Manuale

REPORT SERVIZIO STC

Sommario

Gentile Cliente,
Il presente è un manuale per supportare la lettura del Report Mensile STC in cui troverà l'analisi dei flussi di rete gestiti dal servizio.
Il Report fornisce un'analisi di dettaglio per comprendere l'utilizzo della rete, e lo stato della sicurezza applicata ai flussi in gestione del servizio STC.
In particolare, sono presenti i grafici di analisi e i dettagli, fino a 50 oggetti per tipologia, per: flussi generati, applicazioni, attività web, filtraggio web, utilizzo VPN, tentativi di intrusione, botnet, virus e spyware, attacchi per il periodo precedente del servizio.

Per ulteriori informazioni non esiti a contattare il supporto STC.

1 Report Mensile

I primi giorni di ogni mese il servizio invia il report mensile all'indirizzo mail del referente tecnico del cliente. La mail ha in allegato il report PDF in formato compresso ZIP.
Il report, nella versione attuale in lingua inglese, è organizzato in capitoli: ogni capitolo è un'analisi specifica composta da un grafico e una vista tabellare che esplode i singoli elementi di analisi.
Una tipologia di analisi nel report potrà essere vuota nel caso in cui non siano disponibili dati sull'analisi, ad esempio i virus intercettati dal servizio potrà essere vuota perché non sono stati rilevati virus nel periodo o per configurazione del servizio nel caso in cui si sia deciso di non analizzare la presenza di virus nei flussi di rete.

2 Analisi presenti nel report

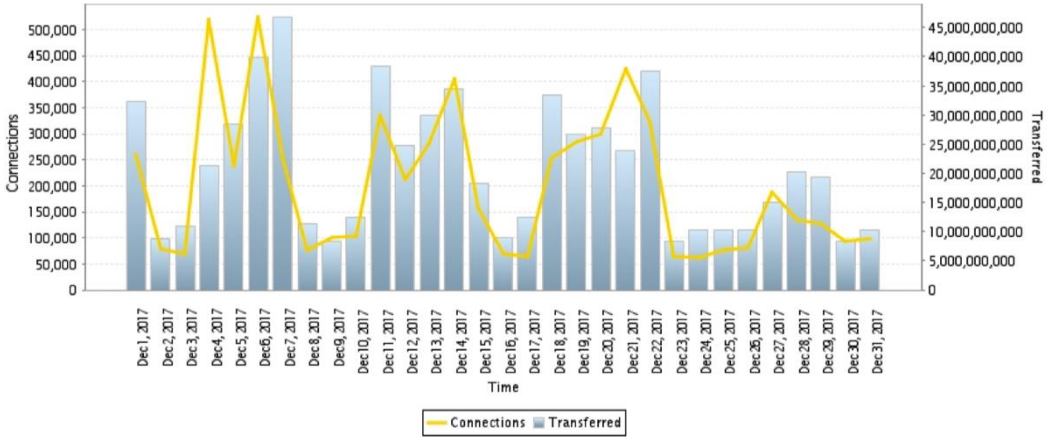
Il report si sviluppa nelle seguenti analisi divise in macro tipologie:

- Utilizzo della rete: Data Usage
- Applicazioni in uso: Applications
- Attività di Navigazione: Web
- Attività VPN: VPN
- Protezione intrusion: Intrusions
- Botnet: Protezione botnet
- Gateway Antivirus: Protezione Antivirus
- Spyware
- Attacks

Per ogni tipologia sono prodotte più analisi che si possono riassumere in tre tipi.

2.1 Informazioni nel periodo

È la rappresentazione grafica e tabellare delle informazioni nel periodo di esame (tipicamente un mese) divise per giorno, come il traffico e le connessioni nel mese.
Esempio:



Elemento di attenzione:

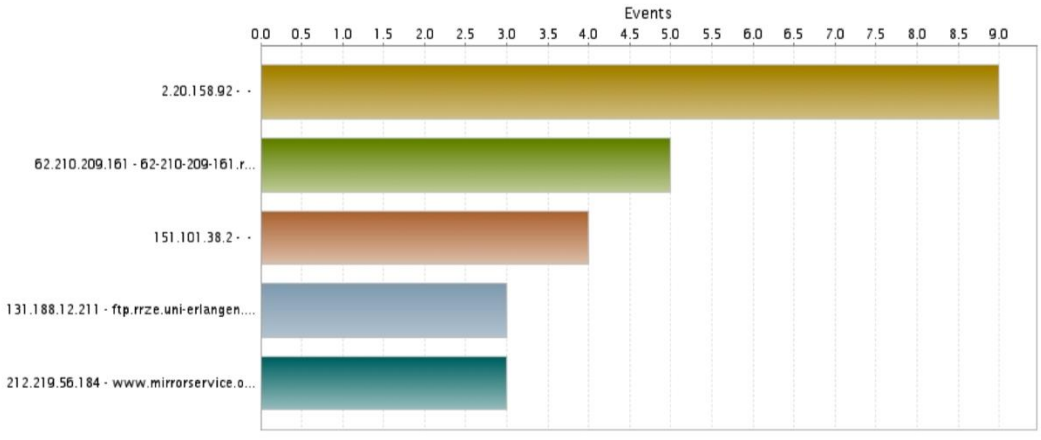
L'utilità principale è verificare l'eventuale presenza di anomalie degli andamenti temporali dell'oggetto di analisi. Eventuali anomalie come picchi o concentrazioni possono essere lecite o sintomo di attività anomale.

2.2 Principali sorgenti/destinazioni/oggetti

Sono le analisi che estraggono i principali o più frequenti eventi della categoria per:

- Sorgente: solitamente chi ha iniziato la connessione o il flusso di rete
- Destinazione: a cui era indirizzato il flusso o la connessione
- Oggetti: per singoli oggetti come categorie fi filtraggio della navigazione.

Esempio:



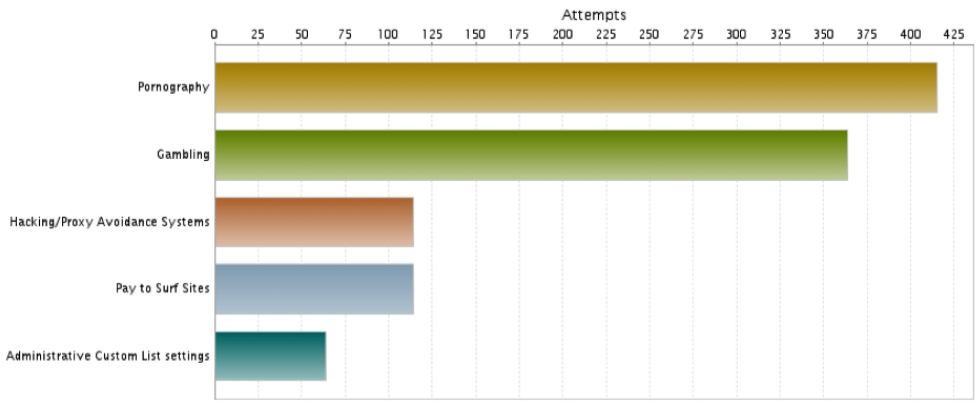
Elemento di attenzione:

Essendo un report dei principali o più frequenti oggetti è utile per comprendere la distribuzione e tipologia di eventi. Nel caso di sorgenti/destinazione è invece estremamente utile per analizzare e individuare puntualmente cosa è avvenuto e chi è stato coinvolto.

2.3 Relazione tra oggetti

È una tipologia di analisi in cui sono messi relazione eventi e oggetti, come le singole categorie dei filtri di navigazione e gli Ip delle postazioni.

Esempio:



	Category			Attempts
1	Pornography			415
	Initiator IP	Initiator Host	User	Attempts
a	192.168.102.103			282
b	192.168.102.68			22
c	216.58.198.46	mil04s04-in-f14.1e100.net		18
d	192.168.120.102			18
e	192.168.120.102	.		16

Elemento di attenzione:

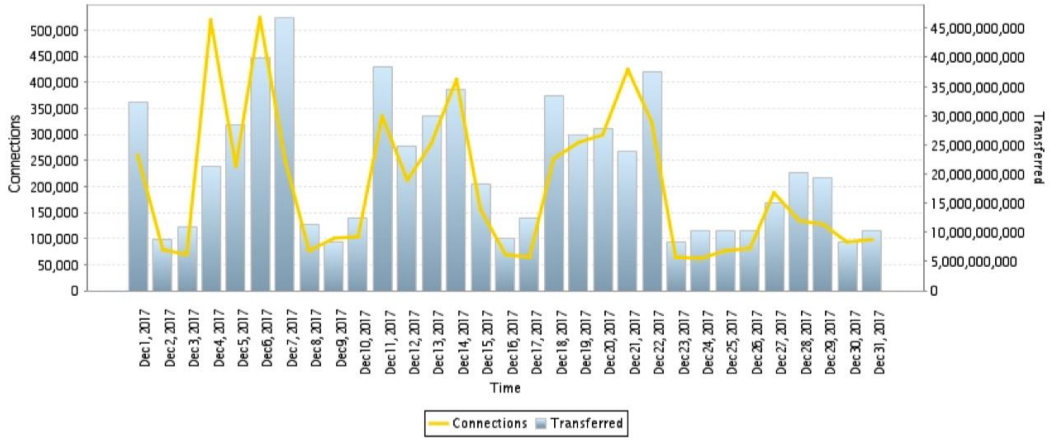
E' principalmente una analisi informativa di relazione tra oggetti, utile per comprendere la distribuzione delle attività e definite eventuali azioni correttive.

