	China	0.3952359759	
368	Guccifer 2.0: All Roads Lead to Russia	ThreatConnect	2016	https://threatconnect.com/b	N		not named	Russia		0.3911829374	
383	Mofang	Fox IT	2016	https://blog.fox-it.com/2016	N		Mofang			0.3750837661	
386	RESEARCH SPOTLIGHT: NEEDLES IN A HAYSTACK	Cisco	2016	https://blogs.cisco.com/secu	N					0.3677818461	
392	StrongPity-Waterhole-Targeting-Italian-Belgian-Encryption-Use	Kaspersky	2016		N					0.3586336931	
400	Operation-C-Major blog(5-18-16)	TrendMicro	2016		N					0.351838281	
413	Scarlet Mimic	PaloAlto Networks	2016	https://researchcenter.paloa	Y	1	Scarlet Mimic	China	China, Tibet	0.3197602905	
414	Shiny Object? Guccifer 2.0 and the DNC Breach	ThreatConnect	2016	https://threatconnect.com/b	N		APT28	Russia		0.3183213292	
416	Let It Ride: The Sofacy Group's DealersChoice Attacks Continue	PaloAlto Networks	2016	https://unit42.paloaltonetw	N		APT28			0.3155346977	
418	**IRONGATE ICS Malware: Nothing to See Here...Masking Malic**	FireEye	2016	https://www.fireeye.com/bl	N					0.3134065373	
420	Pawn Storm Targets German Christian Democratic Union	TrendMicro	2016	https://blog.trendmicro.com	N		APT28	not attributed		0.3099334676	
428	Attack-on-French-Diplomat-Linked-to-Operation-Lotus-Blossom	PaloAlto Networks	2016		N					0.3039217375	
431	when the lights went out	Booz Allen	2016	https://www.boozallen.com/	N		not specified	ıussian interests		0.299259073	
432	Operation Groundbait:	ESET	2016	https://www.welivesecurity.	Y	1	Groundbait	not attributed	Ukraine	0.2991240625	
442	New- Wekby-Attacks-Use- DNS-Requests- As- Command-and- C	PaloAlto Networks	2016	https://researchcenter.paloa	N			Not attributed		0.2731320724	
448	Russian Cyber Operations on Steroids	ThreatConnect	2016	https://threatconnect.com/b	N		APT28	Russia		0.267503653	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
453	PrinceofPersiaInfyMalware(05-02-2016)	PaloAlto Networks	2016		N					0.2604048348	
461	New Sofacy Attacks Against US Government Agency	PaloAlto Networks	2016	https://unit42.paloaltonetw	N		APT28	Russia		0.2531490655	
467	Indian organizations targeted in Suckfly attacks	Symantec	2016	https://www.symantec.com/	N		Suckfly			0.2431793136	
473	NetherlandsCyberAttack(04-21-2016)	TrendMicro	2016		N					0.2341663437	
486	Pawn Storm Ramps Up Spear-phishing Before Zero-Days Get Pa	TrendMicro	2016	https://blog.trendmicro.com	N		APT28	not attributed		0.2154815893	
487	BLACKGEAR Espionage Campaign Evolves, Adds Japan To Target	TrendMicro	2016	https://blog.trendmicro.com	N					0.2152080914	
499	SWIFT attackers' malware linked to more finar	Symantec	2016	https://www.symantec.com/	N		Lazarus	North Korea		0.1986068897	
503	Tracking Elirks Variants in Japan	PaloAlto Networks	2016	https://researchcenter.paloa	N					0.1903886791	
506	**Bears in the Midst: Intrusion into the Democratic National Co**	CrowdStrike	2016	https://www.crowdstrike.co	N		APT29, APT28	Russia		0.1866477249	
517	FANCY BEAR Has an (IT) Itch that They Can't Scratch	ThreatConnect	2016	https://threatconnect.com/b	N		APT28	Russia		0.1719036229	
533	operation-transparent-tribe-threat-insight-en(Mar-01-16)	Proofpoint	2016		N					0.1459131456	
535	En Route with Sednit Part II	ESET	2016	https://www.welivesecurity.	N		APT28/Sednit			0.1442404084	
541	PROMETHIUM and NEODYMIUM	rosoft Security Intelligence	2016	https://blogs.technet.micros	N					0.1390036281	
542	Moonligt - Targeted Attacks in the Middle East	Vectra	2016	https://blog.vectra.ai/blog/r	N					0.1384009275	
553	Pacifier APT	BitDefender	2016		N			N		0.1254005889	
559	UNVEILING PATCHWORK – THE COPY-PASTE APT	Cymmetria	2016	https://s3-us-west-2.amazor	N		Patchwork	not attributed		0.1164816054	
575	The Ghost Dragon	Cylance	2016	https://blog.cylance.com/th	N					0.0981458673	
578	RE-DUBNIUM-FlashExploit(06-20-2016)	Microsoft	2016		N					0.09523521591	
583	KillDisk and BlackEnergy Are Not Just Energy Sector Threats	TrendMicro	2016	https://blog.trendmicro.com	N		BlackEnergy / Sandworm	Russia		0.08874093943	
593	**THE PROJECT SAURON APT**	Kaspersky	2016	https://securelist.com/files/	N		ProjectSauron	Not attributed		0.064848332	
603	NetTraveler APT Targets Russian, European Interests	ProofPoint	2016	https://www.proofpoint.com	Y	3	NetTraveler	China	ssia, Mongolia, Belarus	0.04999636025	
619	Molerats there is more to the naked eye	PWC	2016	https://pwc.blogs.com/cybe	N					0.0243257772	
624	Threat Group-4127 Targets Google Accounts	SecureWorks	2016	https://www.secureworks.co	Y	2	APT28	Russia	Russia, United States	0.01087838654	
627	Sofacy's 'Komplex' OS X Trojan	PaloAlto Networks	2016	https://unit42.paloaltonetw	N		APT28	Russia		0.00426421622	
629	Taiwan targeted with new cyberespionage back door Trojan	Symantec	2016	https://www.symantec.com/	N		Budminer	Not attributed		0.00259129446	
17	Evolution of the GOLD EVERGREEN threat group	SecureWorks	2017	https://www.secureworks.co	N			Individuals		0.943607075	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
18	FIN10: Anatomy of a Cyber Extortion Operation	FireEye	2017	https://www.fireeye.com/bl	N					0.9422953856	
19	Fin7 Spear Phishing Campaign	FireEye	2017	https://www.fireeye.com/bl	N		Fin7			0.9860478741	
20	From BlackEnergy to ExPetr	Kaspersky	2017	https://securelist.com/from-	N		N/A	N/A		0.9667375512	
21	Gaza Cybergang – updated activity in 2017:	Kaspersky	2017	https://securelist.com/gaza-	Y	3	Gaza Cybergang	not attributed	not specified	0.969357844	
26	Investigation Report for the September 2014 Equation malware	Kaspersky	2017	https://securelist.com/inves	N					0.9584819168	
28	Kiev metro hit with a new variant of the infamous Diskcoder ra	ESET	2017	https://www.welivesecurity.	N					0.985324964	
34	No Free Pass for ExPetr	Kaspersky	2017	https://securelist.com/no-fr	N		not named	not attributed		0.9351578644	
35	OilRig Deploys “ALMA Communicator”	PaloAlto Networks	2017	https://researchcenter.paloa	N		OilRig			0.9472423383	
42	PaloAlto The-Blockbuster-Sequel(04-07-2017)	PaloAlto Networks	2017	https://unit42.paloaltonetw	N					0.948210209	
43	Petya ransomware outbreak: Here’s what you need to know	Symantec	2017	https://www.symantec.com/	N					0.8927935374	
46	Russian Bank offices hit with broad phishing wave	RSA	2017	https://community.rsa.com/	N					0.8939311843	
48	ShadowPad in corporate networks	Kaspersky	2017	https://securelist.com/shad	N		ShadowPad	not attributed		0.9766061471	
50	Software Supply Chain Attacks on the Rise, Undermining Custo	CrowdStrike	2017	https://www.crowdstrike.co	N					0.01787015583	
62	Threat Spotlight: Follow the Bad Rabbit	Cisco Talos	2017	https://blog.talosintelligence	N		TeleBots			0.9845949731	
64	Tracking Subaat: Targeted Phishing Attack Leads to Threat Acto	PaloAlto Networks	2017	https://researchcenter.paloa	N					0.9618747714	
