Analisi delle minacce informatiche

Demo Test

- Questa pagina è stata lasciata intenzionalmente bianca -

Indice dei contenuti

1 INTRODUZIONE

L'analisi viene condotta interrogando database pubblici e privati al fine di rilevare evidenze di eventi che possano aver messo/mettere a rischio la sicurezza del perimetro esaminato. Ove previsto, viene effettuato un assessment della rete pubblica con scanner di rete in grado di rilevare le vulnerabilià dell'infrastruttura esposta.

Questo report prende in esame la superficie di attacco, le vulnerabilità tecniche, l'esposizione di asset aziendali su deepweb, dati di account divulgati attraverso data breach di terze parti, infezioni da malware, utilizzo di protocolli insicuri.

L'analisi è in grado di supportare l'azienda nell'individuare, comprendere e far adottare le migliori azioni correttive al fine di mitigare gli attacchi informatici, valutare i propri rischi tecnologici, identificare la divulgazione di dati aziendali.

Si specifica che se tra gli indirizzi IP analizzati sono stati inclusi anche indirizzi dinamici, alcune evidenze che prevedono lo storico dei dati potrebbero essere inesatte a causa di detta dinamicità.

2 PERIMETRO DELL'ANALISI

L'analisi viene svolta sui seguenti asset aziendali:

Reti	Domini	Mail
		mario.rossi@gmail.com

3 EXECUTIVE SUMMARY

COME VIENE CONDOTTA

L'analisi viene condotta interrogando database pubblici e privati al fine di rilevare evidenze di eventi che possano aver messo/mettere a rischio la sicurezza del perimetro esaminato. Ove previsto, viene effettuato un assessment della rete pubblica con scanner di rete in grado di rilevare le vulnerabilità dell'infrastruttura esposta.

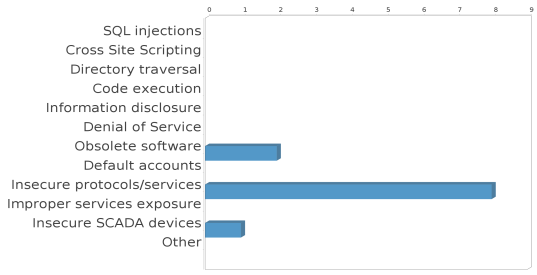
P2P MALWARE BREACHES

85
Applicazioni scaricate tramite file sharing con potenziale codice malevolo.

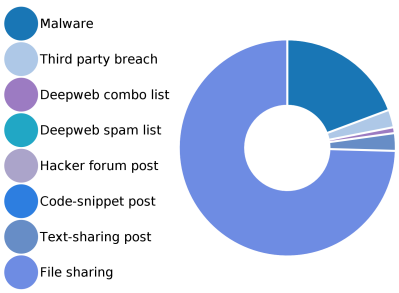
281
Eventi riportati attraverso analisi di botnet

38
Dati aziendali riscontrati in databreach

VULNERABILITIES



CYBER INCIDENTS



19%
degli host analizzati ha almeno una vulnerabilità grave

114
numero totale degli incidenti riportati

L'analisi effettuata prevede un numero massimo di rilevazioni pari a 5 postazioni/email per gli asset indagati. Tale numero non è sufficiente a garantire la rappresentazione dell'intero spettro di evidenze rilevate.

4 DETTAGLI SULLE EVIDENZE

4.1 Infezioni Malware

Dall'analisi svolta, emergono 281 eventi provocati da malware.

Data	Protocollo	Sorgente	Destinazione	Famiglia
2017-10-10 18:31:44 UTC	http	5*****2*****1:27156	3*****.*****8:80	unknown
2017-09-01 07:29:52 UTC	http	1*****2****2:58921	i*****g****t:80	unknown
2017-09-01 07:29:52 UTC	http	1*****2****2:24617	i*****g****t:80	unknown
2017-09-01 07:30:05 UTC	http	1*****2****2:58921	i*****g****t:80	unknown
2017-09-08 07:58:01 UTC	http	1*****2****2:35195	3*****.*****8:80	unknown
2017-09-08 07:58:01 UTC	http	1*****2****2:35195	3*****.*****8:80	unknown
2017-09-08 07:58:09 UTC	http	1*****2****2:35195	3*****.*****8:80	unknown
2017-09-08 07:58:09 UTC	http	1*****2****2:35195	3*****.*****8:80	unknown
2017-09-08 07:58:19 UTC	http	1*****2****2:35195	3*****.*****8:80	unknown
2017-09-08 07:58:19 UTC	http	1*****2****2:35195	3*****.*****8:80	unknown
2017-09-08 07:58:51 UTC	http	1*****2****2:35195	3*****.*****8:80	unknown
2017-09-08 07:58:51 UTC	http	1*****2****2:35195	3*****.*****8:80	unknown
2017-09-08 08:32:00 UTC	http	1*****2****2:5499	3*****.*****8:80	unknown
2017-09-08 08:32:00 UTC	http	1*****2****2:5499	3*****.*****8:80	unknown
2017-09-08 08:32:04 UTC	http	1*****2****2:5499	3*****.*****8:80	unknown
2017-09-08 08:32:04 UTC	http	1*****2****2:5499	3*****.*****8:80	unknown
2017-09-08 14:25:23 UTC	http	1*****2****2:38523	3*****.*****8:80	unknown
2017-09-08 14:25:23 UTC	http	1*****2****2:38523	3*****.*****8:80	unknown
2017-09-08 14:55:58 UTC	http	1*****2****2:53371	3*****.*****8:80	unknown
2017-09-08 14:55:58 UTC	http	1*****2****2:53371	3*****.*****8:80	unknown
2017-09-08 15:20:45 UTC	http	1*****2****2:28027	3*****.*****8:80	unknown
2017-09-08 15:20:45 UTC	http	1*****2****2:28027	3*****.*****8:80	unknown
2017-09-08 15:20:48 UTC	http	1*****2****2:28027	3*****.*****8:80	unknown
2017-09-08 15:20:48 UTC	http	1*****2****2:28027	3*****.*****8:80	unknown

Tabella 1: Infezioni Malware

Data	Protocollo	Sorgente	Destinazione	Famiglia
2017-09-08 15:36:59 UTC	http	1*****2****2:42619	3*****.*****8:80	unknown
2017-09-08 15:36:59 UTC	http	1*****2****2:42619	3*****.*****8:80	unknown
2017-09-11 07:27:56 UTC	http	1*****2****2:43131	3*****.*****8:80	unknown
2017-09-11 07:27:56 UTC	http	1*****2****2:43131	3*****.*****8:80	unknown
2017-09-11 07:28:02 UTC	http	1*****2****2:43131	3*****.*****8:80	unknown
2017-09-11 07:28:02 UTC	http	1*****2****2:43131	3*****.*****8:80	unknown
2017-09-11 07:28:36 UTC	http	1*****2****2:44923	3*****.*****8:80	unknown
2017-09-11 07:28:37 UTC	http	1*****2****2:44923	3*****.*****8:80	unknown
2017-09-11 07:28:37 UTC	http	1*****2****2:44923	3*****.*****8:80	unknown
2017-09-11 07:40:36 UTC	dns	1*****2****2:14851	i*****g****t	unknown
2017-09-11 07:40:36 UTC	dns	1*****2****2:13241	i*****g****t	unknown
2017-09-11 07:40:36 UTC	http	1*****2****2:31867	i*****g****t:80	unknown
2017-09-11 07:40:37 UTC	http	1*****2****2:31867	i*****g****t:80	unknown
2017-09-13 10:08:35 UTC	http	1*****2****2:21883	3*****.*****8:80	unknown
2017-09-13 10:08:35 UTC	http	1*****2****2:21883	3*****.*****8:80	unknown
2017-09-13 10:24:37 UTC	http	1*****2****2:10107	3*****.*****8:80	unknown
2017-09-20 09:54:04 UTC	http	1*****2****2:55849	3*****.*****8:80	unknown
2017-09-20 09:54:05 UTC	http	1*****2****2:55849	3*****.*****8:80	unknown
2017-09-20 09:54:12 UTC	http	1*****2****2:55849	3*****.*****8:80	unknown
2017-09-20 09:54:12 UTC	http	1*****2****2:55849	3*****.*****8:80	unknown
2017-10-02 12:51:34 UTC	dns	1*****2****2:45827	i******b*****t	conficker
2017-10-02 12:51:34 UTC	dns	1*****2****2:9913	i******b*****t	conficker
2017-10-02 12:51:34 UTC	dns	1*****2****2:17849	i******b*****t	conficker
2017-10-03 12:42:11 UTC	http	1*****2****2:14251	t*****e****s:80	unknown
2017-10-03 12:42:11 UTC	http	1*****2****2:14251	t*****e****s:80	unknown
2017-10-03 12:42:26 UTC	http	1*****2****2:14251	t*****e****s:80	unknown
2017-10-03 12:42:27 UTC	http	1*****2****2:14251	t*****e****s:80	unknown
2017-10-03 13:59:08 UTC	dns	1*****2****2:10425	t*****e****s	unknown
2017-10-03 13:59:13 UTC	http	1*****2****2:41001	t*****e****s:80	unknown

Tabella 1: Infezioni Malware

Data	Protocollo	Sorgente	Destinazione	Famiglia
2017-10-03 13:59:13 UTC	http	1*****2****2:41001	t*****e****s:80	unknown
2017-10-03 14:09:09 UTC	dns	1*****2****2:39609	t*****e****s	unknown
2017-10-03 14:09:10 UTC	http	1*****2****2:40745	t*****e****s:80	unknown
2017-10-03 14:09:10 UTC	http	1*****2****2:40745	t*****e****s:80	unknown
2017-10-03 14:38:36 UTC	dns	1*****2****2:46777	t*****e****s	unknown
2017-10-03 14:38:36 UTC	dns	1*****2****2:53177	t*****e****s	unknown
2017-10-03 14:38:37 UTC	dns	1*****2****2:14339	t*****e****s	unknown
2017-10-31 12:13:09 UTC	dns	1*****2****2:45753	y********n********m	unknown
2017-11-02 07:46:47 UTC	dns	1*****2****2:51129	y********n********m	unknown
2017-11-02 07:46:47 UTC	dns	1*****2****2:25859	y********n********m	unknown
2017-11-02 10:11:54 UTC	dns	1*****2****2:54713	y********n********m	unknown
2017-11-02 11:37:55 UTC	dns	1*****2****2:9475	y********n********m	unknown
2017-11-02 11:37:55 UTC	dns	1*****2****2:3769	y********n********m	unknown
2017-11-03 13:19:27 UTC	dns	1*****2****2:65209	y********n********m	unknown
2017-11-03 16:47:04 UTC	dns	1*****2****2:36025	y********n********m	unknown
2017-11-03 16:47:04 UTC	dns	1*****2****2:57347	y********n********m	unknown
2017-11-08 23:12:05 UTC	dns	1*****2****2:64441	v***k***z	unknown
2017-11-08 23:12:06 UTC	dns	1*****2****2:54457	v***k***z	unknown
2017-11-14 17:29:08 UTC	dns	1*****2****2:4537	t*****d*****o	conficker
2017-11-14 17:29:08 UTC	dns	1*****2****2:27651	t*****d*****o	conficker
2017-11-14 17:29:15 UTC	http	1*****2****2:42877	t*****d*****o:80	conficker
2017-11-14 17:29:15 UTC	http	1*****2****2:42877	t*****d*****o:80	conficker
2017-11-15 00:22:54 UTC	dns	1*****2****2:40121	v***k***z	unknown
2017-11-15 00:22:54 UTC	dns	1*****2****2:61955	v***k***z	unknown
2017-11-15 00:22:54 UTC	dns	1*****2****2:20665	v***k***z	unknown
2017-11-15 00:22:54 UTC	dns	1*****2****2:52995	v***k***z	unknown
2017-11-15 00:22:54 UTC	dns	1*****2****2:16899	v***k***z	unknown
2017-11-27 12:06:35 UTC	dns	1*****2****2:9145	y********n********m	unknown
2017-11-27 14:00:40 UTC	dns	1*****2****2:13753	y********n********m	unknown