3 Esplosione report

Di seguito sono esplosi i singoli moduli del report, corredati da un esempio, e con indicazioni utili su come leggerete le informazioni.

3.1 Data Usage – Timeline: Utilizzo della rete nel periodo

Data Usage - Timeline



	Time	Connections	Transferred	Cost
1	Dec 1, 2017	259,068	30.17 GB	USD 308.94
2	Dec 2, 2017	77,540	8.17 GB	USD 83.67
3	Dec 3, 2017	68,354	10.14 GB	USD 103.80

Presenta per ogni giorno il numero di connessioni, il traffico generato, in formato grafico e tabellare con i relativi totali alla fine.

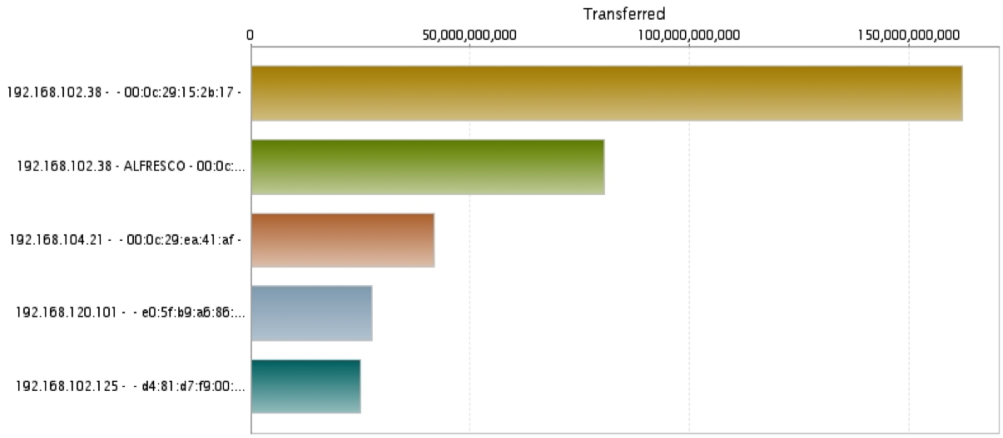
Elementi di attenzione:

Verificare se gli andamenti sono costanti.

Tipicamente avremo un andamento simile del numero di connessioni e del traffico durante il periodo, con un numero maggiore di connessioni e traffico nei giorni lavorativi. Un anomalo numero di connessioni in assenza di traffico importante potrebbe essere ad esempio sintomo di attività anomale di una postazione. Le analisi successive possono fornire ulteriori informazioni utili.

3.2 Data Usage - Top Initiators: Oggetti che hanno utilizzato più la rete

Data Usage - Top Initiators



	Initiator IP	Initiator Host	Initiator MAC	User	Connections	Transferred
1	192.168.102.38		00:0c:29:15:2b:17		6,129	151.1 GB
2	192.168.102.38	ALFRESCO	00:0c:29:15:2b:17		1,843	75.15 GB
3	192.168.104.21		00:0c:29:ea:41:af		61,615	39.04 GB

Presenta gli oggetti di rete (IP) che hanno generato più traffico nel periodo.

La tabella presenta:

- IP: identificativo di rete
- Nome Host (nome del server o del client) se disponibile
- Mac Address: identifica fisicamente la scheda di rete
- Utente: solitamente vuoto
- Numero di connessioni
- Traffico sviluppato

Elementi di attenzione:

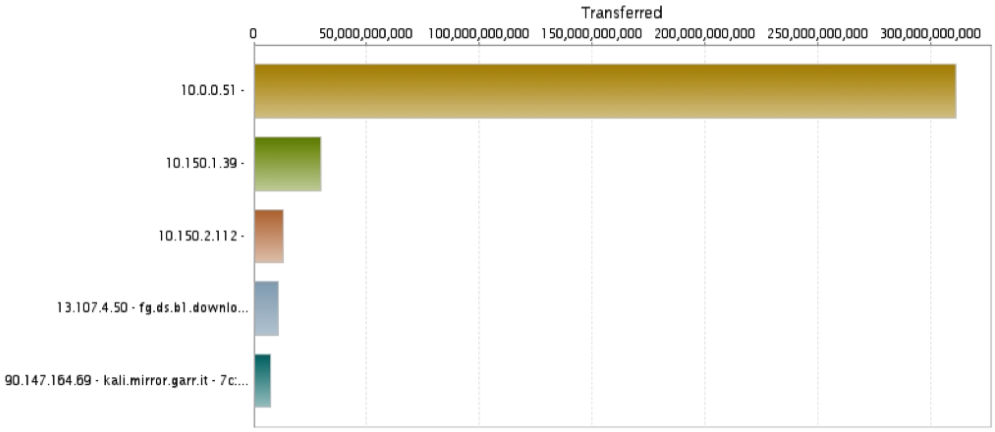
L'analisi è utile per individuare quali oggetti nella rete generano più traffico e permettere di valutare se è atteso o meno.

Se un IP che dovrebbe corrispondere ad un server interno, ad esempio il domain controller, genera molto traffico inatteso potrebbe essere compromesso e svolgere attività non note.

Dell'immagine sopra riportata, ad esempio, l'IP che genera maggiore traffico è un server Documentale aziendale, lo stesso è riportato due volte perché genera traffico verso diverse reti (lan, internet, backup).

3.3 Data Usage - Top Responders: Verso chi è generato il traffico

Data Usage - Top Responders



	Responder IP	Responder Host	Responder MAC	Connections	Transferred
1	10.0.0.51			1,742	289.26 GB
2	10.150.1.39			114	27.71 GB
3	10.150.2.112			43,994	12.22 GB
4	13.107.4.50	fg.ds.b1.download.windowsupdate.com	7c:ad:74:be:72:a8	4	10.14 GB

È l'analisi complementare alla precedente, ci permette di comprendere verso chi la nostra rete genera traffico.

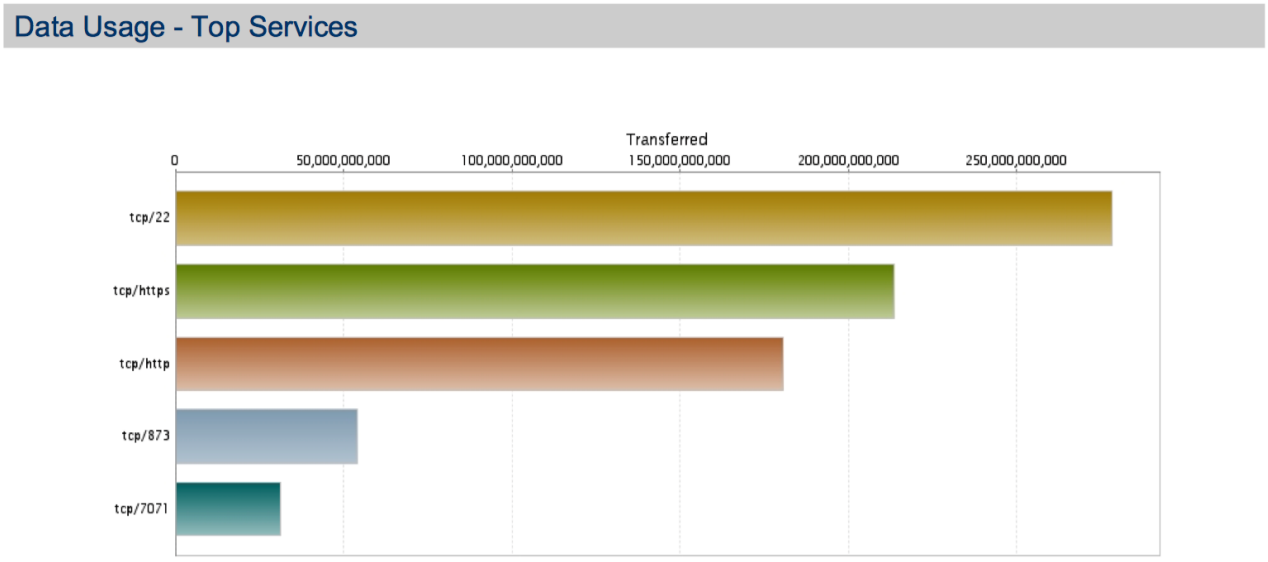
La tabella presenta:

- IP: identificativo verso chi è generato il traffico
- Nome Host (nome del server o del client) se disponibile
- Mac Address: identifica fisicamente la scheda di rete
- Numero di connessioni
- Traffico sviluppato

Elementi di attenzione:

L'analisi è utile per individuare verso quali oggetti la rete ha generano più traffico e permettere di valutare se è atteso o meno, e intraprendere delle azioni correttive. Verificare se gli Ip verso cui è generato il traffico sono noti o meno, in relazione con il nome host. Ad esempio, un flusso anomalo potrebbe essere indice di un uso non conforme della rete aziendale (ad esempio download di software per uso personale). Dell'immagine sopra riportata, ad esempio, l'ip verso cui è generato il maggiore traffico è una rete esterna verso cui sono traferiti i backup della lan, quindi è traffico coretto e atteso.