65	Triton: New Malware Threatens Industrial Safety Systems	Symantec	2017	https://www.symantec.com/	N					0.9777951748	
69	Two Years of Pawn Storm	TrendMicro	2017	https://documents.trendmic	Y	3	APT28	Russia	Russia	0.9447008367	
70	Untangling the Patchwork Cyberespionage Group	TrendMicro	2017	https://blog.trendmicro.com	N		Patchwork	Not attributed		0.9277753917	
82	Operation Wilted Tulip – Exposing a Cyber Espionage Apparatu	ClearSky	2017	https://www.clearskysec.cor	N		Copy Kitten			0.8587098786	
83	Cyberattacks against Ukrainian ICS	Sentryo	2017	https://www.sentryo.net/wp	N					0.8566657172	
84	New FinFisher surveillance campaigns: Internet providers invol	ESET	2017	https://www.welivesecurity.	N		N/A	N/A		0.8538734715	
87	Evidence Aurora still active	Intezer	2017	https://www.intezer.com/ev	N		APT17			0.8505041097	
88	MM CORE IN-MEMORY BACKDOOR RETURNS AS "BIGBOSS" AN	Forecepoint	2017	https://blogs.forcepoint.com	N					0.8478683969	
95	ChessMaster's new strategy	TrendMicro	2017	https://blog.trendmicro.com	N		ChessMaster			0.8409132957	
100	An end to smash and grab	CrowdStrike	2017	https://www.crowdstrike.co	Y	2	Not applicable	China	not specified	0.8252685739	
102	KINGSLAYER - A SUPPLY CHAIN ATTACK	RSA	2017	https://www.rsa.com/en-us/	N		Kingslayer	not attributed		0.8244889075	
109	Introducing White Bear	Kaspersky	2017	https://securelist.com/intro	N		White Bear			0.8124073792	
111	Operation Cloud Hopper	PWC	2017	https://www.pwc.co.uk/issu	N		Cloud Hopper /APT10	China		0.8064865473	
112	APT Trends report Q3 2017	Kaspersky	2017	https://securelist.com/apt-tr	N					0.8064533253	
113	OSX/Proton spreading again through supply-chain attack	ESET	2017	https://www.welivesecurity.	N		not named	not attributed		0.8057321721	
115	APT29 Domain Fronting With TOR	FireEye	2017	https://www.fireeye.com/bl	N		APT29			0.7993540672	
121	CRASHOVERRIDE	Dragos	2017	https://dragos.com/blog/cra	N		Sandworm / BlackEnergy / TeleBots / Quedagh	not attributed		0.7918085024	
123	REDBALDKNIGHT/BRONZE BUTLER’s Daserf Backdoor Now Usir	TrendMicro	2017	https://blog.trendmicro.com	N		BRONZE BUTLER	not attributed		0.7899899565	
131	ChessMaster Makes its Move: A Look into the Campaign’s Cybe	TrendMicro	2017	https://blog.trendmicro.com	N		ChessMaster	Not attributed		0.7753314305	
132	Ocean Lotus Blossoms	Volexity	2017	https://www.volexity.com/b	Y	1	OceanLotus / APT32	Vietnam	Vietnam	0.7739384892	
134	APT Trends report Q2 2017	Kaspersky	2017	https://securelist.com/apt-tr	N					0.7721375245	
137	KopiLuwak: A New JavaScript Payload from Turla	Kaspersky	2017	https://securelist.com/kopilu	N		Turla / Uroburos	Russia-based		0.7632278576	
147	Chessmaster makes its move	TrendMicro	2017	https://blog.trendmicro.com	N					0.7430831513	
150	TeleBots are back: Supply-chain attacks against Ukraine	ESET	2017	https://www.welivesecurity.	N		TeleBots / BlackEnergy / Industroyer	not attributed		0.7414725786	
156	Threat Actors Target Government of Belarus Using CMSTAR Tro	PaloAlto Networks	2017	https://researchcenter.paloa	N					0.7357809438	
163	HawkEye Credential Theft Malware Distributed in Recent Phish	FireEye	2017	https://www.fireeye.com/bl	N					0.7265354033	
165	Inexmar	BitDefender	2017	https://labs.bitdefender.com	N					0.7247707918	
170	“Cyber Conflict” Decoy Document Used In Real Cyber Conflic	Cisco	2017	https://blogs.cisco.com/secu	N		APT28	Russia		0.7136167578	
172	BadRabbit: a closer look at the new version of Petya/NotPetya	Malwarebytes	2017	https://blog.malwarebytes.c	N		not named	not attributed		0.7111578611	
186	Bad Rabbit Highlights Employees’ Role in Cyber Security Attack	Nozomi Networks	2017	https://www.nozominetwork	N		not named	not attributed		0.686450278	
191	THE CARBANAK/FIN7 SYNDICATE	RSA	2017	https://www.rsa.com/en-us/	N		CARBANAK / FIN7			0.6766381442	
201	**Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford**	ClearSky	2017	http://www.clearskysec.com	N		OilRig	Iran		0.6569818946	
217	Insights into Iranian Cyber Espionage: APT33 Targets Aerospace	FireEye	2017	https://www.fireeye.com/bl	N					0.6287142697	
219	XData ransomware making rounds amid global WannaCryptor s	ESET	2017	https://www.welivesecurity.	N					0.6213134974	
222	crowdstrike protects against notpetya	CrowdStrike	2017	https://www.crowdstrike.co	N					0.6189468882	
228	DownAndExec: Banking malware utilizes CDNs in Brazil	ESET	2017	https://www.welivesecurity.	N		not named	not attributed		0.6088058499	
232	Behind the CARBANAK Backdoor	FireEye	2017	https://www.fireeye.com/bl	N					0.6022329704	
233	TRISIS	Dragos	2017	https://dragos.com/blog/tris	N					0.5972931884	
234	WCry Ransomware Analysis	SecureWorks	2017	https://www.secureworks.co	N			Not attributed		0.5935354671	
243	Lookout ViperRAT-IDF(02-16-2017)	Lookout	2017	https://blog.lookout.com/vi	N					0.5740817276	
247	Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3	Recorded Future	2017	https://www.recordedfuture	N			China		0.5694310041	
256	Privileges and Credentials: Phished at the Request of Counsel	FireEye	2017	https://www.fireeye.com/bl	N					0.5541247676	
260	MagicHound-Campaign-Attacks-SaudiTargets(02-15-2017)	PaloAlto Networks	2017		N					0.5515374186	
276	In ExPetr/Petya’s shadow, FakeCry ransomware wave hits Ukrai	Kaspersky	2017	https://securelist.com/in-ex	N		not named	not attributed		0.5272112294	
279	Recent Surge in Spam Emails Carries Repackaged Adwind RAT t	Symantec	2017	https://www.symantec.com/	N					0.523134056	
284	Cyber Espionage is Alive and Well: APT32 and the Threat to Glo	FIreEye	2017	https://www.fireeye.com/bl	Y	3	APT32	Vietnam	multiple	0.5111552893	
286	Sednit update: How Fancy Bear Spent the Year	ESET	2017	https://www.welivesecurity.	N		APT28 / Sednit	not attributed		0.5064528714	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
288	DragonOK-Updates-Tools-Targets-Multiple-Regions(01-05-2017	PaloAlto Networks	2017		N					0.5028097724	
297	Threat Group APT28 Slips Office Malware into Doc Citing NYC T	McAfee	2017	https://securingtomorrow.m	N		APT28			0.48669232	
303	Industrial Control System Threats	Dragos	2017	https://www.dragos.com/m	N					0.4723702118	
307	**LAZARUS UNDER THE HOOD**	Kaspersky	2017	https://securelist.com/files/	N		Lazarus, Bluenoroff	North Korea		0.4653300558	
309	New WannaCryptor-like ransomware attack hits globally: All yo	ESET	2017	https://www.welivesecurity.	N					0.4642401451	
310	Of Pigs and Malware: Examining a Possible Member of the Win	TrendMicro	2017	https://blog.trendmicro.com	N		Winnti	not attributed		0.4631935313	
338	The Curious Case of Mia Ash: Fake Persona Lures Middle Easter	SecureWorks	2017	https://www.secureworks.c	N			Iran		0.4287333625	
343	SIDEWINDER TARGETED ATTACK AGAINST ANDROID IN THE GOLDEN AGE OF AD LIBRARIES	FireEye	2017	https://www.fireeye.com/co	N					0.4236569796	
345	Gazing at Gazer	ESET	2017	https://www.welivesecurity.	N		Turla			0.4212579036	