Tabella 1: Infezioni Malware

Data	Protocollo	Sorgente	Destinazione	Famiglia
2017-11-29 09:20:54 UTC	dns	1*****2****2:10937	c****y****m	unknown
2017-11-30 12:05:03 UTC	dns	1*****2****2:5561	y********n********m	unknown
2017-11-30 13:53:26 UTC	dns	1*****2****2:47363	y********n********m	unknown
2017-11-30 13:53:26 UTC	dns	1*****2****2:2233	y********n********m	unknown
2017-12-01 11:17:32 UTC	dns	1*****2****2:1977	y********n********m	unknown
2017-12-01 11:30:32 UTC	dns	1*****2****2:58809	y********n********m	unknown
2017-12-01 13:51:56 UTC	dns	1*****2****2:22201	y********n********m	unknown
2018-01-08 13:13:29 UTC	http	1*****2****2:53545	a******t******m:80	unknown
2018-01-08 13:13:29 UTC	dns	1*****2****2:51385	a******t******m	unknown
2018-01-08 13:13:29 UTC	dns	1*****2****2:27907	a******t******m	unknown
2018-01-23 16:41:31 UTC	dns	1*****2****2:35769	a******t******m	unknown
2018-01-23 16:41:31 UTC	http	1*****2****2:16169	a******t******m:80	unknown
2018-01-26 09:52:01 UTC	dns	1*****2****2:6329	u*******i******o	unknown
2018-01-26 09:52:01 UTC	http	1*****2****2:21545	u*******i******o:80	unknown
2018-01-26 09:53:53 UTC	http	1*****2****2:34195	u*******i******o:80	unknown
2018-01-26 10:01:51 UTC	http	1*****2****2:42387	u*******i******o:80	unknown
2018-02-01 08:15:48 UTC	dns	1*****2****2:28163	a*****d*****m	unknown
2018-02-01 08:26:11 UTC	dns	1*****2****2:58553	a*****d*****m	unknown
2018-02-20 10:50:38 UTC	http	1*****2****2:4649	x*********l********m:80	unknown
2018-02-20 10:50:38 UTC	dns	1*****2****2:65209	x*********l********m	unknown
2018-02-20 10:50:38 UTC	http	1*****2****2:4649	x*********l********m:80	unknown
2018-02-20 10:51:22 UTC	http	1*****2****2:50301	x*********l********m:80	unknown
2018-02-20 10:51:22 UTC	http	1*****2****2:50301	x*********l********m:80	unknown
2018-02-20 10:52:23 UTC	dns	1*****2****2:38073	w**********i**********m	unknown
2018-02-20 10:52:23 UTC	dns	1*****2****2:1795	w**********i**********m	unknown
2018-02-20 10:56:21 UTC	http	1*****2****2:64893	x*********l********m:80	unknown
2018-02-20 10:56:22 UTC	http	1*****2****2:64893	x*********l********m:80	unknown
2018-02-20 10:56:26 UTC	http	1*****2****2:64893	x*********l********m:80	unknown
2018-02-20 10:56:27 UTC	http	1*****2****2:64893	x*********l********m:80	unknown

Tabella 1: Infezioni Malware

Data	Protocollo	Sorgente	Destinazione	Famiglia
2018-02-20 10:56:29 UTC	http	1*****2****2:64893	x*********l********m:80	unknown
2018-02-20 10:56:29 UTC	http	1*****2****2:64893	x*********l********m:80	unknown
2018-02-20 10:56:44 UTC	http	1*****2****2:64893	x*********l********m:80	unknown
2018-02-20 10:56:44 UTC	http	1*****2****2:64893	x*********l********m:80	unknown
2018-02-20 10:57:28 UTC	http	1*****2****2:34685	x*********l********m:80	unknown
2018-02-20 10:57:28 UTC	http	1*****2****2:34685	x*********l********m:80	unknown
2018-02-20 14:31:04 UTC	http	1*****2****2:25385	x*********l********m:80	unknown
2018-02-20 14:31:04 UTC	http	1*****2****2:25385	x*********l********m:80	unknown
2018-02-20 14:31:04 UTC	dns	1*****2****2:26553	x*********l********m	unknown
2018-02-20 14:31:39 UTC	http	1*****2****2:9513	x*********l********m:80	unknown
2018-02-20 14:31:39 UTC	http	1*****2****2:9513	x*********l********m:80	unknown
2018-02-20 14:33:11 UTC	http	1*****2****2:7209	w**********l*********m:80	unknown
2018-02-20 14:33:11 UTC	dns	1*****2****2:58041	w**********l*********m	unknown
2018-02-20 14:33:11 UTC	http	1*****2****2:7209	w**********l*********m:80	unknown
2018-02-20 14:36:39 UTC	http	1*****2****2:11049	x*********l********m:80	unknown
2018-02-20 14:36:39 UTC	http	1*****2****2:51241	x*********l********m:80	unknown
2018-02-20 18:06:42 UTC	dns	1*****2****2:37817	t****h***m	unknown
2018-02-20 18:06:42 UTC	http	1*****2****2:36649	t****h***m:80	unknown
2018-03-01 06:37:32 UTC	dns	1*****2****2:23225	a*****d*****m	unknown
2018-04-03 11:16:54 UTC	http	1*****2****2:17390	t*******a******m:80	unknown
2018-04-03 11:16:54 UTC	http	1*****2****2:5870	t*******a******m:80	unknown
2018-04-03 11:16:54 UTC	http	1*****2****2:62702	t*******a******m:80	unknown
2018-04-03 11:16:54 UTC	dns	1*****2****2:46851	t*******a******m	unknown
2018-04-03 11:16:54 UTC	http	1*****2****2:60398	t*******a******m:80	unknown
2018-04-03 11:16:54 UTC	http	1*****2****2:62702	t*******a******m:80	unknown
2018-04-03 11:16:54 UTC	http	1*****2****2:16110	t*******a******m:80	unknown
2018-04-03 11:16:54 UTC	http	1*****2****2:29678	t*******a******m:80	unknown
2018-04-03 11:19:36 UTC	http	1*****2****2:28398	w******d******t:80	unknown
2018-04-03 11:19:36 UTC	dns	1*****2****2:49392	w******d******t	unknown

Tabella 1: Infezioni Malware

Data	Protocollo	Sorgente	Destinazione	Famiglia
2018-04-03 11:19:39 UTC	dns	1*****2****2:30211	w******d******t	unknown
2018-04-13 15:24:50 UTC	dns	1*****2****2:51614	t*******a******m	unknown
2018-04-13 15:24:53 UTC	http	1*****2****2:28638	t*******a******m:80	unknown
2018-04-13 15:24:53 UTC	http	1*****2****2:24286	t*******a******m:80	unknown
2018-04-13 15:25:14 UTC	dns	1*****2****2:7279	m****p****t	PushDo
2018-04-13 15:25:16 UTC	http	1*****2****2:57054	m****p****t:80	PushDo
2018-04-13 15:25:16 UTC	http	1*****2****2:62430	m****p****t:80	PushDo
2018-04-13 15:25:17 UTC	http	1*****2****2:30190	w******d******t:80	unknown
2018-04-13 15:25:17 UTC	http	1*****2****2:30190	w******d******t:80	unknown
2018-04-13 15:25:17 UTC	dns	1*****2****2:31404	w******d******t	unknown
2018-04-13 17:43:31 UTC	dns	1*****2****2:16643	w****.***b	unknown
2018-04-13 17:43:34 UTC	dns	1*****2****2:36374	w****.***b	unknown
2018-04-13 17:43:37 UTC	dns	1*****2****2:28233	w****.***b	unknown
2018-04-13 17:43:37 UTC	dns	1*****2****2:28233	w****.***b	unknown
2018-04-13 17:45:18 UTC	dns	1*****2****2:12248	w****.***b	unknown
2018-04-16 14:01:59 UTC	dns	1*****2****2:52181	t*******a******m	unknown
2018-04-16 14:02:00 UTC	http	1*****2****2:48606	t*******a******m:80	unknown
2018-04-19 16:06:11 UTC	dns	1*****2****2:14629	p*********b*********g	unknown
2018-04-19 16:06:11 UTC	dns	1*****2****2:38878	p*********b*********g	unknown
2018-04-19 16:06:11 UTC	dns	1*****2****2:19459	p*********b*********g	unknown
2018-04-23 07:16:37 UTC	dns	1*****2****2:27679	b**********n**********m	unknown
2018-04-23 07:16:37 UTC	dns	1*****2****2:62467	b**********n**********m	unknown
2018-04-23 07:46:14 UTC	dns	1*****2****2:24235	b**********n**********m	unknown
2018-04-23 07:46:14 UTC	dns	1*****2****2:34563	b**********n**********m	unknown
2018-04-23 08:06:31 UTC	dns	1*****2****2:16698	b**********n**********m	unknown
2018-04-23 08:06:31 UTC	dns	1*****2****2:51971	b**********n**********m	unknown
2018-04-23 08:19:02 UTC	dns	1*****2****2:11267	b**********n**********m	unknown
2018-04-23 08:19:02 UTC	dns	1*****2****2:49968	b**********n**********m	unknown
2018-04-23 08:56:19 UTC	dns	1*****2****2:55285	b**********n**********m	unknown