3.4 Data Usage - Top Services: i servizi che hanno generato più traffico



	Service	Connections	Transferred
1	tcp/22	194,371	259.36 GB
2	tcp/https	2,950,705	199.04 GB
3	tcp/http	1,292,132	168.19 GB

Permette di comprendere con che protocolli la nostra rete genera traffico.

La tabella presenta:

- Servizio: tcp/udp e protocollo o porta
- Numero di connessioni
- Traffico sviluppato

Elementi di attenzione:

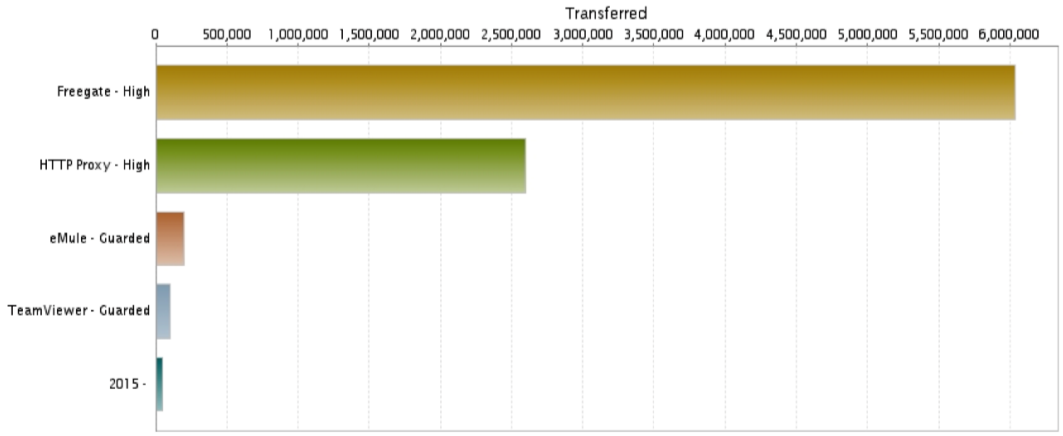
L'analisi è utile per individuare con quali serivizi la rete ha generano più traffico e permettere di valutare se è atteso o meno, e intraprendere delle azioni correttive.

Ad esempio, un protocollo anomalo potrebbe essere indice di un uso non conforme della rete aziendale (importante traffico ftp non atteso).

Dell'immagine sopra riportata, ad esempio il protocollo/porta che genera più traffico verso l'esterno è "tcp/22", che potrebbe essere anomalo, non essendo di uso comune, ma nel caso specifico si è verificato che la rete invia i backup locali nel Cloud usando appunto il protocollo tcp in porta 22.

3.5 Applications - Data Usage: Applicazioni per utilizzo di rete

Applications - Data Usage



	Application	Threat Level	Connections	Transferred
1	Freegate	High	44	5.75 MB
2	HTTP Proxy	High	3,012	2.48 MB
3	eMule	Guarded	27	197.09 KB
4	TeamViewer	Guarded	73	103.63 KB

Permette di individuare quali applicazioni (locali o servizi internet) nostra rete ha maggiormente generato traffico.

La tabella presenta:

- Applicazione/Servizio
- Livello di pericolosità
- Numero di connessioni
- Traffico sviluppato

Elementi di attenzione:

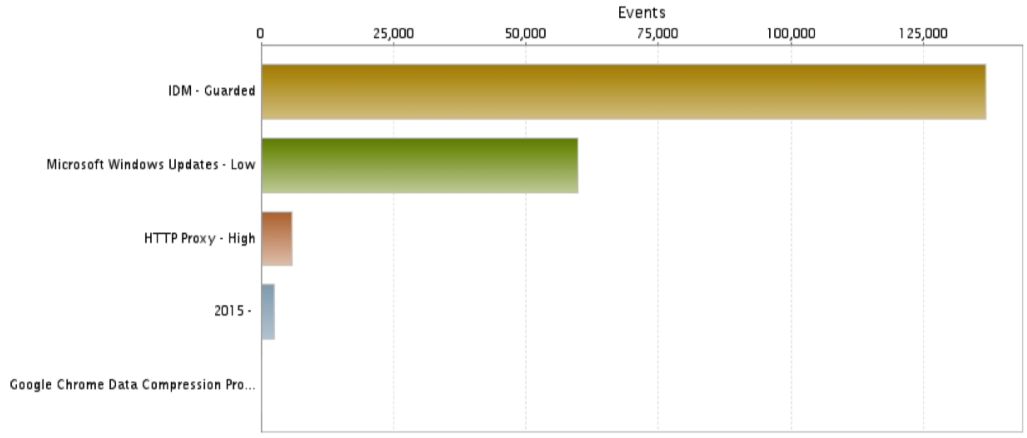
L'analisi è utile per individuare con quali applicazioni la rete ha generano più traffico e permettere di valutare se è atteso o meno, e intraprendere delle azioni correttive.

Un'applicazione anomala potrebbe essere indice di un uso non conforme della rete aziendale, ad esempio download illegale di file.

Dell'immagine sopra riportata, ad esempio, è presente un traffico anomalo con "Freegate" e "Http Proxy", questo rappresenta il tentativo si usare applicazioni o servizi di navigazione anonima esterna o più probabilmente di tentare di aggirare i blocchi della navigazione aziendale.

3.6 Applications - Top Applications Detected: applicazioni più rilevate

Applications - Top Applications Detected



	Application	Threat Level	Events
1	IDM	Guarded	136,776
2	Microsoft Windows Updates	Low	59,818
3	HTTP Proxy	High	5,918

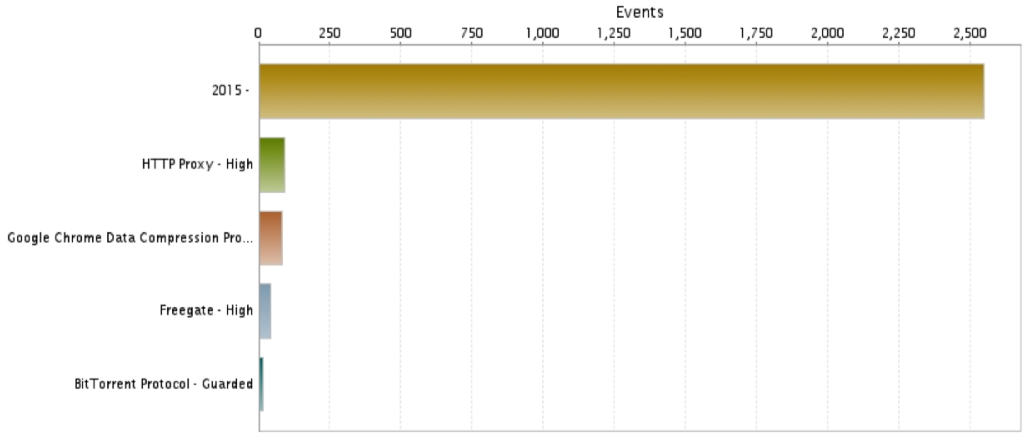
Simile al precedente, ci elenca le applicazioni che sono state per numero più individuate a prescindere dal traffico sviluppato.
La tabella presenta:

- Applicazione/Servizio
- Livello di pericolosità
- Numero volte che stata rilevata

Elementi di attenzione:
L'analisi è utile per individuare quali applicazioni sono in uso nella rete, permettendo di valutare la loro validità a fini aziendali.
Un'applicazione anomala potrebbe essere indice di un uso non conforme della rete aziendale, ad esempio download illegale di file.
Dell'immagine sopra riportata, ad esempio, è presente un elevato uso di "IDM" Internet Download Manager, posso valutare se corretto o meno ed eventualmente richiedere un blocco dell'applicazione.

3.7 Applications - Top Applications Blocked: Applicazioni più bloccate

Applications - Top Applications Blocked



	Application	Threat Level	Events
1	2015		2,551
2	HTTP Proxy	High	90
3	Google Chrome Data Compression Proxy	Low	84

Elenca le applicazioni che sono state per numero più individuate a prescindere dal traffico sviluppato.