348	*IRON TWILIGHT Supports 'Active Measures'*	SecureWorks	2017	https://www.secureworks.c	Y	2	APT28	Russia	gdom, Russia, multiple	0.4176054073	
354	**Operation BugDrop**	CyberX	2017	https://cyberx-labs.com/en/	N					0.4080708024	
364	Ransomware Recap: The Short-Lived Spread of Bad Rabbit Rans	TrendMicro	2017	https://www.trendmicro.cor	N		not named	not attributed		0.3964105979	
365	**WIn32/Industoyer**	ESET	2017	https://www.welivesecurity.	N		unnamed APT	Not attributed		0.3963886299	
369	Dimnie-Hiding-Plain-Sight(03-28-2017)	PaloAlto Networks	2017		N					0.3896972427	
371	Iranian PupyRAT Bites Middle Eastern Organizations	SecureWorks	2017	https://www.secureworks.c	N		COBALT GYPSY	Iran		0.3877737399	
375	Unraveling the Lamberts Toolkit	Kaspersky	2017	https://securelist.com/unrav	N		Longhorn / Lamberts	not attributed		0.3853072001	
382	APT28: At the Center of the Storm	FireEye	2017	https://www.fireeye.com/bl	Y	3	APT28	Russia	Russia	0.3757743042	
390	Industroyer: Biggest threat to industrial control systems since S	ESET	2017	https://www.welivesecurity.	N					0.3596994453	
409	**The Deception Project: A new Japanese-centric threat**	Cylance	2017	https://www.cylance.com/e	N		SnakeWine	China		0.333574036	
412	Operation Electric Powder – Who is targeting Israel Electric Company?	ClearSky	2017	http://www.clearskysec.com	N					0.3258884798	
426	Taiwan Heist: Lazarus Tools and Ransomware	BAE Systems	2017	https://www.baesystems.co	N					0.3056241377	
429	StrongPity2 spyware replaces FinFisher in MitM campaign – ISF	ESET	2017	https://www.welivesecurity.	N		N/A	N/A		0.3035341855	
434	Spear Phishing Techniques Used in Attacks Targeting the Mong	FIreEye	2017	https://www.fireeye.com/bl	N					0.2936458165	
435	http://www.intezer.com/evidence-aurora-operation-still-active	Intezer	2017	http://www.intezer.com/evi	N		APT17			0.2874653641	
441	Pawn Storm Abuses Open Authentication in Advanced Social E	TrendMicro	2017	https://blog.trendmicro.com	N		APT28	Russia		0.2742108799	
444	New Targeted Attack in the Middle East by APT34	FireEye	2017	https://www.fireeye.com/bl	N					0.2688836275	
449	CVE-2017-0199 Used as Zero Day to Distribute FINSPY Espionag	FireEye	2017	https://www.fireeye.com/bl	N					0.2673713724	
450	Significant FormBook Distribution Campaigns Impacting the U.S	FireEye	2017	https://www.fireeye.com/bl	N					0.2654031341	
455	Petya Destructive Malware Variant Spreading via Stolen Creder	FireEye	2017	https://www.fireeye.com/bl	N					0.2576929947	
456	BACKSWING - Pulling a BADRABBIT Out of a Hat	FireEye	2017	https://www.fireeye.com/bl	N					0.2569072988	
460	WannaCry ransomware used in widespread attacks all over the	Kaspersky	2017	https://securelist.com/wann	N		not named	not attributed		0.2536553105	
469	Attackers Deploy New ICS Attack Framework "TRITON"	FireEye	2017	https://www.fireeye.com/bl	N					0.2396088149	
479	From Cybercrime to Cyberpropaganda	TrendMicro	2017	https://blog.trendmicro.com	N		not specified	not attributed		0.2240368844	
481	Report Shamoon StoneDrill final(03-06-2017)	Kaspersky	2017		N					0.2229916898	
484	Longhorn: Tools used by cyberespionage group linked to Vault 7	Symantec	2017	https://www.symantec.com/	N			Not attributed		0.2206898043	
489	Spring Dragon – Updated Activity	Kaspersky	2017	https://securelist.com/spring	N		Spring Dragon/ Lotus Blossom	not attributed		0.2138803683	
495	North Korea bitten by bitcoin bug	Proofpoint	2017	https://www.proofpoint.com	N		Lazarus			0.2031414342	
511	The shadows of Ghosts	RSA	2017	https://community.rsa.com/	N					0.1771532527	
512	North Korean Actors Spear Phish U.S. Electric Companies	FireEye	2017	https://www.fireeye.com/bl	N					0.1769926454	
518	CYBER ATTACK IMPERSONATING IDENTITY OF INDIAN THINK TA	Cysinfo	2017	https://cysinfo.com/cyber-at	N			Pakistan		0.1704991582	
519	ATMitch: remote administration of ATMs	Kaspersky	2017	https://securelist.com/atmit	N		not named	not attributed		0.1694542233	
522	Down the Rabbit Hole	RiskIQ	2017	https://www.riskiq.com/blog	N		TeleBots			0.1617797714	
531	Breaking-Weakest-Link-IDF(02-16-2017)	Kaspersky	2017		N					0.1474960952	
551	The Keyboys are back in town	PWC	2017	https://www.pwc.co.uk/issu	N		KeyBoy / Tropic Trooper			0.1275222903	
552	BRONZE BUTLER Targets Japanese Enterprises	SecureWorks	2017	https://www.secureworks.c	N		Bronze Butler	China		0.1266131608	
557	The Gamaredon Group Toolset Evolution	PaloAlto Networks	2017	https://researchcenter.paloa	N		Gamaredon	Russia (implied)		0.1191912331	
561	Carbon Paper: Peering into Turla's second stage backdoor	ESET	2017	https://www.welivesecurity.	N		Turla / Uroburos	not attributed		0.1155406026	
563	FireEye Uncovers CVE-2017-8759	FireEye	2017	https://www.fireeye.com/bl	N					0.115101712	
565	Obfuscation in the Wild: Targeted Attackers Lead the Way in Ev	FireEye	2017	https://www.fireeye.com/bl	N					0.1095254876	
567	Dragonfly: Western energy sector targeted by sophisticated attack group	Symantec	2017	https://www.symantec.com/	N		DRAGONFLY			0.1048633871	
570	BlackOasis APT and new targeted attacks leveraging zero-day e	Kaspersky	2017	https://securelist.com/black	Y	2	BlackOasis	not attributed	not specified	0.1020464854	
571	URI TERROR ATTACK & KASHMIR PROTEST THEMED SPEAR PHIS	Cysinfo	2017	https://cysinfo.com/uri-terro	N					0.1016967528	
572	Iranian Threat Agent Greenbug Impersonates Israeli High-Tech	ClearSky	2017	https://www.clearskysec.cor	N					0.1015086681	
576	Falcon Intelligence Report: Wanna Ransomware Spreads Rapidl	CrowdStrike	2017	https://www.crowdstrike.co	N					0.09785683205	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
580	Charming Kitten	ClearSky	2017	https://www.clearskysec.cor	y	1	Charming Kitten	Iran	irates, Denmark, India	0.09157084346	
586	WannaCryptor wasn’t the first to use EternalBlue	ESET	2017	https://www.welivesecurity.	N					0.07704477312	
589	BRONZE UNION Cyberespionage Persists Despite Disclosures	SecureWorks	2017	https://www.secureworks.co	N		Bronze Union	China		0.07318880446	
594	WannaCry and Lazarus Group – the missing link?	Kaspersky	2017	https://securelist.com/wann	N		N/A	N/A		0.06437112722	
595	Bad Rabbit: Not-Petya is back with improved ransomware	ESET	2017	https://www.welivesecurity.	N		not named	not attributed		0.06255209478	
599	IBM Full-Shamoon(02-15-2017)	IBM	2017		N					0.05805281521	
600	CYBER ATTACK TARGETING INDIAN NAVY’S SUBMARINE AND W	Cysinfo	2017	https://cysinfo.com/cyber-at	N			Pakistan		0.05753383235	
604	Bad Rabbit ransomware	Kaspersky	2017	https://securelist.com/bad-r	N		not named	not attributed		0.04724952242	
607	APT28 Targets Hospitality Sector, Presents Threat to Travelers	FireEye	2017	https://www.fireeye.com/bl	N					0.041263252	
616	Wire Wire: A West African Cyber Threat	SecureWorks	2017	https://www.secureworks.co	N					0.0287070659	