Tabella 1: Infezioni Malware

Data	Protocollo	Sorgente	Destinazione	Famiglia
2018-04-23 08:56:19 UTC	dns	1*****2****2:48643	b**********n**********m	unknown
2018-04-23 08:58:30 UTC	dns	1*****2****2:52227	b**********n**********m	unknown
2018-04-23 08:58:30 UTC	dns	1*****2****2:45545	b**********n**********m	unknown
2018-04-23 09:23:07 UTC	dns	1*****2****2:64003	b**********n**********m	unknown
2018-04-23 09:23:07 UTC	dns	1*****2****2:12976	b**********n**********m	unknown
2018-04-23 09:56:54 UTC	dns	1*****2****2:35835	b**********n**********m	unknown
2018-04-23 09:56:54 UTC	dns	1*****2****2:54019	b**********n**********m	unknown
2018-04-24 06:58:59 UTC	dns	1*****2****2:47853	b**********n**********m	unknown
2018-04-24 06:58:59 UTC	dns	1*****2****2:58883	b**********n**********m	unknown
2018-04-24 07:04:37 UTC	dns	1*****2****2:3516	b**********n**********m	unknown
2018-04-24 07:04:37 UTC	dns	1*****2****2:47363	b**********n**********m	unknown
2018-04-24 07:05:31 UTC	dns	1*****2****2:30979	b**********n**********m	unknown
2018-04-24 07:05:31 UTC	dns	1*****2****2:6412	b**********n**********m	unknown
2018-04-24 07:46:14 UTC	dns	1*****2****2:23386	b**********n**********m	unknown
2018-04-24 07:46:14 UTC	dns	1*****2****2:57859	b**********n**********m	unknown
2018-04-24 12:49:32 UTC	dns	1*****2****2:61699	b**********n**********m	unknown
2018-04-24 12:49:32 UTC	dns	1*****2****2:53183	b**********n**********m	unknown
2018-04-27 06:57:35 UTC	dns	1*****2****2:57836	b**********n**********m	unknown
2018-04-27 06:58:43 UTC	dns	1*****2****2:18691	b**********n**********m	unknown
2018-04-30 11:59:42 UTC	dns	1*****2****2:63491	b**********n**********m	unknown
2018-04-30 11:59:42 UTC	dns	1*****2****2:41830	b**********n**********m	unknown
2018-04-30 12:10:48 UTC	dns	1*****2****2:56319	b**********n**********m	unknown
2018-04-30 12:10:48 UTC	dns	1*****2****2:55299	b**********n**********m	unknown
2018-05-03 12:13:59 UTC	dns	1*****2****2:62979	b**********n**********m	unknown
2018-05-03 12:13:59 UTC	dns	1*****2****2:52372	b**********n**********m	unknown
2018-05-04 07:25:22 UTC	dns	1*****2****2:15107	b**********n**********m	unknown
2018-05-04 07:25:22 UTC	dns	1*****2****2:25499	b**********n**********m	unknown
2018-05-04 07:45:58 UTC	dns	1*****2****2:23043	b**********n**********m	unknown
2018-05-04 07:45:58 UTC	dns	1*****2****2:17457	b**********n**********m	unknown

Tabella 1: Infezioni Malware

Data	Protocollo	Sorgente	Destinazione	Famiglia
2018-05-04 11:30:26 UTC	dns	1*****2****2:64897	b*********n*********m	unknown
2018-05-04 11:30:26 UTC	dns	1*****2****2:42755	b*********n*********m	unknown
2018-05-07 07:16:27 UTC	dns	1*****2****2:49135	b*********n*********m	unknown
2018-05-07 07:46:40 UTC	dns	1*****2****2:60931	b*********n*********m	unknown
2018-05-07 07:46:40 UTC	dns	1*****2****2:30460	b*********n*********m	unknown
2018-05-07 11:03:51 UTC	dns	1*****2****2:8730	b*********n*********m	unknown
2018-05-07 11:03:51 UTC	dns	1*****2****2:22019	b*********n*********m	unknown
2018-05-08 07:25:19 UTC	dns	1*****2****2:58774	b*********n*********m	unknown
2018-05-08 07:25:19 UTC	dns	1*****2****2:14595	b*********n*********m	unknown
2018-05-08 07:36:54 UTC	dns	1*****2****2:23811	b*********n*********m	unknown
2018-05-08 07:36:54 UTC	dns	1*****2****2:35066	b*********n*********m	unknown
2018-05-08 07:47:50 UTC	dns	1*****2****2:6403	b*********n*********m	unknown
2018-05-08 07:47:50 UTC	dns	1*****2****2:2927	b*********n*********m	unknown
2018-05-08 08:33:59 UTC	dns	1*****2****2:16873	t******a*****m	unknown
2018-05-08 08:33:59 UTC	http	1*****2****2:15523	t******a*****m:80	unknown
2018-05-09 07:47:43 UTC	dns	1*****2****2:55043	b*********n*********m	unknown
2018-05-09 07:47:43 UTC	dns	1*****2****2:21655	b*********n*********m	unknown
2018-05-09 14:35:03 UTC	dns	1*****2****2:25866	a*****e****m	unknown
2018-05-09 14:35:03 UTC	dns	1*****2****2:49411	a*****e****m	unknown
2018-05-09 14:35:03 UTC	dns	1*****2****2:18796	a*****e****m	unknown
2018-05-15 16:06:42 UTC	dns	1*****2****2:6190	b*********n*********m	unknown
2018-05-15 16:06:42 UTC	dns	1*****2****2:3075	b*********n*********m	unknown
2018-05-15 16:18:33 UTC	dns	1*****2****2:64771	b*********n*********m	unknown
2018-05-15 16:18:33 UTC	dns	1*****2****2:24475	b*********n*********m	unknown
2018-05-15 16:18:33 UTC	dns	1*****2****2:58559	b*********n*********m	unknown
2018-05-17 07:21:10 UTC	dns	1*****2****2:43779	b*********n*********m	unknown
2018-05-17 07:21:10 UTC	dns	1*****2****2:57874	b*********n*********m	unknown
2018-05-17 07:47:37 UTC	dns	1*****2****2:3075	b*********n*********m	unknown
2018-05-17 13:11:58 UTC	dns	1*****2****2:48719	b*********n*********m	unknown

Tabella 1: Infezioni Malware

Data	Protocollo	Sorgente	Destinazione	Famiglia
2018-05-17 13:11:58 UTC	dns	1*****2****2:35587	b*********n*********m	unknown
2018-05-17 13:31:18 UTC	dns	1*****2****2:37891	b*********n*********m	unknown
2018-05-17 13:31:18 UTC	dns	1*****2****2:50285	b*********n*********m	unknown
2018-05-17 13:59:11 UTC	dns	1*****2****2:24071	b*********n*********m	unknown
2018-05-17 13:59:11 UTC	dns	1*****2****2:20739	b*********n*********m	unknown
2018-05-17 16:15:23 UTC	dns	1*****2****2:32515	b*********n*********m	unknown
2018-05-17 16:21:09 UTC	dns	1*****2****2:58228	b*********n*********m	unknown
2018-05-18 12:46:15 UTC	dns	1*****2****2:28363	b*********n*********m	unknown
2018-05-21 07:12:27 UTC	dns	1*****2****2:10755	b*********n*********m	unknown
2018-05-21 07:12:27 UTC	dns	1*****2****2:25281	b*********n*********m	unknown
2018-05-21 09:57:20 UTC	dns	1*****2****2:51459	b*********n*********m	unknown
2018-05-21 09:57:20 UTC	dns	1*****2****2:60005	b*********n*********m	unknown
2018-05-21 12:42:33 UTC	dns	1*****2****2:46851	b*********n*********m	unknown
2018-05-21 12:42:33 UTC	dns	1*****2****2:9377	b*********n*********m	unknown
2018-05-22 07:08:42 UTC	dns	1*****2****2:43011	b*********n*********m	unknown
2018-05-22 07:08:42 UTC	dns	1*****2****2:45061	b*********n*********m	unknown
2018-05-22 07:46:19 UTC	dns	1*****2****2:54849	b*********n*********m	unknown
2018-05-22 07:46:19 UTC	dns	1*****2****2:22019	b*********n*********m	unknown
2018-05-22 13:47:51 UTC	dns	1*****2****2:41475	b*********n*********m	unknown
2018-05-22 13:47:51 UTC	dns	1*****2****2:33628	b*********n*********m	unknown
2018-05-22 17:38:32 UTC	http	1*****2****2:37870	b*********n*********m:80	unknown
2018-05-22 17:38:32 UTC	http	1*****2****2:37870	b*********n*********m:80	unknown
2018-05-22 17:38:32 UTC	dns	1*****2****2:30459	b*********n*********m	unknown
2018-05-23 07:46:08 UTC	dns	1*****2****2:9136	b*********n*********m	unknown
2018-05-23 07:46:08 UTC	dns	1*****2****2:14595	b*********n*********m	unknown
2018-05-23 09:27:25 UTC	dns	1*****2****2:45315	b*********n*********m	unknown
2018-05-23 09:27:25 UTC	dns	1*****2****2:64847	b*********n*********m	unknown
2018-05-23 10:37:59 UTC	dns	1*****2****2:57201	b*********n*********m	unknown
2018-05-23 10:37:59 UTC	http	1*****2****2:4334	b*********n*********m:80	unknown

Tabella 1: Infezioni Malware

Data	Protocollo	Sorgente	Destinazione	Famiglia
2018-05-23 10:38:00 UTC	http	1*****2****2:62446	b*********n*********m:80	unknown
2018-05-23 16:11:48 UTC	dns	1*****2****2:3587	b*********n*********m	unknown
2018-05-23 16:11:48 UTC	dns	1*****2****2:37594	b*********n*********m	unknown
2018-05-24 07:46:13 UTC	dns	1*****2****2:52227	b*********n*********m	unknown
2018-05-24 07:46:13 UTC	dns	1*****2****2:59612	b*********n*********m	unknown
2018-05-25 07:11:22 UTC	dns	1*****2****2:49155	b*********n*********m	unknown
2018-05-25 07:11:22 UTC	dns	1*****2****2:20382	b*********n*********m	unknown
2018-05-25 07:46:23 UTC	dns	1*****2****2:38862	b*********n*********m	unknown
2018-05-25 07:46:23 UTC	dns	1*****2****2:4867	b*********n*********m	unknown
2018-05-28 06:48:35 UTC	dns	1*****2****2:52739	b*********n*********m	unknown
2018-05-28 06:48:35 UTC	dns	1*****2****2:5227	b*********n*********m	unknown
2018-05-30 12:47:43 UTC	dns	1*****2****2:27951	b*********n*********m	unknown
2018-05-30 13:01:28 UTC	dns	1*****2****2:44826	b*********n*********m	unknown
2018-05-30 16:10:03 UTC	dns	1*****2****2:36355	b*********n*********m	unknown
2018-05-30 16:10:03 UTC	dns	1*****2****2:5591	b*********n*********m	unknown
2018-05-31 07:25:53 UTC	dns	1*****2****2:11964	b*********n*********m	unknown
2018-05-31 07:25:53 UTC	dns	1*****2****2:56835	b*********n*********m	unknown
2018-05-31 07:46:01 UTC	dns	1*****2****2:16729	b*********n*********m	unknown
2018-05-31 07:56:05 UTC	dns	1*****2****2:47854	b*********n*********m	unknown
2018-05-31 07:56:05 UTC	dns	1*****2****2:60419	b*********n*********m	unknown
2018-06-13 11:09:26 UTC	dns	1*****2****2:41475	b*********n*********m	unknown
2018-06-13 11:09:26 UTC	dns	1*****2****2:62979	b*********n*********m	unknown
2018-06-13 11:09:26 UTC	dns	1*****2****2:9129	b*********n*********m	unknown
2018-06-14 07:46:11 UTC	dns	1*****2****2:1283	b*********n*********m	unknown
2018-06-14 07:46:11 UTC	dns	1*****2****2:33698	b*********n*********m	unknown

Tabella 1: Infezioni Malware

I malware possono comportare gravi rischi per la sicurezza e per la privacy, poiché le infezioni potrebbero propagarsi nel perimetro di rete, danneggiare il contenuto dei vostri sistemi e porre gli stessi sotto il controllo di attaccanti esterni.