La tabella presenta:

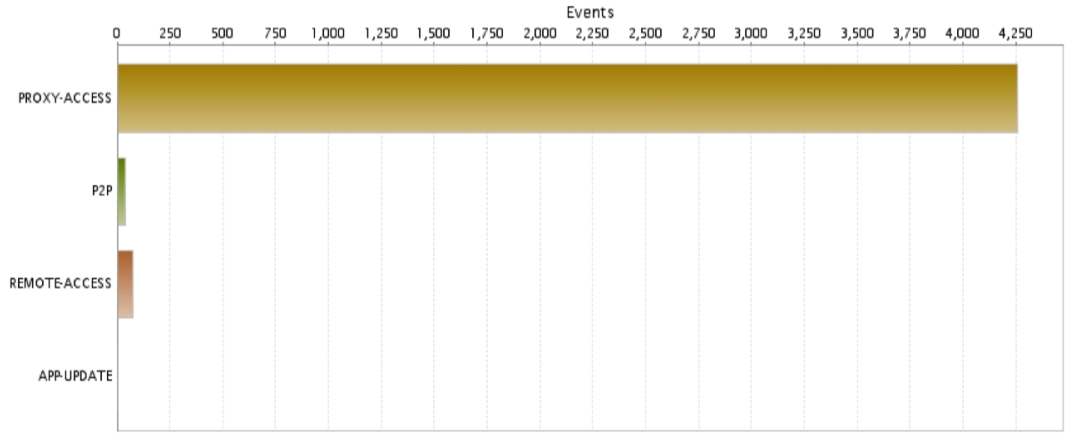
- Applicazione/Servizio
- Livello di pericolosità
- Numero volte che stata bloccata

Elementi di attenzione:

E' sicuramente un analisi informativa, che ci da un idea di cosa il servizio sta bloccando, permettendo di adottare politiche specifiche ad esempio di sensibilizzazione verso i propri utenti o bonifica di software non lecito.

3.8 Applications - Top Categories: Categoria applicazioni per traffico

Applications - Top Categories



	Application Category	Events	Transferred
1	PROXY-ACCESS	4,258	8.32 MB
2	P2P	39	201.62 KB
3	REMOTE-ACCESS	73	103.63 KB

Permette di vedere le categorie di applicazioni (locali o servizi internet) che nella nostra rete hanno maggiormente generato traffico.

La tabella presenta:

- Applicazione/Servizio
- Numero di volte che sono state individuate
- Traffico sviluppato

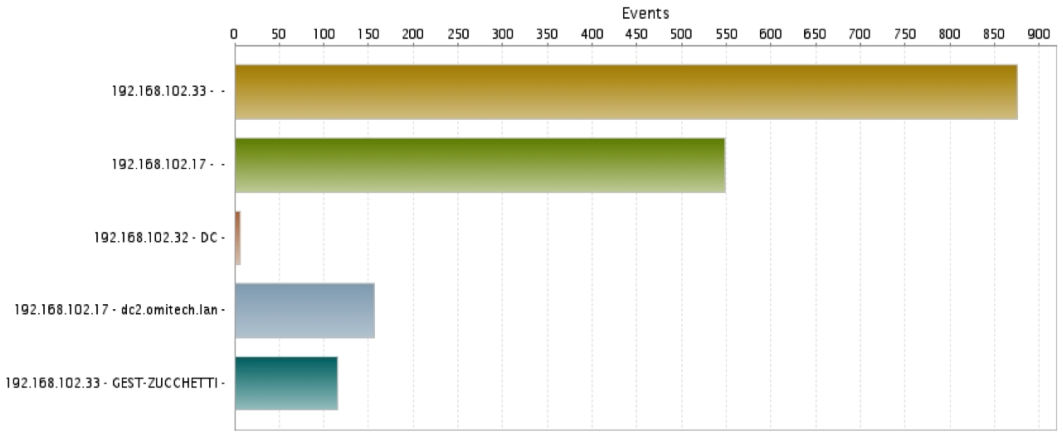
Elementi di attenzione:

La visione aggregata per categoria permette un migliore comprensione della tipologia di applicazioni individuate.

Nel esempio l'uso di proxy è l'aggregazione di quanto riportato nelle applicazioni per traffico.

3.9 Applications - Top Initiators: Applicazioni per IP sorgenti

Applications - Top Initiators



	Initiator IP	Initiator Host	User	Events	Transferred
1	192.168.102.33			875	1.54 MB
2	192.168.102.17			548	1.42 MB

Ci elenca gli oggetti di rete che più hanno utilizzato applicazioni rilevate nelle precedenti analisi.

La tabella presenta:

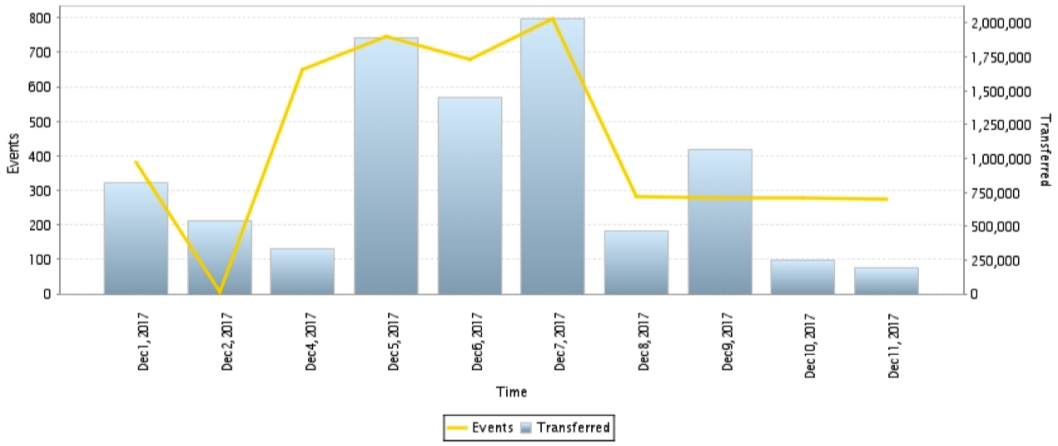
- IP: identificativo di rete
- Nome Host (nome del server o del client) se disponibile
- Utente: solitamente vuoto
- Numero di eventi
- Traffico sviluppato

Elementi di attenzione:

Anche per questa analisi è utile per verificare la presenza di attività attese o meno per poter perdere delle contro misure. Ad esempio, una elevata attività da parte dell'IP di un server che per funzione non dovrebbe dialogare con Internet potrebbe essere sintomo di un uso non lecito, o la presenza si software non corretto sullo stesso server.

3.10 Applications - Timeline: Numero di applicazioni rilevate nel tempo

Applications - Timeline



	Time	Events	Transferred
1	Dec 1, 2017	382	800.18 KB
2	Dec 2, 2017	6	529.01 KB
3	Dec 4, 2017	651	327.07 KB

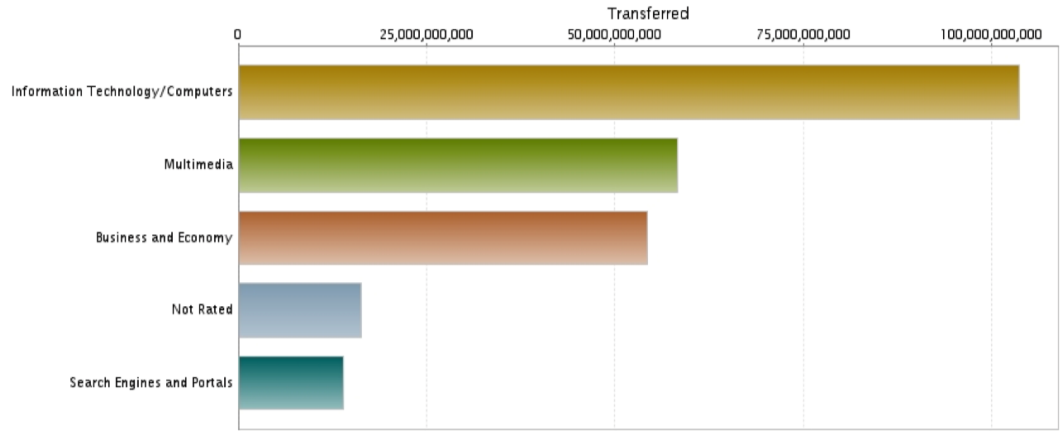
Presenta per ogni giorno il numero di eventi in cui è stata rilevata un'applicazione e il traffico generato.

Elementi di attenzione:

Come tutte le analisi sul periodo per valori aggregati ci servono per individuare gli andamenti ed eventuali anomalie, come alta attività in giornate non lavorative.

