

Summary Report

Domain - Insurance

Category - Antivirus detection

ID	Org ID	Date	Threat Level ID	Info	Attribute Count
992	3	2014-03-30	3	OSINT - old njRAT activity	1
974	3	2018-08-05	3	OSINT - Off-the-shelf RATs Targeting Pakistan	8
971	3	2018-08-03	2	OSINT - Attacks on industrial enterprises using RMS and TeamViewer	5
940	3	2018-06-08	3	OSINT - InvisiMole: surprisingly equipped spyware, undercover since 2013	7
94	2	2015-07-14	2	OSINT An In-Depth Look at How Pawn Stormâ€™s Java Zero-Day Was Used by Trend Micro	3
91	2	2015-07-08	2	OSINT Morpho: Profiting from high-level corporate attacks by Symantec	6
906	3	2018-04-26	2	OSINT - Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide	1
9	3	2014-10-28	2	OSINT - Operation SMN (Novetta)	16
880	3	2018-03-10	2	OSINT - New traces of Hacking Team in the wild	9
860	3	2018-01-20	4	Malware collected via pastebin	2
794	3	2017-10-25	3	OSINT - BadRabbit Ransomware Compiled by ThaiCERT, a member of the Electronic Transactions Development Agency	4
75	2	2015-04-27	3	OSINT Enterprises Hit by BARTALEX Macro Malware in Recent Spam Outbreak by Trend Micro	1

697	3	2017-08-17	2	OSINT - Turla APT actor refreshes KopiLuwak JavaScript backdoor for use in G20-themed attack	1
684	3	2017-07-30	3	OSINT - CowerSnail, from the creators of SambaCry	1
683	3	2017-07-21	3	OSINT - Linux.Bew: un backdoor para el minado de Bitcoin	1
671	3	2017-07-05	3	OSINT - The MeDoc Connection	6
670	3	2017-07-05	3	OSINT - Analysis of TeleBots™ cunning backdoor	1
652	3	2017-06-12	3	OSINT - MacRansom: Offered as Ransomware as a Service	1
651	3	2017-06-12	3	OSINT - Dvmap: the first Android malware with code injection	1
613	3	2017-04-28	3	OSINT - OSX Malware is Catching Up, and it wants to Read Your HTTPS Traffic	1
612	3	2017-04-28	3	OSINT - Alert (TA17-117A) Intrusions Affecting Multiple Victims Across Multiple Sectors	1
576	3	2017-03-13	3	OSINT - New Linux Malware Exploits CGI Vulnerability	1
56	2	2015-02-19	1	OSINT Backdoor.Win32.Equationdrug.A report by Telus	13
558	3	2017-02-13	3	OSINT - Fileless attacks against enterprise networks	4
55	2	2015-03-04	3	OSINT Who's Really Spreading through the Bright Star? by Securelist / Kaspersky	4
535	3	2017-01-25	3	OSINT - Detecting threat actors in recent German industrial attacks with Windows Defender ATP	1
529	3	2017-01-18	3	OSINT - New Mac backdoor using antiquated code	1
506	3	2016-12-13	2	OSINT - Windows 10: protection, detection, and response against recent Depriz malware attacks	4
483	3	2016-11-11	3	OSINT - The first cryptor to exploit Telegram	2
48	2	2015-02-15	4	OSINT Arid Viper: Gaza vs Israel Cyber Conflict by Trend Micro	10

472	3	2016-10-25	2	OSINT - Lifting the lid on Sednit: A closer look at the software it uses	35
469	3	2016-10-22	3	OSINT - The new .LNK between spam and Locky infection	1
465	3	2016-10-14	3	ELF Linux/NyaDrop	1
462	3	2016-10-12	2	OSINT - Odinaff: New Trojan used in high level financial attacks	1
42	2	2015-01-20	1	OSINT Analysis of Project Cobra Another extensible framework used by the Uroburos™ actors from Gdata	2
407	3	2016-08-30	3	OSINT - German Speakers Targeted by SPAM Leading to Ozone RAT	1
363	3	2016-08-08	3	OSINT - Strider: Cyberespionage group turns eye of Sauron on targets	1
360	3	2016-07-28	3	OSINT - The Mad Max DGA	1
358	3	2016-07-26	2	OSINT - Patchwork cyberespionage group expands targets from governments to wide range of industries	1
357	3	2016-07-23	3	OSINT - Kovter becomes almost file-less, creates a new file type, and gets some new certificates	1
34	2	2014-12-12	3	OSINT Fidelis Threat Advisory #1014 "Bots, Machines, and the Matrix"	19
283	3	2016-05-18	2	OSINT - Operation Groundbait: Espionage in Ukrainian war zones	13
280	3	2016-05-12	3	OSINT - Chinese-language Ransomware Makes An Appearance	1
27	2	2014-11-13	3	OSINT Roaming tiger by Anton Cherepanov from ESET	2
249	3	2016-04-19	2	OSINT - Python-Based PWOBot Targets European Organizations	1
221	3	2016-03-25	3	OSINT - New self-protecting USB trojan able to avoid detection	2
210	3	2016-03-16	3	OSINT - Malicious iBanking application with new uninstall countermeasures	1
184	3	2016-03-06	3	OSINT - New OS X Ransomware KeRanger Infected Transmission BitTorrent Client	1

				Installer	
1502	8	2018-01-08	1	Turla: Mosquito Whitepaper	13
1483	8	2019-05-28	4	Turla PowerShell blogpost	5
1475	8	2019-07-29	1	Machete just got sharper	7
14	2	2013-02-08	2	OSINT Adobe Zero-day Used in LadyBoyle Attack blog post by Symantec	5
1324	8	2018-11-19	1	OceanLotus - WateringHole - Framework B 2018	2
1316	8	2020-11-30	1	Turla Crutch: Keeping the “back door” open	3
1229	3	2022-01-16	4	MSFT - MSTIC - Destructive malware targeting Ukrainian organizations	2
1214	3	2021-03-26	2	OSINT - Analyzing attacks taking advantage of the Exchange Server vulnerabilities	14
121	3	2015-09-17	1	OSINT - THE DUKES 7 years of Russian cyberespionage	35
120	2	2015-09-14	3	OSINT The Shade Encryptor: a Double Threat by Kaspersky	7
12	2	2014-11-05	3	OSINT Banking Trojan DRIDEX Uses Macros for Infection blog post from Trend Micro	1
1134	3	2019-12-12	1	OSINT - GALLIUM: Targeting global telecom	1
1121	8	2019-10-07	1	Operation Ghost - White Paper	13
1114	3	2019-09-09	3	OSINT - ESET discovered an undocumented backdoor used by the infamous Stealth Falcon group	1
1077	8	2019-05-03	4	ESET Turla LightNeuron Research	2