Numerose potrebbero essere le cause che provocano un'infezione da malware: questa potrebbe essere per esempio provocata da un'attacco phishing, dal mancato compimento di aggiornamenti sul sistema, dall'utilizzo di applicazioni non attendibili o dall'utilizzo di versioni di antivirus/antimalware obsoleti.

Pertanto, si consiglia di aggiornare immediatamente i propri sistemi, installare un antimalware su tutte le postazioni ed impedire agli utenti la deliberata installazione di applicazioni potenzialmente pericolose.

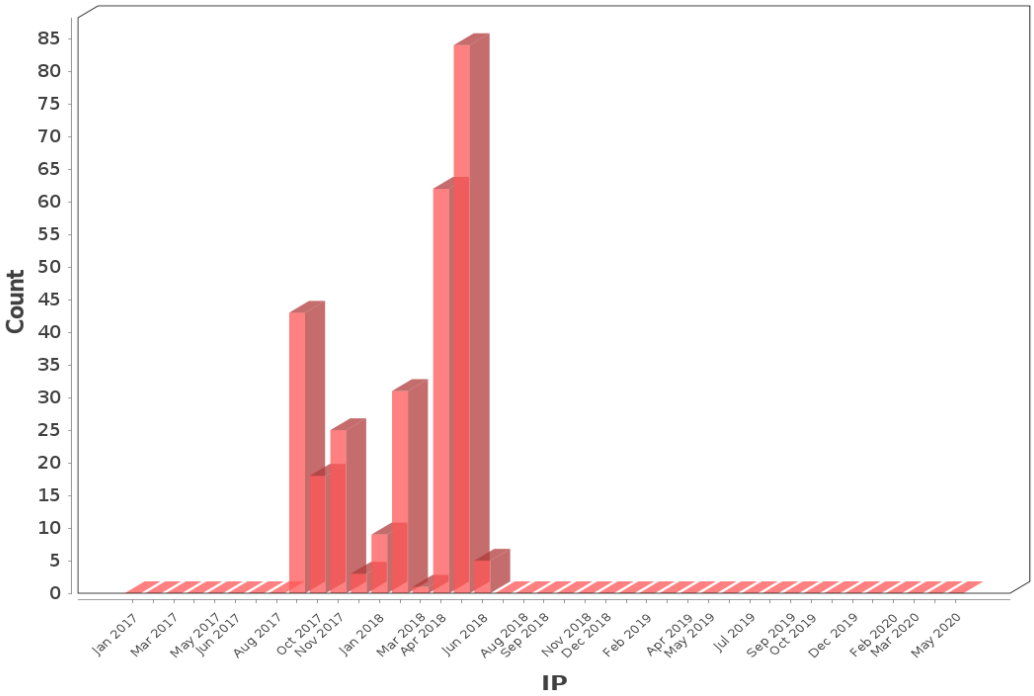


Grafico 1: Distribuzione eventi malware

4.2 Peer-to-Peer

Dall'analisi svolta, risultano 85 attività P2P che coinvolgono il vostro target.

IP	Data	Numero di evidenze	Files
5*****2*****1	13-09-2017	2	Jean Michel Jarre - Sublime Mix (Promo 2006) - Electronic
5*****2*****1	22-10-2017	2	Fruity Loops Studio 9.0 XXL
5*****2*****1	23-10-2017	2	FRUITY LOOPS Studio Producer Edition 9-cracks incl
5*****2*****1	05-11-2017	4	The Witcher 3: Wild Hunt - Blood and Wine (2.0.0.45) (GOG) The Witcher 3: Hild Hunt - Hearts of Stone (2.0.0.45) (GOG)
5*****2*****1	25-11-2017	2	FIFA 13 INTERNAL-RELOADED
5*****2*****1	13-05-2018	2	Ryszard Ä‡wirlej - RÄ™czna Robota [PL] eds [[emailÂ protected]]
5*****2*****1	12-06-2018	1	The.Sims.4.Dine.Out.INTERNAL-RELOADED
1*****.*****0	24-09-2017	31	Marcin Ciszewski - Powstanie Warszawskie [PL] MP3-256 Steve Cavanagh - Obrona [Audiobook PL] eds [[emailÂ protected]] Steve Cavanagh - Zarzut [Audiobook PL] eds [[emailÂ protected]] Tim Johnston - W DÃ³Å‚ [Audiobook PL] eds [[emailÂ protected]] Marcin WroÅ‚ski - Komisarz Maciejewski 1-8 [PL] eds [[emailÂ protected]] Katarzyna Bonda - Lampiony

Tabella 2: Peer-to-Peer

IP	Data	Numero di evidenze	Files
			[Audiobook PL] eds [[emailÂ protected]] Lee Child - Sprawa osobista [Audiobook PL] eds [[emailÂ protected]] Arno Strobel - Schemat [Audiobook PL] eds [[emailÂ protected]] Robin Cook - Znieczulenie [PL] [emailÂ protected] Grzegorz Kalinowski - SmierÄ‡ Frajerom [PL] [emailÂ protected]* Ryszard Ä‡wirlej - RÄ™czna Robota [PL] eds [[emailÂ protected]] Adam Cioczek - Koniec Gry [PL] eds [[emailÂ protected]] Nicolas Searle - Dobry Klamca PL] [emailÂ protected] Remigiusz MrÃ³z - Behawiorysta [PL] [emailÂ protected] Remigiusz Mroz - Chor Zapomnianych Glosow Rachel Abbott - Zabij mnie znÃ³w [PL] eds [[emailÂ protected]]
1*****.*****0	25-09-2017	2	Marek Å»elkowski - Kot z Cheshire [PL] [emailÂ protected]
1*****.*****0	26-09-2017	1	Slawek Michorzewski - Cyrk [PL] [emailÂ protected]
1*****.*****0	27-10-2017	1	Slawek Michorzewski - Cyrk [PL] [emailÂ protected]

Tabella 2: Peer-to-Peer

IP	Data	Numero di evidenze	Files
1*****.*****0	26-01-2018	2	Georges Brassens - Discografia [Mp3 128-160 kbps] [TNT Village]
1*****.*****0	17-05-2018	2	This Butt's 4 U 3 - Alexis Texas; Rita Faltoyano; Maria Bellucci
3*****2****9	19-10-2017	3	- non disponibile -
3*****2****9	04-11-2017	1	Rezerwat - Dotykaj (2016) [[emailÂ protected]]
3*****2****9	05-11-2017	3	- non disponibile -
3*****2****9	06-11-2017	1	- non disponibile -
3*****2****9	12-11-2017	1	Rezerwat - Dotykaj (2016) [[emailÂ protected]]
3*****2****9	22-11-2017	1	Rezerwat - Dotykaj (2016) [[emailÂ protected]]
3*****2****9	03-12-2017	2	Armin van Buuren Pres. Armind Best Of (2016) UKHx [EDM RG]
3*****2****9	08-12-2017	1	Rezerwat - Dotykaj (2016) [[emailÂ protected]]
3*****2****9	13-12-2017	1	Rezerwat - Dotykaj (2016) [[emailÂ protected]]
3*****2****9	16-12-2017	2	- non disponibile -
3*****2****9	25-12-2017	5	- non disponibile -
3*****2****9	07-01-2018	1	Izabela Trojanowska - Na Skos (2016) [[emailÂ protected]]
3*****2****9	12-01-2018	3	- non disponibile -
3*****2****9	28-01-2018	1	Izabela Trojanowska - Na Skos (2016) [[emailÂ protected]]
3*****2****9	05-03-2018	1	- non disponibile -
3*****.*****0	07-01-2018	4	Ryszard Ä‡wirlej - RÄ™czna Robota [PL] eds [[emailÂ protected]] Marcin WroÅ‚ski - Komisarz

Tabella 2: Peer-to-Peer

IP	Data	Numero di evidenze	Files
			Maciejewski 1-8 [PL] eds [[emailÂ protected]]

Tabella 2: Peer-to-Peer

Effettuare dei download tramite servizi P2P quali ad esempio BitTorrent rappresenta un'attività particolarmente pericolosa, poiché può comportare conseguenze dannose sia per il sistema stesso (i file scaricati potrebbero essere copie fasulle nonché malevoli dell'originale) sia per la reputazione di chi la compie. Sulle postazioni PC dell'organizzazione l'utente dovrebbe usufruire solo di un insieme limitato di funzionalità, le sole essenziali per lo svolgimento della propria attività lavorativa: in tal modo si riduce notevolmente il rischio di imbattersi nel download di file pericolosi. Per tale ragione, si consiglia di limitare i permessi dell'utente e, se possibile, di navigare sul web utilizzando un proxy che aiuti a filtrare il traffico malevolo.