3.11 Web Activity - Top Categories: Navigazione per categorie

Web Activity - Top Categories



	Category	Browse Time	Hits	Transferred
1	Information Technology/Computers	226h 25m 01s	543,401	96.44 GB
2	Multimedia	20h 14m 31s	48,581	54.33 GB
3	Business and Economy	389h 20m 43s	934,429	50.57 GB

È analizzata l'attività di navigazione per categorie. La tabella presenta:

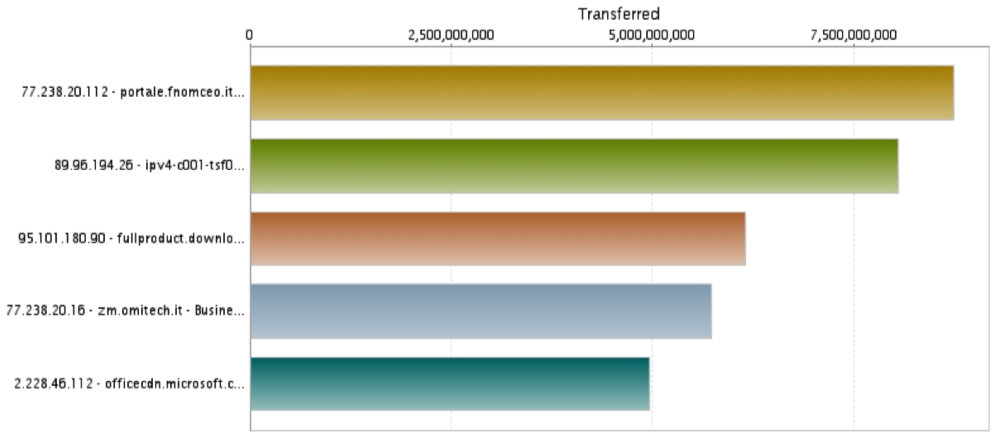
- Categoria
- Tempo di navigazione
- Numero di eventi
- Traffico sviluppato

Elementi di attenzione:

Ci permette di avere una visione generale del traffico di navigazione in termini di categorie, tempo e traffico. La relazione tra i valori permette di individuare quanto tempo e l'impatto in traffico, ad esempio, della navigazione nei social, o come nell'esempio sopra riportato in siti di distribuzione multimediale (video o musica). Permettendo di valutare il comportamento globale ed eventualmente intraprendere azioni correttive in termini di sensibilizzazione o blocco.

3.12 Web Activity - Top Sites: attività per singoli siti

Web Activity - Top Sites



	Site IP	Site Name	Category	Browse Time	Hits	Transferred
1	77.238.20.112	portale.fnomceo.it	Health	13h 15m 46s	31,831	8.14 GB
2	89.96.194.26	ipv4-c001-tsf001-fastweb-isp.1.oca.nflxvideo.net	Multimedia	00h 04m 34s	183	7.5 GB
3	95.101.180.90	fullproduct.download.microsoft.com	Information Technology/Computers	00h 00m 01s	1	5.73 GB

È analizzata l'attività di navigazione per singolo sito. La tabella presenta:

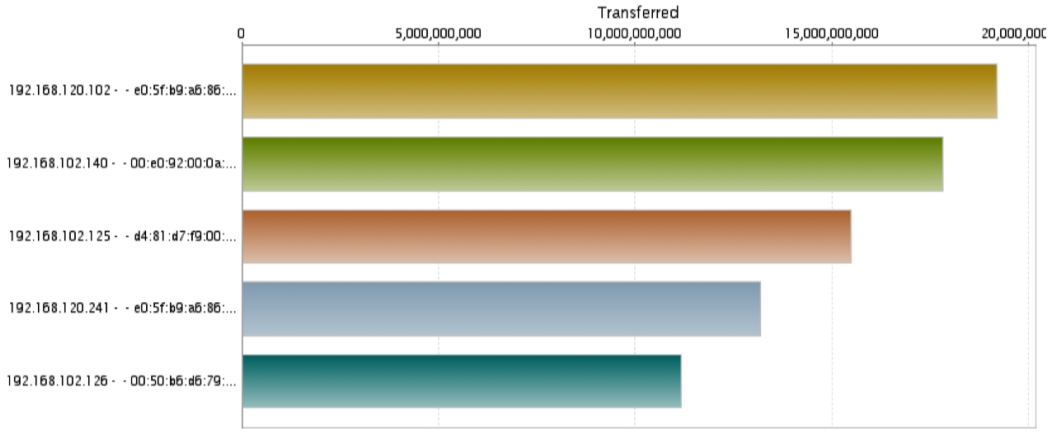
- IP sito
- Nome del sito
- Categoria
- Tempo di navigazione
- Numero di eventi
- Traffico sviluppato

Elementi di attenzione:

Ci permette di avere una visione più dettagliata della precedente del traffico di navigazione in termini di siti, tempo e traffico. Rispetto alla precedente è puntuale per individuare anomalie nell'uso della rete.

3.13 Web Activity - Top Initiators: Navigazione per Sorgente

Web Activity - Top Initiators



	Initiator IP	Initiator Host	Initiator MAC	User	Browse Time	Hits	Transferred
1	192.168.120.102		e0:5f:b9:a6:86:d6		42h 45m 36s	102,624	17.88 GB
2	192.168.102.140		00:e0:92:00:0a:d9		27h 02m 42s	64,908	16.58 GB
3	192.168.102.125		d4:81:d7:f9:00:12		18h 47m 22s	45,095	14.42 GB

È l'analisi complementare alla precedente, ci permette di comprendere cosa nella nostra rete genera traffico web.

La tabella presenta:

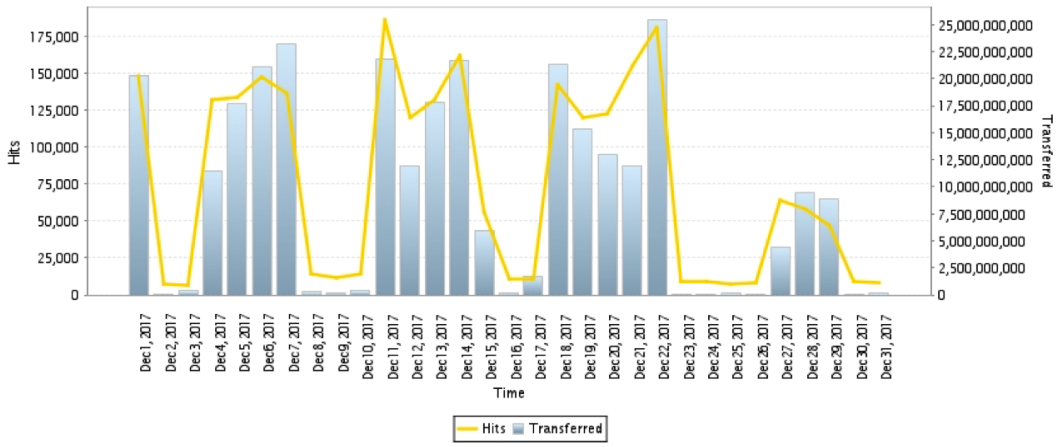
- IP: identificativo sorgente che ha generato il traffico
- Nome Host (nome del server o del client) se disponibile
- Mac Address: identifica fisicamente la scheda di rete
- Utente: solitamente vuoto
- Tempo di navigazione
- Numero di connessioni
- Traffico sviluppato

Elementi di attenzione:

L'analisi è utile per individuare singoli oggetti nella nostra rete che hanno generato il traffico web permettendo di individuare attività non attese.

3.14 Web Activity – Timeline: Navigazione nel tempo

Web Activity - Timeline



	Time	Browse Time	Hits	Transferred
1	Dec 1, 2017	61h 33m 43s	147,749	18.92 GB
2	Dec 2, 2017	03h 02m 42s	7,308	107.89 MB
3	Dec 3, 2017	02h 46m 49s	6,673	345.3 MB

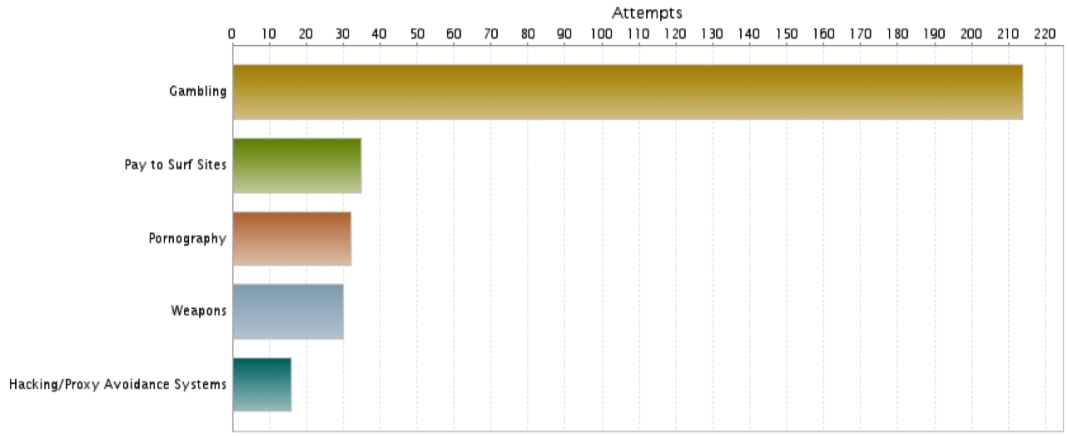
Presenta per ogni giorno il tempo di navigazione, il numero di eventi e traffico sviluppato dalla navigazione web.

Elementi di attenzione:

Come tutte le analisi sul periodo per valori aggregati ci servono per individuare gli andamenti ed eventuali anomalie, come alta attività in giornate non lavorative.