617	AES-NI aka SOREBRECT Ransomware	ThreatVector	2017	https://threatvector.cylance.	N		not named	not attributed		0.02569473217	
623	Protecting the Software Supply Chain: Deep Insights into the C	CrowdStrike	2017	https://www.crowdstrike.co	N					0.0156478288	
626	Following the Trail of BlackTech’s Cyber Espionage Campaigns	TrendMicro	2017	https://blog.trendmicro.com	N		BlackTech	not attributed		0.00518770459	
628	Threat actors leverage EternalBlue exploit to deliver non-Wann	FireEye	2017	https://www.fireeye.com/bl	N					0.00326861692	
2	Analysis of CVE-2018-8174 VBScript 0day and APT actor relatec	Qihoo360	2018	https://blog.360totalsecurity	N		APT C-06 / Darkhotel			0.9496506989	
7	Chinese Espionage Group TEMP.Periscope Targets Cambodia	FireEye	2018	https://www.fireeye.com/bl	Y	2	Temp.Periscope	China	Cambodia	0.971996108	
8	Confucius Update: New Tools and Techniques, Further Connect	TrendMicro	2018	https://blog.trendmicro.com	N		Confucius	Not attributed		0.8904404944	
10	DarkVishnya: Banks attacked through direct connection to loca	Kaspersky	2018	https://securelist.com/darkv	N					0.9458855732	
15	ESET’s guide makes it possible to peek into FinFisher	ESET	2018	https://www.welivesecurity.	N		N/A	N/A		0.9204255595	
22	Hacking Group Spies on Android Users in India Using PoriewSpy	TrendMicro	2018	https://blog.trendmicro.com	N		not specified	not attributed		0.9988470323	
25	Inception Framework: Alive and Well, and Hiding Behind Proxie	Symantec	2018	https://www.symantec.com/	N					0.9392785732	
30	LoJax: First UEFI rootkit found in the wild, courtesy of the Sedn	ESET	2018	https://www.welivesecurity.	N		APT28 / Sednit	not attributed		0.9609055533	
31	Meet CrowdStrike’s Adversary of the Month for November: HE	CrowdStrike	2018	https://www.crowdstrike.co	N		HENDRIX KITTEN			0.8230654393	
49	Skygofree: Following in the footsteps of HackingTeam	Kaspersky	2018	https://securelist.com/skygo	N					0.8875415919	
68	Two Birds, One STONE PANDA	CrowdStrike	2018	https://www.crowdstrike.co	N		STONE PANDA			0.9834197914	
72	Software Supply Chain Attacks Gained Traction in 2017 and Are	CrowdStrike	2018	https://www.crowdstrike.co	N					0.9690569193	
73	Meet CrowdStrike’s Adversary of the Month for September: CC	CrowdStrike	2018	https://www.crowdstrike.co	N		COBALT SPIDER			0.9633455812	
74	Lazarus KillDisks Central American casino	ESET	2018	https://www.welivesecurity.	N		Lazarus	not attributed		0.8817812786	
98	A Totally Tubular Treatise on TRITON and TriStation	FireEye	2018	https://www.fireeye.com/bl	N					0.8308905641	
103	Leafminer: New Espionage Campaigns Targeting Middle Easter	Symantec	2018	https://www.symantec.com/	N		Leafminer			0.8225381254	
108	Energetic Bear/Crouching Yeti: attacks on servers	Kaspersky	2018	https://securelist.com/energ	N		Energetic Bear / Crouching Yeti	Russia		0.8160140601	
117	Meet CrowdStrike’s Adversary of the Month for July: WICKED S	CrowdStrike	2018	https://www.crowdstrike.co	N		WICKED SPIDER			0.7969192332	
120	Meet CrowdStrike’s Adversary of the Month for January: VOOD	CrowdStrike	2018	https://www.crowdstrike.co	N		VOODOO BEAR			0.7922332813	
122	New Andariel Reconnaissance Tactics Hint At Next Targets	TrendMicro	2018	https://blog.trendmicro.com	Y	2	Andariel / Lazarus	Not attributed	South Korea	0.7903363963	
124	Masha and these Bears	Kaspersky	2018	https://securelist.com/mash	N		APT28	Russia		0.7828415686	
125	Sofacy Attacks Multiple Government Entities	PaloAlto Networks	2018	https://unit42.paloaltonetw	N		APT28	Not attributed		0.7813496836	
126	Update on Pawn Storm: New Targets and Politically Motivated	TrendMicro	2018	https://blog.trendmicro.com	N		APT28			0.7801441862	
127	New traces of Hacking Team in the wild	ESET	2018	https://www.welivesecurity.	N		N/A	N/A		0.7796899237	
129	APT Trends report Q1 2018	Kaspersky	2018	https://securelist.com/apt-tr	N		N/A	N/A		0.7763166894	
133	The devil’s in the Rich header	Kaspersky	2018	https://securelist.com/the-d	N		Olympic Destroyer	not attributed		0.7731406956	
152	Gallmaker: New Attack Group Eschews Malware to Live off the	Symantec	2018	https://www.symantec.com/	N		Gallmaker			0.7395954301	
159	Shedding Skin – Turla’s Fresh Faces	Kaspersky	2018	https://securelist.com/shedc	N		Turla			0.7318847722	
161	Not So Cozy: An Uncomfortable Examination of a Suspected AP	FireEye	2018	https://www.fireeye.com/bl	N		APT29	Russia		0.7289314667	
164	ChessMaster Adds Updated Tools to Its Arsenal	TrendMicro	2018	https://blog.trendmicro.com	N		ChessMaster	not attributed		0.7251544364	
173	SamSam Ransomware Campaigns	SecureWorks	2018	https://www.secureworks.co	N		GOLD LOWELL			0.7108255695	
176	The Rotexy mobile Trojan – banker and ransomware	Kaspersky	2018	https://securelist.com/the-r	N					0.7095036969	
177	New Telegram-abusing Android RAT discovered in the wild	ESET	2018	https://www.welivesecurity.	N		not named	not attributed		0.7075632568	
179	The Urpage Connection to Bahamut, Confucius and Patchwork	TrendMicro	2018	https://blog.trendmicro.com	N		Urpage	Not attributed		0.7045997854	
180	Supply-chain attack on cryptocurrency exchange gate.io	ESET	2018	https://www.welivesecurity.	N		not named	not attributed		0.697111469	
190	Threats in the Netherlands	Kaspersky	2018	https://securelist.com/threa	N					0.6775670534	
197	Big Game Hunting: The Evolution of INDRIK SPIDER From Dride	CrowdStrike	2018	https://www.crowdstrike.co	N		INDRIK SPIDER			0.663361327	
202	Dark Tequila Añejo	Kaspersky	2018	https://securelist.com/dark-	N					0.6495811088	
203	Olympic destroyer is still alive	Kaspersky	2018	https://securelist.com/olymp	N					0.6489206754	
204	Meet CrowdStrike’s Adversary of the Month for April: STARDUS	CrowdStrike	2018	https://www.crowdstrike.co	N		STARDUST CHOLLIMA			0.6488158835	
213	GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Ship	SecureWorks	2018	https://www.secureworks.co	N		GOLD GALLEON	Nigeria		0.6327955457	
214	Campaign Possibly Connected to “MuddyWater” Surfaces in th	TrendMicro	2018	https://blog.trendmicro.com	N		MuddyWater	not attributed		0.6318333945	
218	MuddyWater expands operations	Kaspersky	2018	https://securelist.com/mudc	N		MuddyWater			0.6276439856	
223	Supply Chain Attack Operation Red Signature Targets South Kor	TrendMicro	2018	https://blog.trendmicro.com	N		Red Signature	Not attributed		0.6159544879	
226	Octopus-infested seas of Central Asia	Kaspersky	2018	https://securelist.com/octop	N		Octopus			0.6138234805	
231	Iranian Threat Group Updates Tactics, Techniques and Procedu	FireEye	2018	https://www.fireeye.com/bl	N					0.6056456879	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
239	APT38: Details on New North Korean Regime-Backed Threat Gr	FireEye	2018	https://www.fireeye.com/bl	N		APT38	North Korea		0.5820625306	