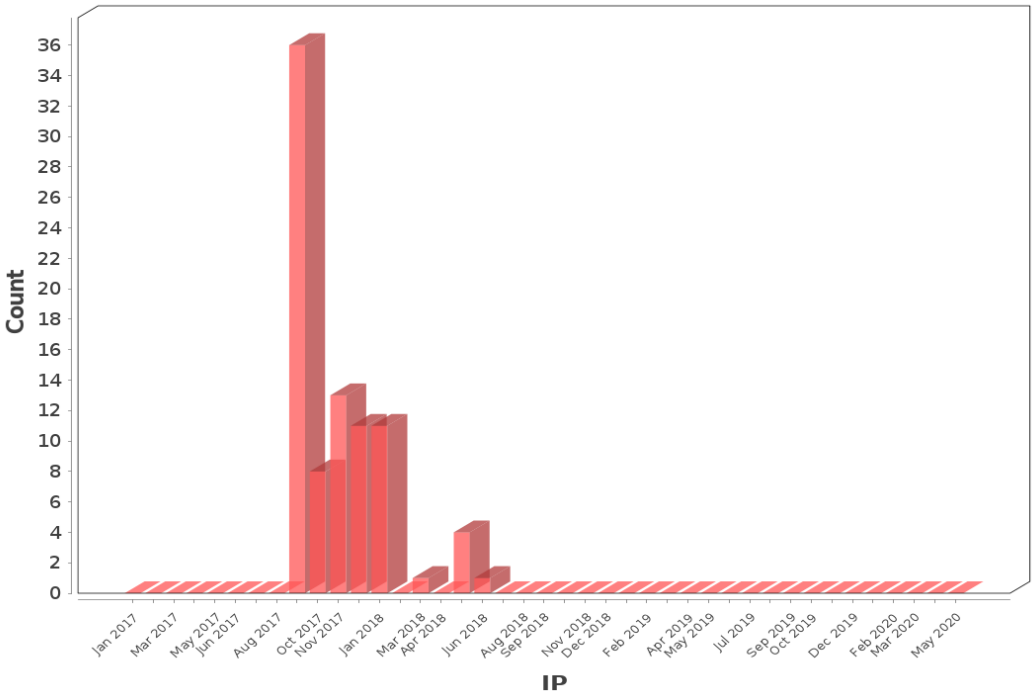


Grafico 2: Distribuzione eventi P2P

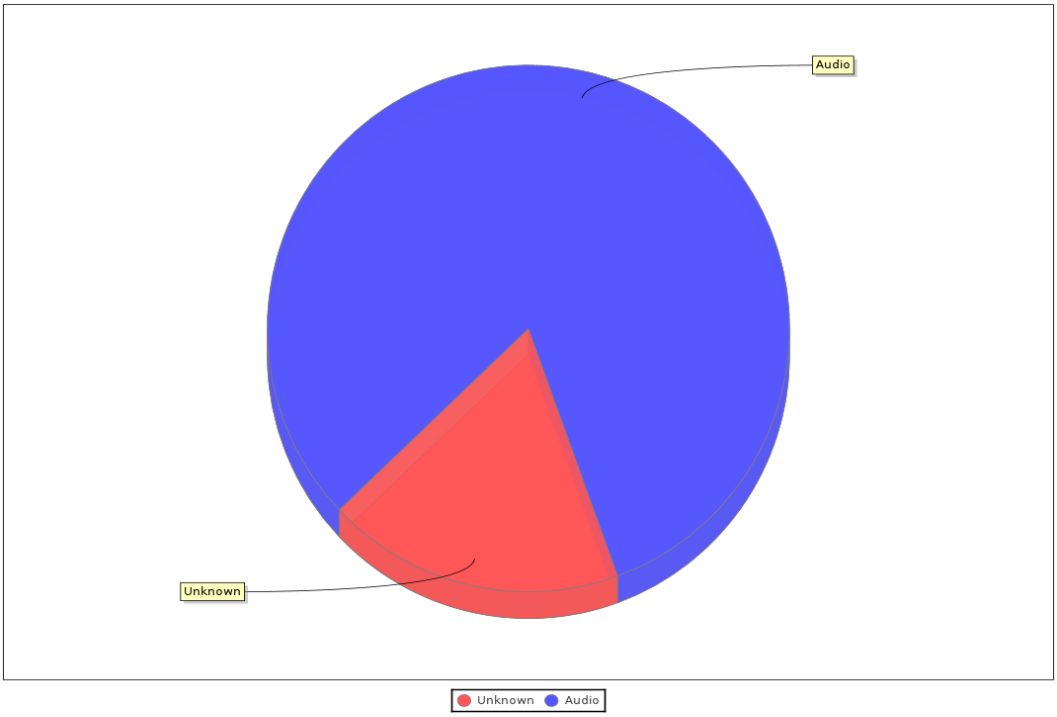


Grafico 3: Distribuzione tipologia file scaricati

4.3 Analisi email violate

Analizzando i data breach avvenuti negli ultimi anni, sono emersi riscontri per 5 indirizzi email aziendali univoci.

E-mail	Password in chiaro	Data	Sorgente
a****b***t	no	01-06-2012	dropbox
b****b***t	no	01-06-2012	dropbox
u****b***t	no	01-06-2012	dropbox
a*****@*****t	no	01-10-2013	adobe
b****b***t	no	01-10-2013	adobe
a****b***t	no	01-10-2013	adobe
l*******s******t	no	01-10-2013	adobe
a****b***t	no	01-10-2013	adobe
a*****@*****t	no	01-10-2013	adobe
a*****@*****t	no	01-10-2013	adobe
a****b***t	no	01-10-2013	adobe
a*****@*****t	no	01-10-2013	adobe
a****b***t	no	01-10-2013	adobe
a*****@*****t	no	01-10-2013	adobe
a*****@*****t	no	01-10-2013	adobe
a****b***t	no	01-06-2016	sensitive source
a****b***t	no	01-06-2016	sensitive source
a****b***t	no	01-06-2016	sensitive source
b****b***t	no	01-06-2016	sensitive source
a****b***t	no	01-06-2016	sensitive source

Tabella 3: Email violate

E-mail	Password in chiaro	Data	Sorgente
a****b***t	no	01-06-2016	sensitive source
a****b***t	no	01-06-2016	sensitive source
a****b***t	no	01-06-2016	sensitive source
b****b***t	si	01-12-2016	antipublic
b****b***t	si	01-12-2016	antipublic
b****b***t	si	01-12-2016	antipublic
b****b***t	si	01-12-2016	antipublic
b****b***t	si	01-12-2016	antipublic

Tabella 3: Email violate

Gli indirizzi email utilizzati dagli utenti per registrarsi presso i servizi web rappresentano un dato personale costantemente esposto. Infatti i più famosi service provider sono costantemente sotto la lente d'ingrandimento di cyber criminali, che spesso riescono a trafugare i dati dei clienti ottenendo talvolta accesso ad informazioni confidenziali (si pensi ad un furto di credenziali bancarie). Bisogna tenere conto del fatto che l'utilizzo di account adibiti ad uso lavorativo può portare alla pubblicazione di informazioni non solo personali, ma che possono coinvolgere un'intera organizzazione, esponendola quantomeno ad un danno reputazionale. Per questo motivo si consiglia di riservare l'account aziendale a scopi prettamente lavorativi (evitando di utilizzarlo - ad esempio - sui social network), al fine di evitare per quanto possibile che un data breach possa rappresentare, oltre che un danno per l'utente, anche un danno per i colleghi e per l'impresa.

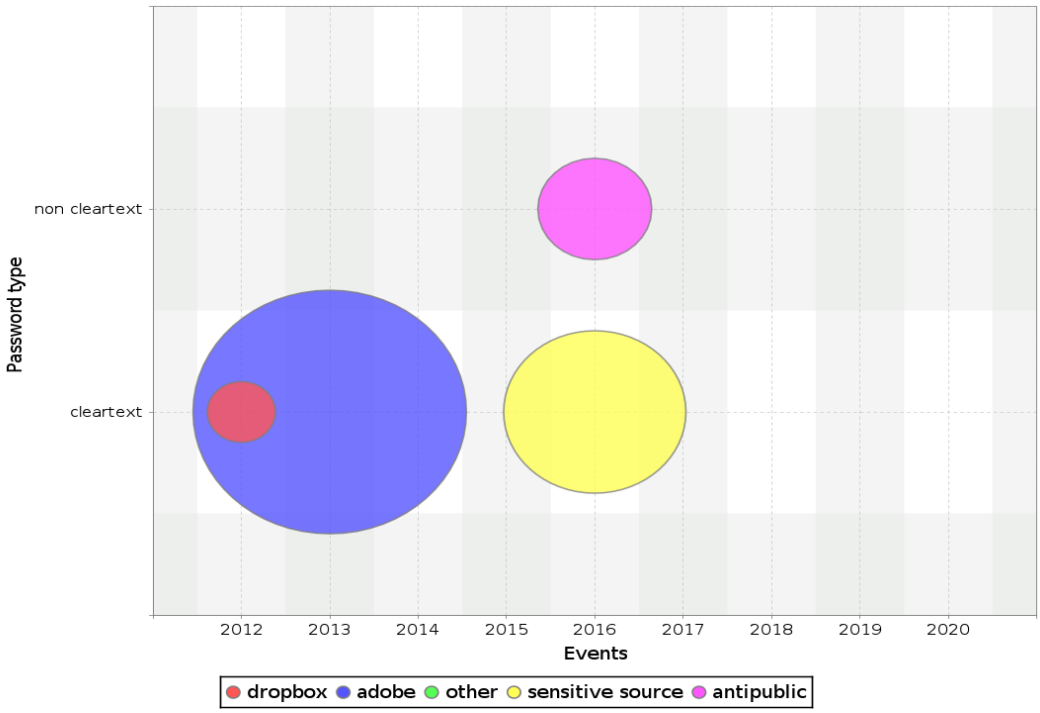


Grafico 4: Distribuzione delle email emerse dai data breach

4.4 Analisi Deep Web

Dall'analisi effettuata nei canali underground, emergono 3 evidenze che riguardano gli asset.

Asset	Link	Data	Tag	Numero di eventi
5*****2*****1	https://pastebin.com/JfEkLKQR	02-12-2017	ipv4: 335	335
b**.*t	https://pastebin.com/suPshHZ1	06-09-2017	email: 19767 ipv4: 1 link: 6154	25922
m**.*c	https://pastebin.com/mCDtDKT6	28-09-2017	link: 3337	3337

Tabella 4: Eventi nel Deep Web

Nei canali del Deep Web (forum, market, ed altre sorgenti underground) circolano numerose informazioni difficilmente catturabili nel Clear Web. Queste informazioni, talvolta, sono correlate ad attività criminali compiute da hacker, che potrebbero comunicare, tra gli altri motivi, per vendere o acquistare toolkit malevoli, organizzare attacchi, screditare persone o pubblicare dati confidenziali. Essere oggetto di discussione in queste bacheche rappresenta una minaccia per l'organizzazione, e l'attività di threat intelligence compie uno sforzo massiccio per intercettare queste comunicazioni, con lo scopo di prevenire o quantomeno limitare il più possibile i danni sul target. Si consiglia di istruire il più possibile i propri dipendenti ad un uso consapevole delle proprie postazioni e di adottare le più comuni ed indispensabili buone norme di sicurezza (ad esempio utilizzare sistemi antimalware), al fine di ridurre il più possibile la superficie d'attacco e minimizzare il più possibile i rischi.