3.15 Web Filter - Top Categories: Filtro Navigazione per Categorie

Web Filter - Top Categories



	Category	Attempts
1	Gambling	214
2	Pay to Surf Sites	35
3	Pornography	32

Sono analizzati gli eventi n cui i filtro navigazione è intervenuto bloccando l'accesso al sito per categorie. La tabella presenta:

- Categoria
- Numero di eventi

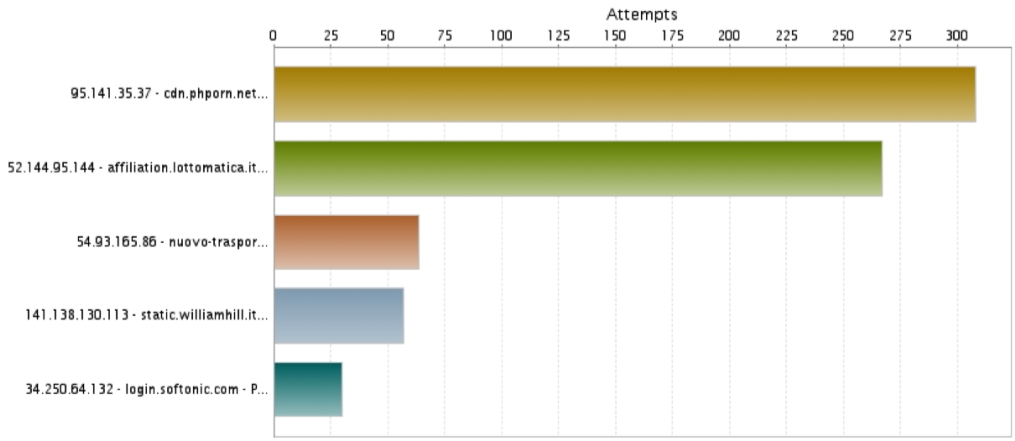
Elementi di attenzione:

Ci permette di avere una visione generale dell'efficacia dei filtri di navigazione in termini di categorie.

Permettendo di valutare il comportamento globale ed eventualmente intraprendere azioni correttive in termini di sensibilizzazione.

3.16 Web Filter - Top Sites: Filtro Navigazione per Sito

Web Filter - Top Sites



	Site IP	Site Name	Category	Attempts
1	95.141.35.37	cdn.phporn.net	Pornography	308
2	52.144.95.144	affiliation.lottomatica.it	Gambling	267
3	54.93.165.86	nuovo-trasporto-viaggiatori-s-p. dynatracesaas.com	Hacking/Proxy Avoidance Systems	64

È analizzata l'attività dei filtri di navigazione per singolo sito. La tabella presenta:

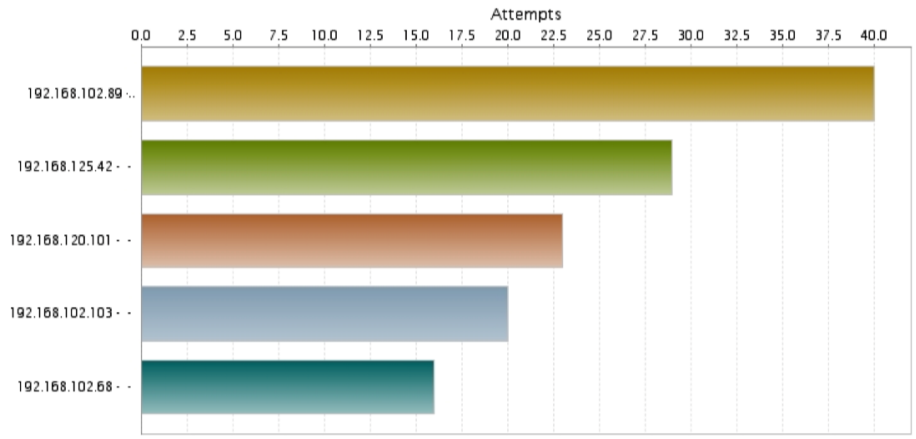
- IP sito
- Nome del sito
- Categoria
- Numero di eventi

Elementi di attenzione:

Ci permette di avere una visione più dettagliata della precedente dell'efficacia dei filtri di navigazione in termini di siti.

3.17 Web Filter - Top Initiators : Filtro Navigazione per Sorgente

Web Filter - Top Initiators



	Initiator IP	Initiator Host	User	Attempts
1	192.168.102.89			40
2	192.168.125.42			29
3	192.168.120.101			23

È analizzata l'attività dei filtri di navigazione per singolo sorgente. La tabella presenta:

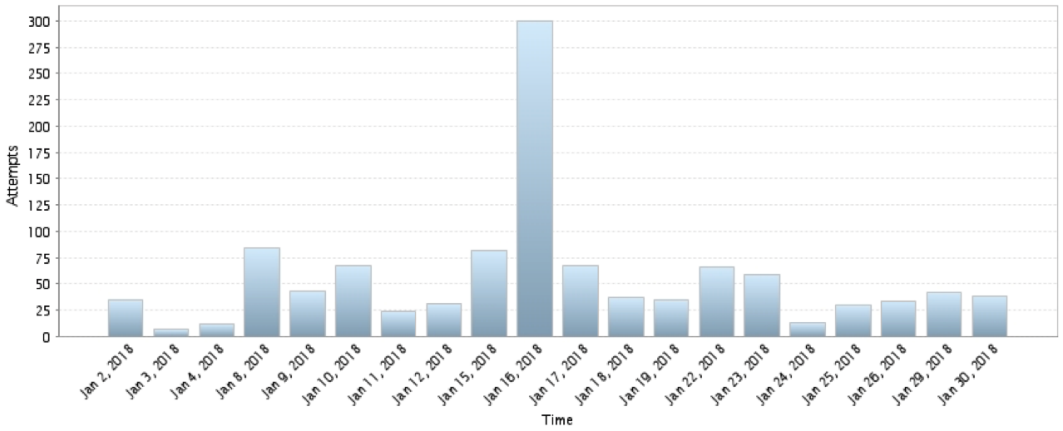
- IP sorgente
- Nome host (se disponibile)
- Utente: solitamente vuoto
- Numero di eventi

Elementi di attenzione:

Ci permette di avere una visione complementare alla della precedente dell'efficacia dei filtri di navigazione in termini di sorgenti, utili per individuare ad esempio software anomalo nelle postazioni. Spesso i tentativi di apertura di siti bloccati da policy aziendali possono essere fatti in modo inconsapevole dall'utente es per la presenza di software malevolo.

3.18 Web Filter – Timeline: Filtro Navigazione nel periodo

Web Filter - Timeline



	Time	Attempts
1	Jan 2, 2018	35
2	Jan 3, 2018	7
3	Jan 4, 2018	12

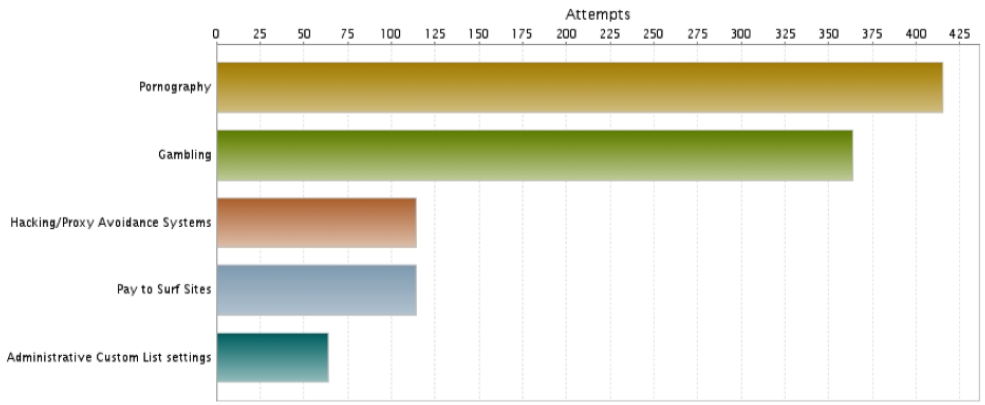
Presenta per ogni giorno il numero di tentativi di navigazione bloccati dai filtri.

Elementi di attenzione:

Come tutte le analisi sul periodo per valori aggregati ci servono per individuare gli andamenti ed eventuali anomalie, come alta attività in giornate non lavorative. Nell'esempio riportato il 16 gennaio c'è stato un anomalo intervento più di tre volte rispetto allo standard dell'attività di filtraggio. La ripetizione di anomalie potrebbe essere sintomo di postazioni compromesse.