242	Attacks Leveraging Adobe Zero-Day (CVE-2018-4878) – Threat A	FireEye	2018	https://www.fireeye.com/bl	N					0.5768079471	
246	BackSwap malware finds innovative ways to empty bank accou	ESET	2018	https://www.welivesecurity.	N		not named	not attributed		0.5706512054	
248	Operation AppleJeus: Lazarus hits cryptocurrency exchange wit	Kaspersky	2018	https://securelist.com/opera	N		Lazarus			0.5685727569	
253	Meet CrowdStrike’s Adversary of the Month for October: DUNG	CrowdStrike	2018	https://www.crowdstrike.co	N		DUNGEON SPIDER			0.5584455305	
257	DanaBot shifts its targeting to Europe, adds new features	ESET	2018	https://www.welivesecurity.	N		DanaBot	not attributed		0.554048131	
261	InvisiMole: Surprisingly equipped spyware, undercover since 20	ESET	2018	https://www.welivesecurity.	N		not named	not attributed		0.5480635229	
262	SamSam: Targeted Ransomware Attacks Continue	Symantec	2018	https://www.symantec.com/	N		SamSam			0.5450887434	
267	Lazarus Group Targets More Cryptocurrency Exchanges	Intezer	2018	http://www.intezer.com/laza	N		Lazarus			0.5403063244	
271	APT28: New Espionage Operations Target Military and Governm	Symantec	2018	https://www.symantec.com/	N		APT28	Russia		0.531937226	
273	Meet CrowdStrike’s Adversary of the Month for May: MYTHIC L	CrowdStrike	2018	https://www.crowdstrike.co	N		MYTHIC LEOPARD			0.5292958251	
274	OlympicDestroyer is here to trick the industry	Kaspersky	2018	https://securelist.com/olymp	N		Olympic Destroyer	not attributed		0.5276153451	
280	Lazarus Campaign Targeting Cryptocurrencies Reveals Remote C	TrendMicro	2018	https://blog.trendmicro.com	N		Lazarus	not attributed		0.5211029766	
283	Farewell to Kelihos and ZOMBIE SPIDER	CrowdStrike	2018	https://www.crowdstrike.co	N					0.5133558558	
290	Cryptocurrency Mining Malware Landscape	SecureWorks	2018	https://www.secureworks.co	N					0.5017693165	
292	Iran’s Hacker Hierarchy Exposed	Recorded Future	2018	https://www.recordedfuture	N					0.4975171224	
300	Cutwail Spam Campaign Uses Steganography to Distribute URL	CrowdStrike	2018	https://www.crowdstrike.co	N		NARWHAL SPIDER			0.4796828339	
301	Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Ta	FireEye	2018	https://www.fireeye.com/bl	N					0.4767970164	
306	Emotet launches major new spam campaign	ESET	2018	https://www.welivesecurity.	N		Emotet	not attributed		0.4668688653	
308	The sample analysis of APT-C-27’s recent attack	Qihoo360	2018	https://blog.360totalsecurity	N		APT C-27			0.4652973961	
319	Who’s who in the Zoo	Kaspersky	2018	https://securelist.com/whos	N		ZooPark	not atributed		0.4514530769	
323	Another Potential MuddyWater Campaign uses Powershell-bas	TrendMicro	2018	https://blog.trendmicro.com	N		MuddyWater	Not attributed		0.4485433752	
332	On the Hunt for FIN7: Pursuing an Enigmatic and Evasive Globa	FireEye	2018	https://www.fireeye.com/bl	N		FIN7 / Carbanak			0.4392972778	
335	linkedin Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail	Symantec	2018	https://www.symantec.com/	N					0.4308146083	
350	Operation Parliament, who is doing what?	Kaspersky	2018	https://securelist.com/opera	N		Operational Parliament	not atributed		0.4122401709	
358	DarkPulsar	Kaspersky	2018	https://securelist.com/darkp	N					0.404391965	
380	New PowerShell-based Backdoor Found in Turkey, Strikingly Sin	TrendMicro	2018	https://blog.trendmicro.com	N		MuddyWater	Not attributed		0.3813609987	
385	Meet CrowdStrike’s Adversary of the Month for February: MUM	CrowdStrike	2018	https://www.crowdstrike.co	N		MUMMY SPIDER			0.370130732	
387	FASTCash: How the Lazarus Group is Emptying Millions from AT	Symantec	2018	https://www.symantec.com/	N		Lazarus			0.3670624957	
389	New TeleBots backdoor: First evidence linking Industroyer to N	ESET	2018	https://www.welivesecurity.	N		TeleBots / BlackEnergy / Industroyer / Quedagh	not attributed		0.3605096191	
393	New MacOS Backdoor Linked to OceanLotus Found	TrendMicro	2018	https://blog.trendmicro.com	Y	3	APT32 / OceanLotus	not attributed	not specified	0.358369074	
396	Chafer: Latest Attacks Reveal Heightened Ambitions	Symantec	2018	https://www.symantec.com/	N					0.3559947993	
401	Remote Control Interloper: Analyzing New Chinese htpRAT Malware Attacks Against ASEAN	RiskIQ	2018	https://cdn.riskiq.com/wp-c	N					0.351288202	
407	LuckyMouse signs malicious NDISProxy driver with certificate o	Kaspersky	2018	https://securelist.com/lucky	N		LuckyMouse	China		0.3408641484	
411	Darkhotel APT is back	Qihoo360	2018	https://blog.360totalsecurity	N		APT C-06 / Darkhotel			0.3261165722	
419	Seedworm: Group Compromises Government Agencies, Oil & G	Symantec	2018	https://www.symantec.com/	N		Seedworm	not attributed		0.313165045	
422	Lazarus Continues Heists, Mounts Attacks on Financial Organiza	TrendMicro	2018	https://blog.trendmicro.com	N		Lazarus	Not attributed		0.3070754325	
423	Sednit update: Analysis of Zebrocy	ESET	2018	https://www.welivesecurity.	N		APT28 / Sednit	not attributed		0.3065122779	
439	Burning Umbrella	TRG	2018	https://401trg.com/burning-	N					0.2770303561	
440	New Orangeworm attack group targets the healthcare sector in	Symantec	2018	https://www.symantec.com/	N					0.2750668548	
443	VPNFilter EXIF to C2 mechanism analysed	Kaspersky	2018	https://securelist.com/vpnfil	N		not named	not attributed		0.2727639771	
446	Metamorfo Campaigns Targeting Brazilian Users	FireEye	2018	https://www.fireeye.com/bl	N					0.2684630765	
447	TRITON Attribution: Russian Government-Owned Lab Most Like	FireEye	2018	https://www.fireeye.com/bl	N		TRITON	Russia		0.2677179346	

Report No.	Title	Company	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Randomizer	
454	Why North Korean Cyberwarfare is Likely to Intensify	CrowdStrike	2018	https://www.crowdstrike.co	N					0.2581405967	
470	APT10 Targeting Japanese Corporations Using Updated TTPs	FireEye	2018	https://www.fireeye.com/bl	N		APT10			0.2371560392	
476	NIGERIAN CONFRATERNITIES EMERGE AS BUSINESS EMAIL COMPROMISE THREAT	CrowdStrike	2018	https://www.crowdstrike.co	N					0.2312517309	
477	linkedin Attackers Abuse WMIC to Download Malicious Files	Symantec	2018	https://www.symantec.com/	N					0.2285048004	
478	OceanLotus ships new backdoor using old tricks	ESET	2018	https://www.welivesecurity.	N		APT 32 / Ocean Lotus	not attributed		0.2271047298	
480	Ammyy Admin compromised with malware again; World Cup u	ESET	2018	https://www.welivesecurity.	N		not named	not attributed		0.2239271751	
492	Certificates stolen from Taiwanese tech-companies misused in	ESET	2018	https://www.welivesecurity.	N		not named	not attributed		0.2082645642	
504	Meet CrowdStrike's Adversary of the Month for August: GOBLI	CrowdStrike	2018	https://www.crowdstrike.co	N		GOBLIN PANDA			0.1894110021	
505	Bring Your Own Land (BYOL) – A Novel Red Teaming Technique	FireEye	2018	https://www.fireeye.com/bl	N		N/A	N/A		0.1878861816	