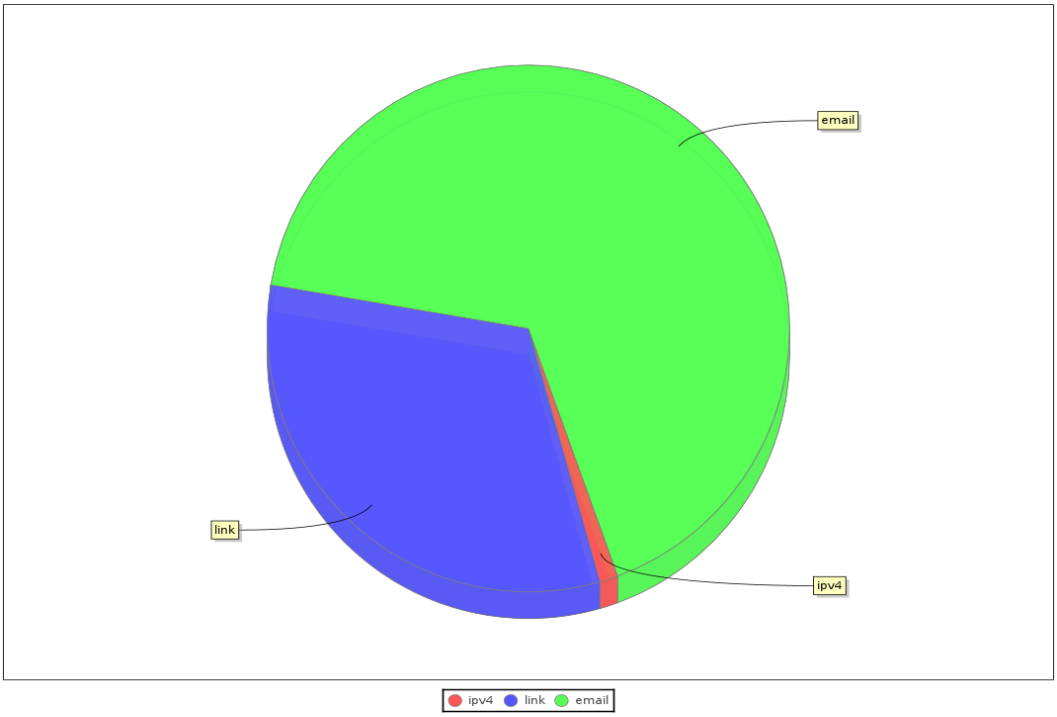


Grafico 5: Distribuzione attività nel Deep Web

4.5 Superficie d'attacco

Dall'analisi effettuata sul perimetro aziendale, sono state rilevate 7 porte aperte.

IP	Data rilevazione	Porta
4****.***1	22-11-2017	995
1*****1****8	14-03-2018	22
4****.***1	22-11-2017	443
8*****1*****0	14-03-2018	20000
1*****2****2	14-03-2018	443
1******.******6	14-03-2018	443
4****8****5	14-03-2018	23

Tabella 5: Porte aperte

Esporre sulla rete pubblica dei servizi rappresenta un rischio per la sicurezza dell'azienda poiché offre un canale d'accesso agli attaccanti, che utilizzandole possono accedere dall'esterno e poi, sfruttando le più avanzate tecniche di hacking, possono acquisire o compromettere informazioni riservate, provocando una perdita economica tangibile all'organizzazione. Molto spesso una situazione di questo tipo è dovuta ad una mancata configurazione dei dispositivi di rete: le impostazioni di default con cui essi sono stato installati, la maggior parte delle volte, non sono assolutamente sufficienti a proteggere il perimetro di rete aziendale. Altra circostanza particolarmente critica è costituita dall'utilizzo di porte come telnet e ftp, che consentono la trasmissione di informazioni in chiaro e pertanto andrebbero disabilitate. Per questi motivi, si suggerisce caldamente di affidarsi a personale specializzato che si occupi di disabilitare i servizi inutili e/o pericolosi e di configurare correttamente le connessioni di rete aziendali, magari proteggendole con dispositivi come firewall (c.d. hardening dei sistemi).

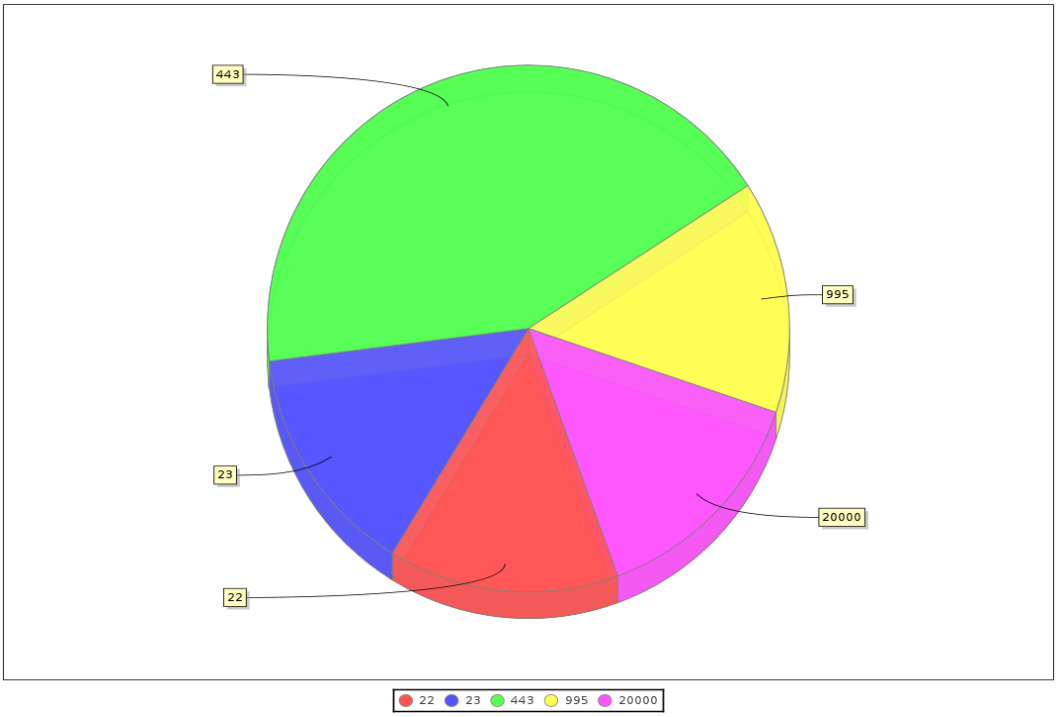


Grafico 6: Distribuzione porte aperte

4.6 Vulnerability Assessment

Il Vulnerability Assessment è stato effettuato utilizzando modalità di rilevamento passive.

Nell'analisi delle minacce è stato verificato se i vostri asset sono esposti alle seguenti vulnerabilità:

- SSLv3: sebbene molti browser e server abbiano ormai integrato le più recenti evoluzioni del protocollo di cifratura delle comunicazioni HTTPS - in particolare TLS 1.2 - gran parte di essi offrono tutt'oggi la possibilità di comunicare con protocolli obsoleti quali es. SSL 3.0. SSLv3 soffre di molteplici vulnerabilità architetturali per le quali è stato deprecato e posto fuori dalle principali policy di compliance in materia di sicurezza informatica;
- I server che accettano, come suite di cifratura, RSA_EXPORT sono esposti alla cosiddetta vulnerabilità FREAK. Questa vulnerabilità può portare ad un downgrade della robustezza della comunicazione, favorendo gli attaccanti che tentano di decifrare il traffico;
- Un server che accetti la suite di cifratura DHE_EXPORT presenta un'altra problematica, denominata LogJam, i cui effetti sono gli stessi della vulnerabilità FREAK;
- HEARTBLEED, una grave vulnerabilità scoperta nel 2014, rappresenta un difetto di implementazione che permette agli attaccanti di visualizzare porzioni di memoria non autorizzate, permettendo ad esempio di accedere alla chiave privata utilizzata dal web server o a cookie di sessione presenti in memoria al momento dell'attacco.
- L'utilizzo di protocolli INSICURI, la cui presenza sul perimetro è sconsigliata e potrebbe favorire la violazione dei sistemi aziendali da parte di un attaccante.
- L'esposizione INAPPROPRIATA di servizi (es. MySQL), con conseguente rischio di violazione di dati confidenziali.
- Il rilevamento sulla rete pubblica aziendale di dispositivi SCADA, che potrebbero essere violati (es. manomissione di un sensore di temperatura) con rischi per la sicurezza fisica delle strutture e delle persone.

Sono state rilevate 11 vulnerabilità sul vostro perimetro.

Target	Vulnerabilità	Severity	Soluzione
4****8****5	Insecure protocols/services	HIGH	Chiudi le ACL del firewall o disabilita i servizi non necessari.
1******.******6	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	MEDIUM	Riconfigura il servizio rimuovendo il supporto per le suite di cifratura EXPORT_RSA.

Tabella 6: Vulnerability Assessment

Target	Vulnerabilità	Severity	Soluzione
4*****.***1	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	MEDIUM	Riconfigura il servizio rimuovendo il supporto per le suite di cifratura EXPORT_RSA.
4*****.***1	SSL Version 2 and 3 Protocol Detection	MEDIUM	Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e SSL 3.0. Utilizza TLS 1.1 (con suite di cifratura approvate) o una versione più recente.
8*****1*****0	Insecure protocols/services	MEDIUM	Chiudi le ACL del firewall o disabilita i servizi non necessari.
8*****1*****0	Insecure SCADA devices	MEDIUM	Disabilita l'accesso da remoto a questo dispositivo e, se possibile, spostalo dalla perimetro internet pubblico dell'azienda.
1******.******6	SSL Version 2 and 3 Protocol Detection	MEDIUM	Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e SSL 3.0. Utilizza TLS 1.1 (con suite di cifratura approvate) o una versione più recente.
1*****1****8	Insecure protocols/services	MEDIUM	Chiudi le ACL del firewall o disabilita i servizi non necessari.
1******.******6	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	LOW	Riconfigura il servizio rimuovendo il supporto per le suite di cifratura EXPORT_DHE.
1*****1****8	Improper services exposure	LOW	Disabilita l'accesso da remoto a questo servizio, o configuralo tramite una Virtual Private Network.
4*****.***1	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	LOW	Riconfigura il servizio rimuovendo il supporto per le suite di cifratura EXPORT_DHE.

Tabella 6: Vulnerability Assessment

Ogni tipo di applicazione e servizio che si interfaccia col web rappresenta una potenziale minaccia per l'organizzazione, soprattutto se mal configurata, non aggiornata o utilizzata in malo modo. Tra queste applicazioni rientrano anche una serie di strumenti che supportano l'utente nella comunicazione attraverso internet: ad esempio, un frequente numero di vulnerabilità si riscontra nella configurazione SSL dei propri sistemi e nei certificati digitali che si adottano per tali comunicazioni. Per questo motivo, si suggerisce di monitorare i propri sistemi, mantenere aggiornate tutte le applicazioni che vi sono installate ed affidarsi a personale specializzato per lo

svolgimento di attività di analisi, quali ad esempio Vulnerability Assessment e Penetration Test.