3.19 Web Filter - Web Filter By Category: Filtraggio per categoria

Web Filter - Web Filter By Category



	Category			Attempts
1	Pornography			415
	Initiator IP	Initiator Host	User	Attempts
a	192.168.102.103			282
b	192.168.102.68			22
c	216.58.198.46	mil04s04-in-f14.1e100.net		18
d	192.168.120.102			18
e	192.168.120.102	.		16

Rispetto ai precedenti è un'analisi più dettagliata in cui sono esplose le categorie bloccate e gli oggetti che hanno generato il blocco, indicando:

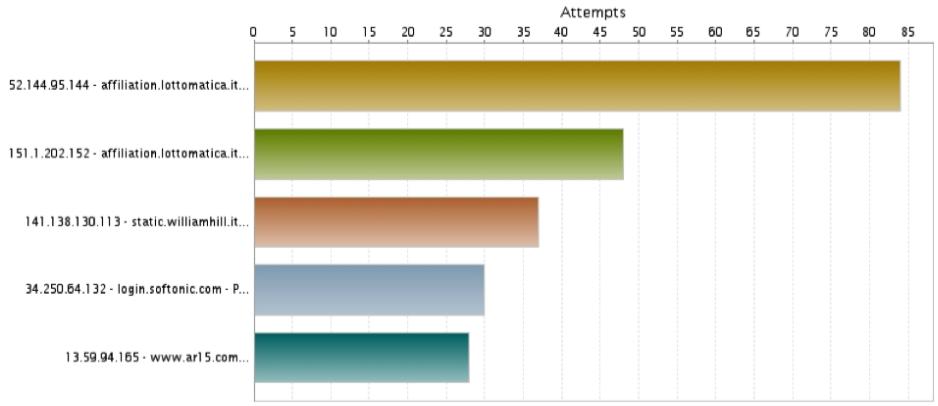
- Ip Sorgente
- Nome host: se disponibile
- Utente: solitamente vuoto
- Numero eventi

Elementi di attenzione:

L'analisi ci permette di avere una visione chiara e dettagliata dell'intervento dei filtri per individuare ad esempio gli oggetti di rete che ripetutamente incorrono nel blocco di navigazione. Un numero elevato e costante nel tempo di blocco per lo stesso oggetto è sintomo di una probabile presenza di software malevolo, spesso plugin o add on malevoli dei browser inavvertitamente installati.

3.20 Web Filter - Web Filter By Site: Filtro per siti

Web Filter - Web Filter By Site



	Site IP	Site Name	Category	Attempts
1	52.144.95.144	affiliation.lottomatica.it	Gambling	84
	Initiator IP	**Initiator Host**	**User**	**Attempts**
a	192.168.102.89			11
b	192.168.102.68			10
c	192.168.102.111			10
d	192.168.102.89			10
e	192.168.102.63			10

Rispetto ai precedenti è l'analisi ancora più dettagliata in cui sono esplosi i tentativi di accesso per singoli siti e gli oggetti che hanno generato il blocco, indicando:

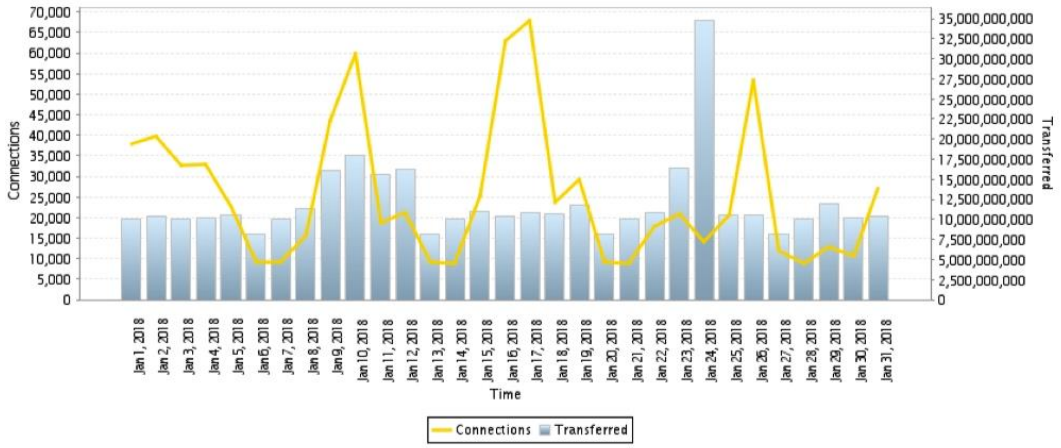
- Ip Sorgente
- Nome host: se disponibile
- Utente: solitamente vuoto
- Numero eventi

Elementi di attenzione:

L'analisi ci permette di avere altre indicazioni utili sui comportamenti di rete. I casi in cui abbiamo per singoli oggetti bloccati una distribuzione omogenea dei blocchi è probabile che sia generati in modo "normale", come l'inclusione da pagine lecite di immagini o altro da siti bloccati. Mentre singoli oggetti sorgenti/destinazione che generano un elevato numero di blocchi potrebbero evidenziare situaizoni anomale.

3.21 VPN Usage – Timeline: utilizzo VPN

VPN Usage - Timeline



	Time	Connections	Transferred
1	Jan 1, 2018	37,984	9.44 GB
2	Jan 2, 2018	39,747	9.63 GB
3	Jan 3, 2018	32,648	9.43 GB
4	Jan 4, 2018	33,091	9.55 GB

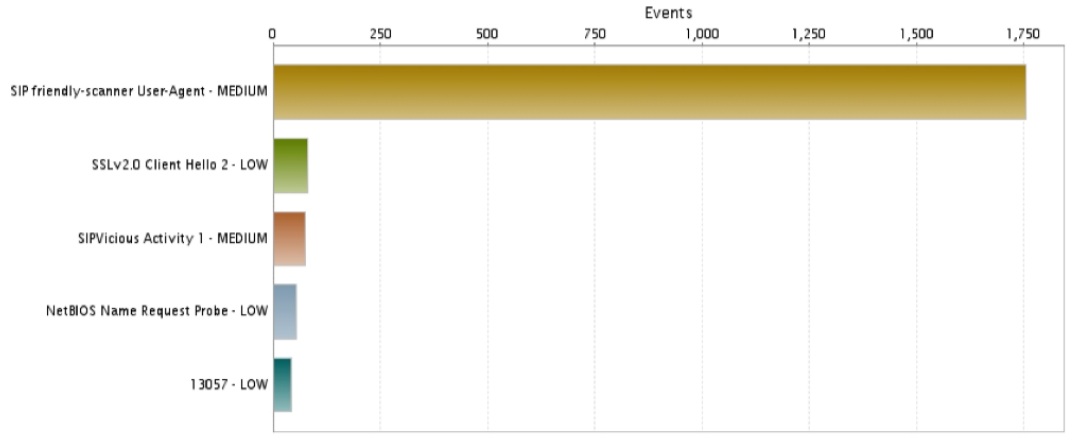
Presenta per ogni giorno il numero di connessioni generati nei flussi VPN e il relativo traffico.

Elementi di attenzione:

L'analisi permette di evidenziare i flussi VPN (tra reti o da client) e verificare la presenza di anomalie, come picchi particolarmente importanti di connessioni o traffico.
Nell'esempio soprariportato ad esempio il 24 gennaio.

3.22 Intrusions - Top Intrusions Detected: Protezione intrusioni

Intrusions - Top Intrusions Detected



	Intrusion	Priority Threat	Events
1	SIP friendly-scanner User-Agent	MEDIUM	1,755
2	SSLv2.0 Client Hello 2	LOW	81
3	SIPVicious Activity 1	MEDIUM	75

STC comprende anche un servizio per contrastare I tentativo di intrusione nella rete protetta, questo primo report evidenzia i tentativi registrati.
La tabella presenta:

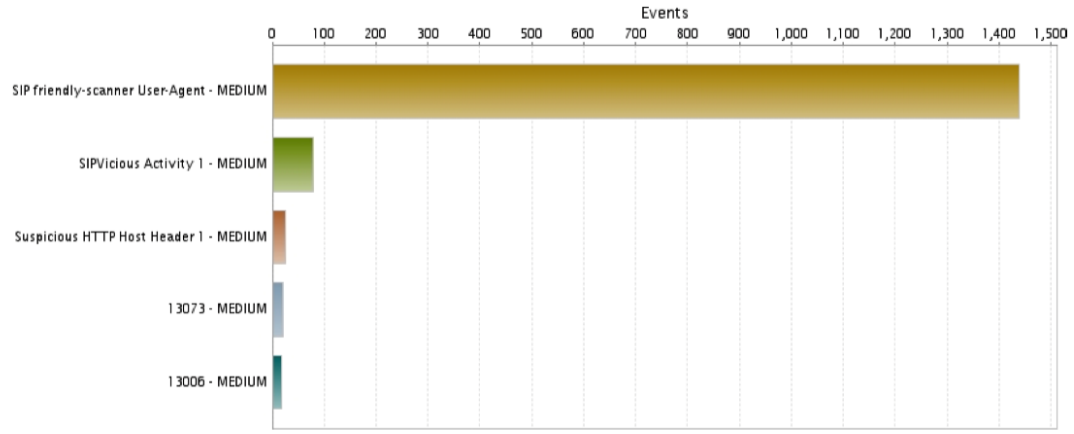
- Tipo di tentativo
- Criticità/Pericolosità
- Numero di eventi

Elementi di attenzione:

A meno di configurazioni particolarmente rilassate il servizio anti intrusione blocca i tentativi non autorizzati, rimane utile avere un'indicazione di che tipologia di attacchi sono in corso.
Nell'esempio riportato è sotto attacco il servizio SIP, se è presente una centrale telefonica SIP è utili verificare il livello di protezione.