507	M-Trends	FireEye	2018	https://www.fireeye.com/bl	Y	3	apt32	Vietnam	vietnam	0.1852556192	
508	Blackgear Cyberespionage Campaign Resurfaces, Abuses Social	TrendMicro	2018	https://blog.trendmicro.com	N		BlackGear / TopGear	Not attributed		0.1838698599	
509	RedAlpha: New Campaigns Discovered Targeting the Tibetan C	Recorded Future	2018	https://www.recordedfuture	Y	1	RedAlpha	China	India, China, Taiwan	0.1821988959	
523	Suspected Iranian Influence Operation Leverages Network of Ir	FireEye	2018	https://www.fireeye.com/bl	N		not named	Iran		0.161518397	
526	GreyEnergy: Updated arsenal of one of the most dangerous thr	ESET	2018	https://www.welivesecurity.	N		GreyEnergy /	not attributed		0.1555848823	
529	Fake Software Update Abuses NetSupport Remote Access Tool	FireEye	2018	https://www.fireeye.com/bl	N					0.152031109	
530	Turla Mosquito: A shift towards more generic tools	ESET	2018	https://www.welivesecurity.	N		Turla	not attributed		0.1519713041	
536	The Evolution of Emotet: From Banking Trojan to Threat Distrib	Symantec	2018	https://www.symantec.com/	N		Emotet			0.1441214648	
537	APT37	FireEye	2018	https://www.fireeye.com/bl	Y	2	APT37 / Reaper	North Korea	th Korea, North Korea	0.1438896321	
539	Malicious spear phishing campaign targets upcoming winter ol	CrowdStrike	2018	https://www.crowdstrike.co	N					0.141804724	
547	Deciphering Confucius' Cyberespionage Operations	TrendMicro	2018	https://blog.trendmicro.com	N		PatchWork /	not attributed		0.1305242523	
548	SANNY Malware Delivery Method Updated in Recently Observe	FireEye	2018	https://www.fireeye.com/bl	N					0.1305105259	
550	The Slingshot APT FAQ	Kaspersky	2018	https://securelist.com/apt-sl	N		Slingshot	not attributed		0.1292724511	
554	ICS Tactical Security Trends: Analysis of the Most Frequent Secu	FireEye	2018	https://www.fireeye.com/bl	N					0.1251772307	
558	Brief Analysis on APT Attack through Cryptocurrency Trading Sc	Qihoo360	2018	https://blog.360totalsecurity	N		APT-C-26 / Lazarus group			0.1172857942	
569	LuckyMouse hits national data center to organize country-level	Kaspersky	2018	https://securelist.com/lucky	N		Lucky Mouse / APT27	China		0.1036265926	
574	Turla: In and out of its unique Outlook backdoor	ESET	2018	https://www.welivesecurity.	N		Turla	not attributed		0.1009299356	
581	Thrip: Espionage Group Hits Satellite, Telecoms, and Defense C	Symantec	2018	https://www.symantec.com/	N					0.09026705726	
585	Arrests Put New Focus on CARBON SPIDER Adversary Group	CrowdStrike	2018	https://www.crowdstrike.co	N		CARBON SPIDER			0.0830992018	
588	QUASAR,	ESET	2018	https://www.welivesecurity.	N		not named	not attributed		0.07391500815	
591	A Slice of 2017 Sofacy Activity	Kaspersky	2018	https://securelist.com/a-slic	Y	3	APT28	not attributed	not specified	0.06774498434	
598	Meet CrowdStrike's Adversary of the Month for June: MUSTAN	CrowdStrike	2018	https://www.crowdstrike.co	N		MUSTANG PANDA			0.05866394411	
601	Glupteba is no longer part of Windigo	ESET	2018	https://www.welivesecurity.	N		not clear	not attributed		0.0537175307	
609	Tropic Trooper's New Strategy	TrendMicro	2018	https://blog.trendmicro.com	N		KeyBoy / Tropic Trooper			0.04018109752	
614	Diplomats in Eastern Europe bitten by a Turla mosquito	ESET	2018	https://www.welivesecurity.	N		Turla	not attributed		0.03457402681	

Report No.	Title	Date	Link	CSO mentioned	CSO focus	Threat actor	Attribution	CSO country	Attack vector	Spyware infrastructure
696	Tracking GhostNet	2009	https://issuu.com/citizenlab/docs/iwm-ghostnet	Y	2	Not specified	China	India, United States	Spear phishing	
635	Backdoors are Forever	2012	https://citizenlab.ca/2012/10/backdoors-are-for	Y	1	Not specified	Not attributed	Morocco, United Arab Emirates	spear phishing, comm	Morocco, United Arab Emirates
638	Campaign Targeting Syrian Activists Escalates with New Surveillance Malware	2012	https://www.eff.org/deeplinks/2012/04/campai	Y	1	pro-Syrian government hackers	not attributed	Syria	social engineering (malicious file sent via skype), malware	
642	Fake Skype Encryption Tool Targeted at Syrian Activists Promises Security, Delivers Spyware	2012	https://www.eff.org/deeplinks/2012/05/fake-sk	Y	1	not specified	not attributed	Syria	social engineering (fake security software containing malware), malware	
643	Fake YouTube Site Targets Syrian Activists With Malware	2012	https://www.eff.org/deeplinks/2012/03/fake-yo	Y	1	not specified	not attributed	Syria	social engineering, malware	
646	FROM BAHRAIN WITH LOVE	2012	https://citizenlab.ca/2012/07/from-bahrain-with	Y	1	not specified	not attributed	Bahrain	phishing	
652	Information Operations and Tibetan Rights in the Wa	2012	https://citizenlab.ca/2012/03/information-opera	y	1	Not specified	China	China, Tibet	Social engineering	
654	Iranian anti-censorship software 'Simurgh' circulated	2012	https://citizenlab.ca/2012/05/iranian-anti-censo	N		Not specified	Not attributed		not specified	
661	New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan	2012	https://www.eff.org/deeplinks/2012/07/new-bla	Y	1	Syrian pro-goverr	not attributed	Syria	social engineering, malware	
663	New Wave of Facebook Phishing Attacks Targets Syrian Activists	2012	https://www.eff.org/deeplinks/2012/04/new-wa	Y	1	not specified	not attributed	Syria	social engineering (facebook phishing), malware	
673	Pro-Syrian Government Hackers Target Activists With Fake Anti-Hacking Tool	2012	https://www.eff.org/deeplinks/2012/08/syrian-r	Y	1	not specified	not attributed	Syria	social engineering, malware	
675	RECENT OBSERVATIONS IN TIBET-RELATED INFORMAT	2012	https://citizenlab.ca/2012/07/recent-observatio	Y	1	not specified	Not attributed	Tibet, China	spear phishing	
683	Spoofing the European Parliament	2012	https://citizenlab.ca/2012/06/spoofing-the-euro	Y	1	not specified	Not attributed	Not specified	phishing	
686	Syrian Activists Targeted with BlackShades Spy Softwa	2012	https://citizenlab.ca/2012/06/syrian-activists-ta	Y	1	Not specified	Not attributed	Syria	Skype file transfer	
687	Syrian Activists Targeted With Facebook Phishing Attack	2012	https://www.eff.org/deeplinks/2012/03/pro-syr	Y	1	not specified	not attributed	Syria	social engineering (facebook phishing)	
691	The Internet is Back in Syria and So is Malware Targeting Syrian Activists	2012	https://www.eff.org/deeplinks/2012/12/iinterne	Y	1	not specified	not attributed	Syria	social engineering, malware, spyware	Syria
694	THE SMARTPHONE WHO LOVED ME	2012	https://citizenlab.ca/2012/08/the-smartphone-v	Y	1	not specified	Not attributed	Bahrain	social engineering, spy	Bahrain, Brunei, the Czech Republic, Ethiopia, Indonesia, Mongolia, Singapore, the Netherlands, Turkmenistan, and the United Arab