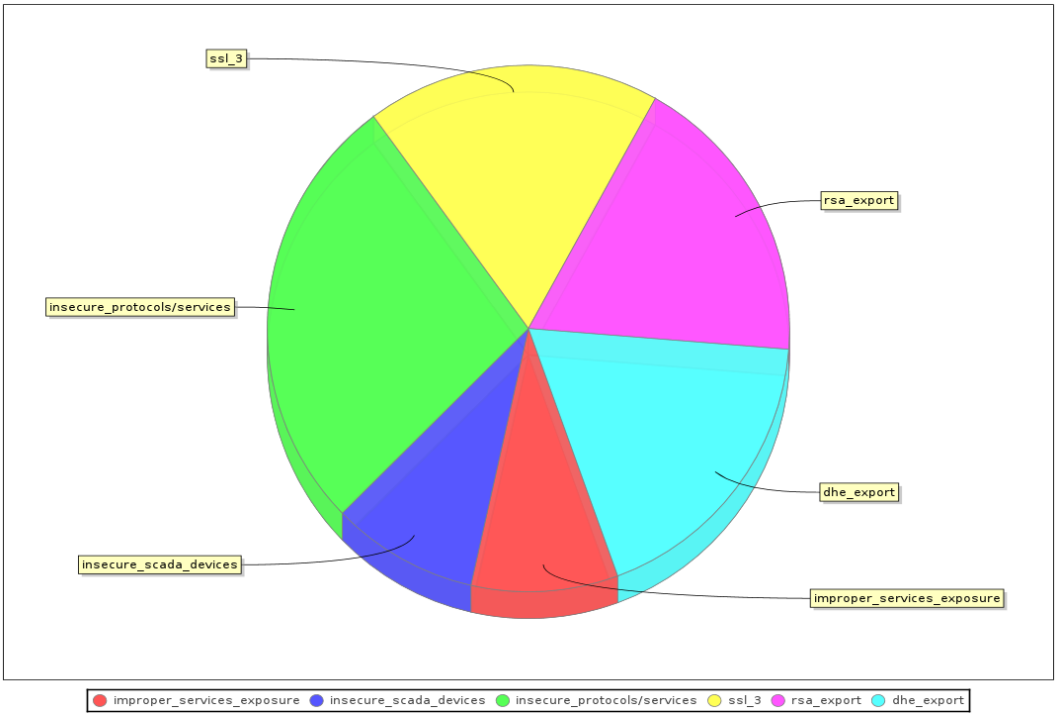


Grafico 7: Distribuzione vulnerabilità passive

- ALLEGATI -

ALLEGATO 1: METRICA DELLE VULNERABILITÀ

1.1 CVSS2 SCORE

CVSS2 Score è uno standard utilizzato per descrivere le caratteristiche e l'impatto di una vulnerabilità. Esso è composto da tre indici primari: "Base vector", "Temporal vector" ed "Environment vector": ogni indice è composto da un riferimento numerico, variabile tra 0 e 10, che indentifica la gravità della vulnerabilità e da un vettore che ne specifica le caratteristiche. Per una dettagliata documentazione relativa il calcolo e le specifiche dello standard CVSS2 si faccia riferimento al NVD Common Vulnerability Scoring System Support v2 e alla FIRST CSSV 2.0 Guide.

1.2 BASE VECTOR

Il "Base vector" identifica le caratteristiche di una vulnerabilità costanti nel tempo come combinazione di sei fattori; essi definiscono sia le modalità con cui è possibile sfruttare la vulnerabilità e se sono necessarie condizioni al contorno al fine di effettuare un attacco con successo ("Access Vector", "Access Complexity", "Authentication metrics"), sia l'impatto in termini di perdita di confidenzialità, integrità e disponibilità qualora la vulnerabilità sia sfruttata.

1.2.1 ACCESS VECTOR (AV)

Questa metrica definisce la modalità tramite cui è possibile sfruttare la vulnerabilità, classificabile nei seguenti valori.

Valore	Descrizione
Local (L)	La vulnerabilità è sfruttabile unicamente avendo un accesso al target con privilegi locali; l'aggressore deve quindi avere un accesso fisico al target o una shell remota disponibile.
Adjacent Network (A)	La vulnerabilità è sfruttabile unicamente se l'aggressore ha accesso ad una rete collegata a quella dov'è presente il target (IP subnet, Bluetooth, IEEE 802.11).
Network (N)	La vulnerabilità è sfruttabile senza avere accesso alla rete locale; in genere, queste vulnerabilità sono dette "remotely exploited" (es. RPC buffer overflow).

Tabella 7: Metrica Access Vector (AV)

1.2.2 ACCESS COMPLEXITY (AC)

Questa metrica descrive la complessità necessaria ad eseguire l'attacco: alcune vulnerabilità, per poter essere sfruttate con successo, richiedono diverse azioni quali l'apertura di un file infetto, lo scaricamento di un allegato da email, etc. Nella tabella a seguire sono indicate le possibili classificazioni di questa metrica.

Valore	Descrizione
High (H)	Per portare a termine l'attacco con successo devono essere presenti alcune condizioni a contorno quali: • l'aggressore deve già possedere specifici privilegi o la possibilità di eseguire spoofing di altri sistemi (es. DNS Hijacking); • l'attacco dipende dall'utilizzo di metodi di "social engineering", di facile identificazione per persone addestrate; ad esempio la vittima deve eseguire azioni sospette o atipiche come eseguire l'allegato di una mail; • le condizioni che rendono il sistema vulnerabile, nella realtà hanno rare applicazioni; il sistema potrebbe essere compromesso "in teoria" ma, ad esempio, la scrittura del codice necessario a sfruttare la vulnerabilità potrebbe rivelarsi estremamente lunga e complessa; se esiste una "race condition", la finestra per sfruttarla è molto stretta.
Medium (M)	Per sfruttare la vulnerabilità sono necessarie condizioni particolari, ad esempio: • la parte vulnerabile è limitata ad un gruppo di sistemi o utenti con specifici livelli di autorizzazione; • al fine di eseguire l'attacco con successo, l'aggressore deve avere a disposizione informazioni non di pubblico dominio; • la configurazione affetta dalla vulnerabilità non è presente nell'installazione di default o normalmente non è utilizzata; l'attacco necessità di attività di "social engineering" che possono occasionalmente confondere anche gli utenti più cauti (attacchi di phishing che modificano la status bar del browser per mostrare un link fasullo).
Low (L)	Non sussistono particolari condizioni per sfruttare la vulnerabilità: • il prodotto affetto dalla vulnerabilità è normalmente acceduto da una vasto bacino di utenti (es. Internet); • la configurazione vulnerabile è quella presente nell'installazione di default; • l'attacco può essere eseguito manualmente e richiede poche skill o informazioni aggiuntive; se esiste una "race condition", è facilmente sfruttabile.

Tabella 8: Metrica Access Complexity (AC)

1.2.3 AUTHENTICATION (AU)

Questa metrica specifica se e in che numero l'aggressore deve autenticarsi al sistema target per sfruttare la vulnerabilità con successo. Non è tenuto conto della complessità del sistema di

autenticazione, ma si valuta unicamente se un attaccante deve fornire credenziali valide prima dell'attacco. Questa metrica è classificabile nei seguenti valori.

Valore	Descrizione
Multiple (M)	Per sfruttare la vulnerabilità l'aggressore deve autenticarsi due o più volte.
Single (S)	Per sfruttare la vulnerabilità l'aggressore deve autenticarsi una sola volta.
None (N)	Non è necessaria alcuna autenticazione.

Tabella 9: Metrica Authentication (Au)

1.2.4 CONFIDENTIALITY IMPACT (C)

Questa metrica misura l'impatto sulla confidenzialità del sistema qualora la vulnerabilità sia sfruttata con successo. Per "confidenzialità" si intende sia la possibilità di accedere a informazioni presenti sul sistema unicamente per gli utenti autorizzati sia la possibilità di impedirne l'accesso a quelli non autorizzati. A questa metrica sono associati i seguenti valori.

Valore	Descrizione
None (N)	Lo sfruttamento della vulnerabilità non ha impatto sulla confidenzialità del sistema.
Partial (P)	Lo sfruttamento della vulnerabilità permette di accedere a molte informazioni presenti sul sistema ma non di ottenere il controllo totale dello stesso.
Complete (C)	Lo sfruttamento della vulnerabilità permette di accedere a tutte le informazioni presenti sul sistema oggetto dell'attacco.

Tabella 10: Metrica Confidentiality Impact (C)

1.2.5 INTEGRITY IMPACT (I)

Questa metrica valuta l'impatto sull'integrità dei dati del sistema qualora la vulnerabilità sia sfruttata con successo. Con "integrità" s'intende la garanzia che le informazioni non possano essere alterate. A questa metrica sono associati i seguenti valori.

Valore	Descrizione
None (N)	Lo sfruttamento della vulnerabilità non ha impatto sull'integrità del sistema.
Partial (P)	Lo sfruttamento della vulnerabilità permette di modificare alcuni file di sistema o dati presenti su di esso; tuttavia

Tabella 11: Metrica Integrity Impact (I)

Valore	Descrizione
	l'aggressore non ha il controllo su cosa può modificare oppure ha accesso ad un limitato insieme di informazioni.
Complete (C)	Lo sfruttamento della vulnerabilità porta ad una compromissione totale dell'integrità del sistema; l'aggressore può modificare tutti i file presenti sul sistema target.

Tabella 11: Metrica Integrity Impact (I)

1.2.6 AVAILABILITY IMPACT (A)

Questa metrica misura l'impatto sulla disponibilità a fronte di una vulnerabilità sfruttata con successo. Con disponibilità s'intende la possibilità di accedere costantemente alla risorsa. L'attaccante può ad esempio saturare la banda della rete, la CPU di un sistema o lo spazio disco del sistema target. I possibili valori associabili a questa metrica sono i seguenti.

Valore	Descrizione
None (N)	Lo sfruttamento della vulnerabilità non ha impatti sulla disponibilità.
Partial (P)	Lo sfruttamento della vulnerabilità causa una riduzione delle performance o brevi interruzioni del servizio. Ad esempio un flood attack può limitare, per la durata dell'attacco, il numero di connessioni accettate da un servizio internet.
Complete (C)	Lo sfruttamento della vulnerabilità porta ad un disservizio generale; l'aggressore può rendere la risorsa inutilizzabile.

Tabella 12: Metrica Authentication (A)

Come esempio, una vulnerabilità con le seguenti metriche di base:

- Access Vector: Low;
- Access Complexity: Medium;
- Authentication: None;
- Confidentiality Impact: None;
- Integrity Impact: Partial;
- Availability Impact: Complete

avrà il seguente Base vector: AV:L/AC:M/Au:N/C:N/I:P/A:C

1.3 LIVELLI DI CRITICITÀ (SEVERITY)

La severity delle vulnerabilità è espressa in tre differenti livelli di rischio che vengono di seguito descritti.

Livello di criticità	Descrizione
 HIGH	La vulnerabilità consente ad un aggressore di compromettere il sistema target e/o consentire di recuperare informazioni particolarmente sensibili. (CVSS score: 7.0-10.0)
 MEDIUM	La vulnerabilità potrebbe permettere ad un aggressore di compromettere il sistema target, ma alcune circostanze al contorno impediscono di sfruttarla efficaciemente. (CVSS score: 4.0-6.9)
 LOW	La vulnerabilità consente ad un aggressore di ottenere informazioni utili per pianificare successivi attacchi mirati al sistema target. (CVSS score: 0.0-3.9)

Tabella 13: Livelli di criticità

1.4 RIFERIMENTI

Nella tabella seguente si riportano infine i riferimenti utilizzati per le vulnerabilità rilevate; essi consentono di recuperare, presso i portali indicati, informazioni aggiuntive su tali vulnerabilità.

Riferimento	Descrizione	URL
CVE	Common Vulnerabilities and Exposures	http://www.cve.mitre.org/
CAN	CVE Candidate Name	http://www.cve.mitre.org/
BID	Bugtraq ID	http://www.securityfocus.com/bid
XF	ISS XForce Database	http://xforce.iss.net/
SECUNIA	Secunia Bulletin	http://secunia.com
OSVDB	Open Source Vulnerability Data Base	http://www.ovsdb.org
OWASP	Open Web Application Security Project	http://www.owasp.org

Tabella 14: Riferimenti vulnerabilità

ALLEGATO 2: DETTAGLI SULLE VULNERABILITÀ

Sono state trovate 11 vulnerabilità.

2.1 HOST 1******.******6

Sono state rilevate 3 vulnerabilità su questo host.

Asset: 1******.******6

Severity: MEDIUM

Date: 2018-03-14 07:23:49 UTC

Port: 443

IP: 1******.******6

CVSS score: 4.3

CVSS vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

L'host supporta le suite di cifratura EXPORT_RSA con chiavi di lunghezza inferiore a 512 bit. Un attaccante potrebbe fattorizzare un modulo RSA in un breve lasso di tempo

Un attaccante, tramite attacco man-in-the-middle potrebbe effettuare il downgrade della sessione forzando l'utilizzo di suite EXPORT_RSA. Perciò, si raccomanda di disabilitare il supporto di suite di cifratura deboli.

Soluzione:

Riconfigura il servizio rimuovendo il supporto per le suite di cifratura EXPORT_RSA.

Asset: 1******.******6

Severity: MEDIUM

Date: 2018-03-14 07:23:49 UTC

Port: 443

IP: 1******.******6

CVSS score: 5

CVSS vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

SSL Version 2 and 3 Protocol Detection

Il servizio accetta connessioni cifrate mediante SSL 2.0 e/o SSL 3.0. Queste versioni di SSL hanno numerose criticità, ad esempio:

- Uno schema di padding insicuro con gli algoritmi di cifratura CBC;
- Schemi di rinegoziazione dei parametri insicuri.

Un attaccante può sfruttare queste vulnerabilità per compiere attacchi man-in-the-middle o per decrittare le comunicazioni tra server e client.

Anche se SSL/TLS possiede strumenti efficaci per scegliere la più recente versione supportata del protocollo (facendo sì che tali versioni obsolete vengano scelte solo quando client o server non ne supportano altre), molti browser implementano tale meccanismo in maniera non sicura permettendo all'attaccante di effettuare un "downgrade" della connessione (come accade nell' attacco POODLE). Perciò si raccomanda di disabilitare del tutto tali protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per effettuare comunicazioni sicure. A partire dalla data stabilita dallo standard PCI DSS v3.1, qualsiasi versione di SSL non corrisponderà alla definizione, data dal PCI SSC, di 'crittografia forte'.

Soluzione:

Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e SSL 3.0. Utilizza TLS 1.1 (con suite di cifratura approvate) o una versione più recente.

Asset: 1******.******6

Severity: LOW

Date: 2018-03-14 07:23:49 UTC

Port: 443

IP: 1******.******6

CVSS score: 2.6

CVSS vector: CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N

SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

L'host supporta le suite di cifratura EXPORT_DHE con chiavi di lunghezza inferiore a 512 bit. Tramite crittoanalisi, una terza parte può indovinare la chiave condivisa in un breve lasso di tempo.
Un attaccante, tramite attacco man-in-the-middle potrebbe effettuare il downgrade della sessione forzando l'utilizzo di suite EXPORT_DHE. Perciò, si raccomanda di disabilitare il supporto di suite di cifratura deboli.

Soluzione:

Riconfigura il servizio rimuovendo il supporto per le suite di cifratura EXPORT_DHE.

2.2 HOST 1*****1****8

Sono state rilevate 2 vulnerabilità su questo host.

Asset: 1*****1****8

Severity: MEDIUM

Date: 2018-03-14 07:23:49 UTC

Port: 22

IP: 1*****1****8

Insecure protocols/services

Sull'host remoto è stato individuato un protocollo insicuro. Questo servizio potrebbe essere facilmente violato da un attaccante perché obsoleto e/o espone traffico di rete in chiaro, compromettendone confidenzialità ed integrità.

Soluzione:

Chiudi le ACL del firewall o disabilita i servizi non necessari.

Asset: 1*****1****8

Severity: LOW

Date: 2018-03-14 07:23:49 UTC

Port: 22

IP: 1*****1****8

Improper services exposure

L'host remoto espone un servizio inappropriato che tipicamente gestisce dati confidenziali. Per tale ragione un attaccante potrebbe essere attratto e tentare di violarlo.

Soluzione:

Disabilita l'accesso da remoto a questo servizio, o configuralo tramite una Virtual Private Network.

2.3 HOST 4****.***1

Sono state rilevate 3 vulnerabilità su questo host.

Asset: 4*****.***1

Severity: MEDIUM

Date: 2017-11-22 06:49:32 UTC

Port: 443

IP: 4*****.***1

CVSS score: 4.3

CVSS vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

L'host supporta le suite di cifratura EXPORT_RSA con chiavi di lunghezza inferiore a 512 bit. Un attaccante potrebbe fattorizzare un modulo RSA in un breve lasso di tempo

Un attaccante, tramite attacco man-in-the-middle potrebbe effettuare il downgrade della sessione forzando l'utilizzo di suite EXPORT_RSA. Perciò, si raccomanda di disabilitare il supporto di suite di cifratura deboli.

Soluzione:

Riconfigura il servizio rimuovendo il supporto per le suite di cifratura EXPORT_RSA.

Asset: 4*****.***1

Severity: MEDIUM

Date: 2017-11-22 06:49:32 UTC

Port: 443

IP: 4*****.***1

CVSS score: 5

CVSS vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

SSL Version 2 and 3 Protocol Detection

Il servizio accetta connessioni cifrate mediante SSL 2.0 e/o SSL 3.0. Queste versioni di SSL hanno numerose criticità, ad esempio:

- Uno schema di padding insicuro con gli algoritmi di cifratura CBC;
- Schemi di rinegoziazione dei parametri insicuri.

Un attaccante può sfruttare queste vulnerabilità per compiere attacchi man-in-the-middle o per decrittare le comunicazioni tra server e client.

Anche se SSL/TLS possiede strumenti efficaci per scegliere la più recente versione supportata del protocollo (facendo sì che tali versioni obsolete vengano scelte solo quando client o server non ne supportano altre), molti browser implementano tale meccanismo in maniera non sicura permettendo all'attaccante di effettuare un "downgrade" della connessione (come accade nell' attacco POODLE). Perciò si raccomanda di disabilitare del tutto tali protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per effettuare comunicazioni sicure. A partire dalla data stabilita dallo standard PCI DSS v3.1, qualsiasi versione di SSL non corrisponderà alla definizione, data dal PCI SSC, di 'crittografia forte'.

Soluzione:

Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e SSL 3.0. Utilizza TLS 1.1 (con suite di cifratura approvate) o una versione più recente.

Asset: 4*****.***1

Severity: LOW

Date: 2017-11-22 06:49:32 UTC

Port: 443

IP: 4*****.***1

CVSS score: 2.6

CVSS vector: CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N

SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

L'host supporta le suite di cifratura EXPORT_DHE con chiavi di lunghezza inferiore a 512 bit. Tramite crittoanalisi, una terza parte può indovinare la chiave condivisa in un breve lasso di tempo.

Un attaccante, tramite attacco man-in-the-middle potrebbe effettuare il downgrade della sessione forzando l'utilizzo di suite EXPORT_DHE. Perciò, si raccomanda di disabilitare il supporto di suite di cifratura deboli.

Soluzione:

Riconfigura il servizio rimuovendo il supporto per le suite di cifratura EXPORT_DHE.

2.4 HOST 4****8****5

Su questo host è stata rilevata una vulnerabilità.

Asset: 4****8****5

Severity: HIGH

Date: 2018-03-14 07:23:49 UTC

Port: 23

IP: 4****8****5

Insecure protocols/services

Sull'host remoto è stato individuato un protocollo insicuro. Questo servizio potrebbe essere facilmente violato da un attaccante perché obsoleto e/o espone traffico di rete in chiaro, compromettendone confidenzialità ed integrità.

Soluzione:

Chiudi le ACL del firewall o disabilita i servizi non necessari.

2.5 HOST 8*****1*****0

Sono state rilevate 2 vulnerabilità su questo host.

Asset: 8*****1*****0

Severity: MEDIUM

Date: 2018-03-14 07:23:49 UTC

Port: 20000

IP: 8*****1*****0

Insecure protocols/services

Sull'host remoto è stato individuato un protocollo insicuro. Questo servizio potrebbe essere facilmente violato da un attaccante perché obsoleto e/o espone traffico di rete in chiaro, compromettendone confidenzialità ed integrità.

Soluzione:

Chiudi le ACL del firewall o disabilita i servizi non necessari.

Asset: 8*****1*****0

Severity: MEDIUM

Date: 2018-03-14 07:23:49 UTC

Port: 20000

IP: 8*****1*****0

Insecure SCADA devices

Sull'host remoto è stato individuato un dispositivo SCADA. Esso di solito gestisce parametri critici (come dati provenienti dai sensori) che potrebbero essere controllati e manipolati da remoto (ad esempio aprendo una valvola)

Soluzione:

Disabilita l'accesso da remoto a questo dispositivo e, se possibile, spostalo dalla perimetro internet pubblico dell'azienda.