697	Trojan Hidden in Fake Revolutionary Documents Targets Syrian Activists	2012	https://www.eff.org/deeplinks/2012/05/trojan-h	Y	1	not specified	not attributed	Syria	social engineering (skype phishing), malware	
630	A CALL TO HARM	2013	https://citizenlab.ca/2013/06/a-call-to-harm/	Y	1	pro-government a	Not attributed	Syria	social engineering	
633	APT1's GLASSES – Watching a Human Rights Organiza	2013	https://citizenlab.ca/2013/02/apt1s-glasses-wat	Y	1	APT1	China	Tibet, China	spear phishing	
645	For their Eyes Only	2013	https://citizenlab.ca/storage/finfisher/final/forth	Y	1	Not specified	Not attributed	Vietnam, Ethiopia, Bahrain	commercial spyware	Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysi
671	PERMISSION TO SPY	2013	https://citizenlab.ca/2013/04/permission-to-spy	Y	1	Not specified	Not attributed	Not specified	spear phishing	
674	QUANTUM OF SURVEILLANCE	2013	https://citizenlab.ca/2013/12/syrian-malware-ca	Y	1	not specified	not attributed	Syria	social engineering (social media, phishing, compromised security tools)	
685	SURTR	2013	https://citizenlab.ca/2013/08/surtr-malware-fan	Y	1	not specified	not attributed	not specified	phishing	
700	You only click twice	2013	https://citizenlab.ca/2013/03/you-only-click-twi	Y	1	Not specified	Not attributed	Ethiopia, Vietnam, Bahrain	social engineering, co	Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesi
648	Hacking Team and the Targeting of Ethiopian Journali	2014	https://citizenlab.ca/2014/02/hacking-team-targ	Y	1		not attributed	Belgium, United States	social engineering (malicious file sent over skype), commercial spyware	
650	Hacking Team's US Nexus	2014	https://citizenlab.ca/2014/02/hacking-teams-us	Y	2	Not specified	Not attributed	not specified	commercial spyware	Azerbaijan, Colombia, Ethiopia, Korea, Mexico, Morocco, Poland, Thailand, Uzbekistan, and the United Arab Emirates
658	Maliciously Repackaged Psiphon Found	2014	https://citizenlab.ca/2014/03/maliciously-repacl	Y	1	not specified	Not attributed	Syria	social engineering	
659	Malware Attack Targeting Syrian ISIS Critics	2014	https://citizenlab.ca/2014/12/malware-attack-ta	Y	1	not specified	not attributed	Iraq, Syria	spear phishing	
660	Mapping Hacking Team's "Untraceable" Spyware	2014	https://citizenlab.ca/2014/02/mapping-hacking-	Y	1	not specified	Not attributed	Not specified	exploits, social engine	Azerbaijan, Colombia, Egypt, Ethiopia, Hungary, Italy, Kazakhstan, Korea, Malaysia, Mexico, Morocco, Nigeria, Oman, Panama, Poland, Saudi Arab
672	POLICE STORY	2014	https://citizenlab.ca/2014/06/backdoor-hacking	Y	1		Not attributed	Saudi Arabia, Ethiopia, Morocco, United Arab Emirates, United States	social engineering (ma	Saudi Arabia
681	Schrodinger's Cat Video and the Death of Clear-Text	2014	https://citizenlab.ca/2014/08/cat-video-and-the	Y	2	not specified	not attributed	bahrain, morocco, united arab emirates, united states	network injection	
698	Vietnamese Malware Gets Very Personal	2014	https://www.eff.org/deeplinks/2014/01/vie	Y	1	not specified	Vietnam	Vietnam, United States	malware, DDoS	
631	A difficult profession	2015	https://www.hrw.org/report/2015/07/15/difficu	Y	2	not specified	not attributed	Serbia, Republika Srpska, Kosovo	not specified	
649	Hacking Team Reloaded?	2015	https://citizenlab.ca/2015/03/hacking-team-relo	Y	1	Ethiopian Informa	Ethiopia	United States	spear phishing, comm	Ethiopia
657	LONDON CALLINGTwo-Factor Authentication Phishing	2015	https://citizenlab.ca/2015/08/iran_two_factor_p	Y	2	not specified	Iran	not specified	phishing	
662	New Spear Phishing Campaign Pretends to be EFF	2015	https://www.eff.org/deeplinks/2015/08/new-sp	Y	1	Pawn Storm / AP	Russia	not specified	spear phishing	
668	PACKRAT	2015	https://citizenlab.ca/2015/12/packrat-report/	Y	1	Packrat	not attributed	Venezuela, Argentina, Brazil, Ecuador	phishing via email and SMS	
670	PAY NO ATTENTION TO THE SERVER BEHIND THE PRO	2015	https://citizenlab.ca/2015/10/mapping-finfisher	Y	2	multiple	Bahrain	not specified	not specified, multiple	Angola,Bangladesh,Belgium,Bosnia and Herzegovina,Czech Republic,Egypt,Ethiopia, Gabon,Indonesia,Italy,Jordan,Kazakhstan, Kenya,Lebanon,Macedonia,Malaysia,Mexico, Mongolia,Morocco,Nigeria,Oman,Paraguay, Romania,Saudi Arabia,Serbia,Slovenia,Spain, Taiwan,Turkey,Turkmenistan,Venezuela, South Africa
689	Targeted Attacks against Tibetan and Hong Kong Grou	2015	https://citizenlab.ca/2015/06/targeted-attacks-a	Y	1	not specified	not attributed	not specified	phishing	
690	Targeted Malware Attacks against NGO Linked to Atta	2015	https://citizenlab.ca/2015/10/targeted-attacks-r	Y	1	not specified	Not attributed	not specified	spear phishing,	
695	Tibetan Uprising Day Malware Attacks	2015	https://citizenlab.ca/2015/03/tibetan-uprising-d	Y	1	Not specified	not attributed	not specified	phishing, spear phishing	
699	What we know about the South Korea NIS's use of Ha	2015	https://citizenlab.ca/2015/08/what-we-know-ab	N		Not specified	Not attributed		commercial spyware	south korea
636	BETWEEN HONG KONG AND BURMA	2016	https://citizenlab.ca/2016/04/between-hon	Y	1	not specified	Not attributed	China	spear phishing	
647	GROUP5	2016	https://citizenlab.ca/2016/08/group5-syria/	Y	1	Group5	not attributed	Syria	spear phishing, watering holes	
655	IT'S PARLIAMENTARY KeyBoy and the targeting of the	2016	https://citizenlab.ca/2016/11/parliament-keybo	Y	1	not specified	Not attributed	India	spear phishing	
656	KEEP CALM AND (DON'T) ENABLE MACROS	2016	https://citizenlab.ca/2016/05/stealth-falcon/	Y	1	Stealth Falcon	United Arab Emi	United Arab Emirates, United Kingdom	spear phishing, comm	United Arab Emirates
667	Operation Manul	2016	https://www.eff.org/files/2018/01/29/operation	Y	1	Appin Security Gr	Kazakhstan	Kazakhstan, multiple	phishing, commercial spyware	Kazakhstan
682	SHIFTING TACTICS - Tracking changes in years-long espionage campaign against Tibetans	2016	https://citizenlab.ca/2016/03/shifting-tactics/	Y	1	Scarlet Mimic	not attributed	not specified	phishing	
693	THE MILLION DOLLAR DISSIDENT	2016	https://citizenlab.ca/2016/08/million-dollar-diss	Y	1	not specified	Not attributed	United Arab Emirates	SMS phishing, comme	Mexico, Kenya, United Arab Emirates
637	BITTER SWEET	2017	https://citizenlab.ca/2017/02/bittersweet-nso-m	Y	1	not specified	Mexico	Mexico	spear phishing, SMS phishing, commercial spyware	
639	CHAMPING AT THE CYBERBIT	2017	https://citizenlab.ca/2017/12/champing-cyberbi	Y	1	not specified	Ethiopia	Ethiopia, Eritrea, UK, US, South Africa, Australia, India, Japan, Qatar, Yemen, Rwanda, Kenya, Uganda, Egypt, Italy, Germany, Belgium, Norway, Canada	phishing emails, commercial spyware	
640	COMMERCIAL SPYWARE	2017	https://citizenlab.ca/2017/12/legal-overview-eth	Y	1		Not attributed			
641	Ethiopia - New spate of abusive surveillance	2017	https://www.hrw.org/news/2017/12/06/ethiopi	Y	1	not specified	Ethiopia	United States	commercial spyware	
653	INSIDER INFORMATION	2017	https://citizenlab.ca/2017/07/insider-informatio	Y	1	Not specified	Not attributed	China	phishing, website compromise, malware	
664	NILE PHISH	2017	https://citizenlab.ca/2017/02/nilephish-report/	Y	1	not specified	not attributed	Egypt	phishing, SMS phishing	
676	RECKLESS EXPLOIT	2017	https://citizenlab.ca/2017/06/reckless-exploit-m	Y	1	not specified	Mexico	Mexico, United States	commercial spyware	
677	RECKLESS III	2017	https://citizenlab.ca/2017/07/mexico-disappear	Y	3	Not specified	Not attributed			
678	RECKLESS IV	2017	https://citizenlab.ca/2017/08/lawyers-murdered	Y	3	not specified	Not attributed			
679	Reckless redux	2017	https://citizenlab.ca/2017/06/more-mexican-nso	Y	3	not specified	Mexico		commercial spyware	
680	RECKLESS V	2017	https://citizenlab.ca/2017/08/nso-spyware-mex	Y	1	Not specified	Not attributed	Mexico	SMS phishing, commercial spyware	
688	Tainted Leaks	2017	https://citizenlab.ca/2017/05/tainted-leaks-disir	Y	1	not specified	Russia	Russia, United States	phishing	
632	Amnesty International Among Targets of NSO-powere	2018	https://www.amnesty.org/en/latest/research/20	Y	1		Not attributed	Saudi Arabia	WhatsApp spear phish	Zambia, Congo, Kazakhstan, Hungary, Latvia
634	Audacity in adversity	2018	https://www.hrw.org/report/2018/04/16/audacity-adversity	Y	3		Kuwait	Kuwait		
644	FAMILIAR FEELING	2018	https://citizenlab.ca/2018/08/familiar-feeling-a-	Y	1	Tropic Trooper	Not attributed	China	spear phishing	
651	HIDE AND SEEK	2018	https://citizenlab.ca/2018/09/hide-and-seek-tra	Y	1		Not attributed	Not specified		lgeria, Bahrain, Bangladesh, Brazil, Canada, Cote d'Ivoire, Egypt, France, Greece, India, Iraq, Israel, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Latvia, Lebanon, Libya, Mexico, Morocco, the Netherlands, Oman, Pakistan, Palestine, Poland, Qatar, Rwanda, Saudi Arabia, Singapore, South Africa, Switzerland, Tajikistan, Thailand, Togo, Tunisia, Turkey, the UAE, Uganda, the United Kingdom, the United States, Uzbekistan, Yemen, and Zambia
665	NSO Group Infrastructure Linked to Targeting of Amn	2018	https://citizenlab.ca/2018/07/nso-spyware-targ	Y	1	not specified	Not attributed	not specified	SMS phishing, social media phishing	
666	Operation Dark Caracal	2018	https://www.eff.org/press/releases/eff-and-look	Y	1	Dark Caracal	not attributed	not specified	trojanized apps (mobile malware)	
669	PAKISTAN: HUMAN RIGHTS UNDER SURVEILLANCE	2018	https://www.amnesty.org/download/Document	Y	1	Crimson / Project	Not attributed	Pakistan	spear phishing via email and messaging services, social engineering via social media	
684	SPYING ON A BUDGET	2018	https://citizenlab.ca/2018/01/spying-on-a-budg	Y	1	not specified	Not attributed	China	phishing emails	
692	The Kingdom came to Canada	2018	https://citizenlab.ca/2018/10/the-kingdom-cam	Y	1	Not specified	Saudi Arabia	Canada	SMS phishing	

Infosec reports		
Column	Title	Notes
E	CSO mentioned	This is a binary variable, recording whether a report mentions targeting of civil society organizations (Y) or not (N). Civil Society Organizations (CSO) are defined as independent organizations and individuals who engage in nonviolent political activity, including activists, dissidents, journalists, academics and nongovernment organizations. We exclude think thanks because these often receive government funding and carry out research to directly support policy-making by a specific government. Importantly, since the distinguishing characteristic of civil society is non-violent political engagement, journalists and academics are only counted as civil society actors if this condition applies to them. Hence, reports that make general references to "media" or "research institutes" as target sectors of an operation are not coded as mentioning civil society. Reports that highlight targeting of specific journalists, academics or academic institutes that are engaged in non-violent political engagement, such as advocacy work, are coded as civil society.
H	Type	This variable captures the type of report, distinguishing among three different types: 1 = Focused APT report, considers political context and interests, looks into targeting patterns, wider analysis of TTP (beyond purely technical details), attempts attribution; 2 = Threat survey; survey of trends in targeted threats over specific time, or survey of evolution a specific type of threat, or survey of attack trends on a specific sector; 3 = Focus on technical aspects of attack, discussing technical details and indicators while targeting or political context discussed not at all or in passing only
F	CSO focus	Tracks the focus on CSO targeting among reports that do discuss such targeting. Recorded on a spectrum of 1-3: 1 = Primary focus of the report is on CSO targeting; 2 = Secondary focus on CSO, i.e. the primary focus is on another target, but civil society targeting is discussed in some detail and with some analysis. For example, a report on a specific threat actor may focus on its targeting of government entities, but also discuss targeting of civil society groups by the same actor; 3 = CSO targeting is only mentioned in passing, without any analysis. For example, a report may include CSOs within target lists at the end of the report, but do not discuss this targeting in the report itself. Similarly, a report focusing on a specific threat actor may mention briefly that the same actor has previously targeted civil society, but without further context or analysis.

K	Threat Actor	This column is for reference only and records the name of the threat actor to which a cyber operation is attributed, as named by the company publishing the report. If the threat actor is known under other, more common names, this name should be added.
L	Attribution	Attribution is reported among a spectrum of confidence, but for simplicity we record it here as a binary value of attribution/non-attribution as well as the name of the state to which an operation is attributed. Attribution is recorded whenever the report in question attributes the activity it discusses to a specific state, regardless of the level of confidence. Attribution is also recorded for reports where the introduction of a threat actor links to previous reporting on the same actor that clearly attributes it to a state. On the other hand, reports in which attribution is merely implied based on circumstantial evidence (i.e. the objectives align with Chinese interests) are not recorded as attribution. Reports making no mention or attempt at attribution are (obviously) also coded as "not attributed".
Q	CSO country	Records the country/countries in which CSOs targeted are located. Country names are recorded in full text, e.g. 'Ethiopia'.