3.23 Intrusions - Top Intrusions Blocked: Protezione intrusione Blocchi

Intrusions - Top Intrusions Blocked



	Intrusion	Priority Threat	Events
1	SIP friendly-scanner User-Agent	MEDIUM	1,439
2	SIPVicious Activity 1	MEDIUM	79
3	Suspicious HTTP Host Header 1	MEDIUM	25

Oltre a individuare i tentativi di intrusione il servizio è attivo nel blocco degli istessi.

La tabella presenta:

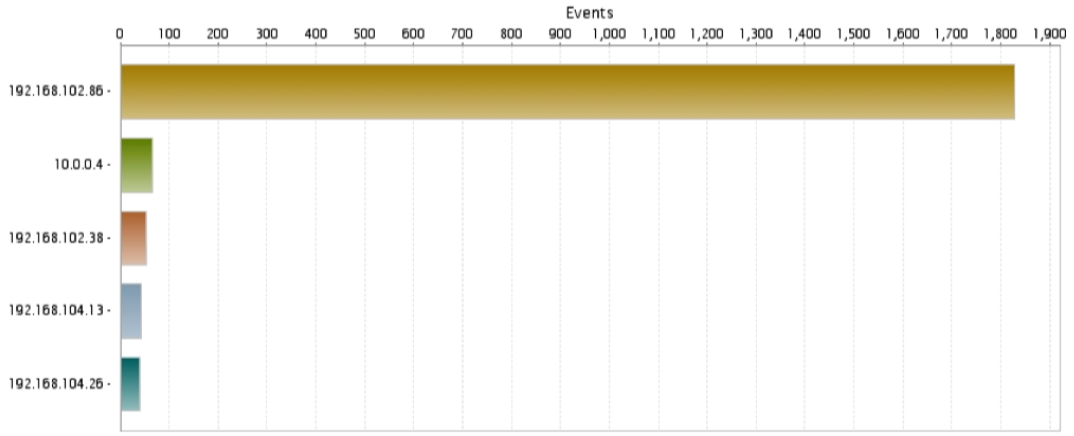
- Tipo di tentativo
- Criticità/Pericolosità
- Numero di eventi

Elementi di attenzione:

La corrispondenza tra i tentativi individuati e I blocchi indica una corretta configurazione della protezione.

3.24 Intrusions - Top Targets: Protezione intrusione target

Intrusions - Top Targets



	Target IP	Target Host	Events
1	192.168.102.86		1,829
2	10.0.0.4		65
3	192.168.102.38		52
4	192.168.104.13		42

Il report evidenzia verso quali oggetti delle reti protette sono stati fatti tentativi di intrusione. La tabella presenta:

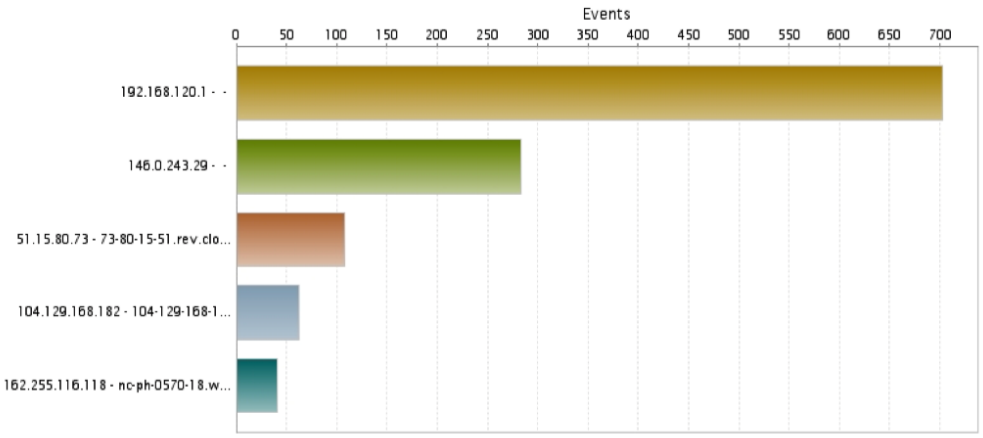
- IP taget
- Nome host (se disponibile)
- Numero di eventi

Elementi di attenzione:

Situazioni di picchi elevati verso un singolo target possono indicare un effettivo tentativo di attacco, o la presenza di software no aggiornato o con possibili falle di sicurezza.

3.25 Intrusions - Top Initiators: Protezione intrusione Sorgenti

Intrusions - Top Initiators



	Initiator IP	Initiator Host	User	Events
1	192.168.120.1			702
2	146.0.243.29			283
3	51.15.80.73	73-80-15-51.rev.cloud.scaleway.com		108
4	104.129.168.182	104-129-168-182.static.as40244.net		62

L'analisi delle sorgenti dei tendativi di intrusione presenta:

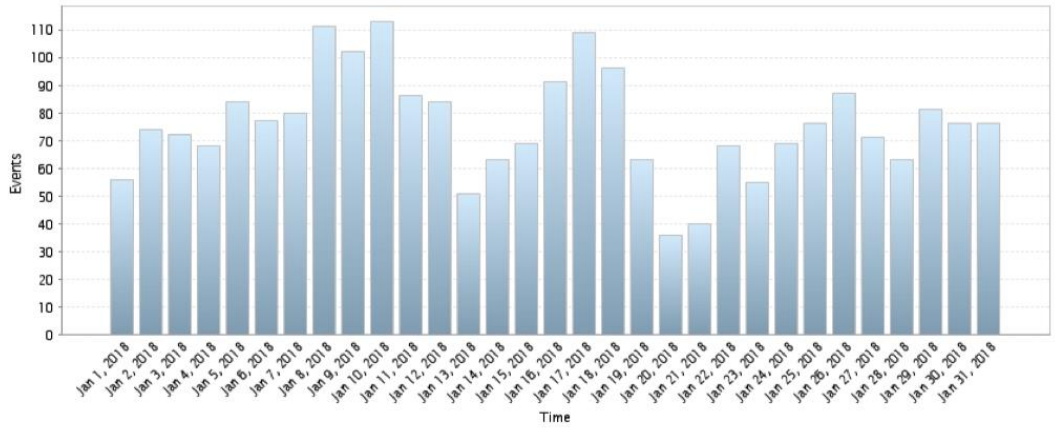
- IP sorgente
- Nome host (se disponibile)
- Numero di eventi

Elementi di attenzione:

I tentatici di intrusione solitamente dovrebbero avere come sorgente reti esterne, nel caso di IP associati a proprie reti, come nell'esempio riportato, è importante analizzare la sorgente. Se è una postazione o un server è possibile che le connessioni bloccate come intrusioni siano legittime (falso positivo) o siano reali e spesso generate sa software malevolo o oggetti compromessi.

3.26 Intrusions – Timeline: Protezione intrusione nel period

Intrusions - Timeline



	Time	Events
1	Jan 1, 2018	56
2	Jan 2, 2018	74
3	Jan 3, 2018	72
4	Jan 4, 2018	68
5	Jan 5, 2018	84

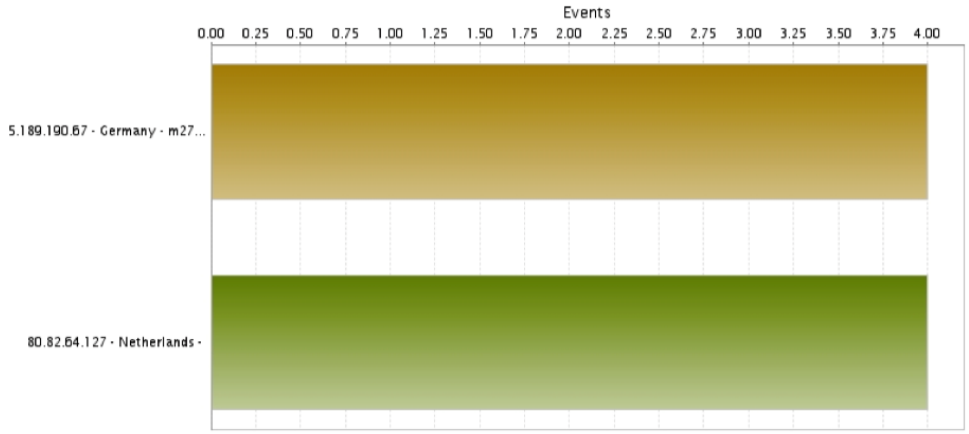
Presenta per ogni giorno il numero di connessioni individuate come tentativi di intrusione.

Elementi di attenzione:

L'analisi permette di evidenziare la presenza di anomalie, come picchi particolarmente importanti di connessioni potenzialmente pericolose.

Botnet – Initiators: Botnet Sorgenti

Botnet - Initiators



	Initiator IP	Initiator Country	Initiator Host	Events
1	5.189.190.67	Germany	m2767.contaboserver.net	11
2	5.189.190.67	Germany	m2767.contaboserver.net	4
3	80.82.64.127	Netherlands		4
	Total:			**19**

Una botnet è una rete controllata da un botmaster e composta da dispositivi infettati da malware specializzato, detti bot o zombie. STC controlla e analizza le connessioni per intercettare e bloccare il traffico individuato come botnet.
In questo caso sono elencati le sorgenti indivisuate:
La tabella presenta:

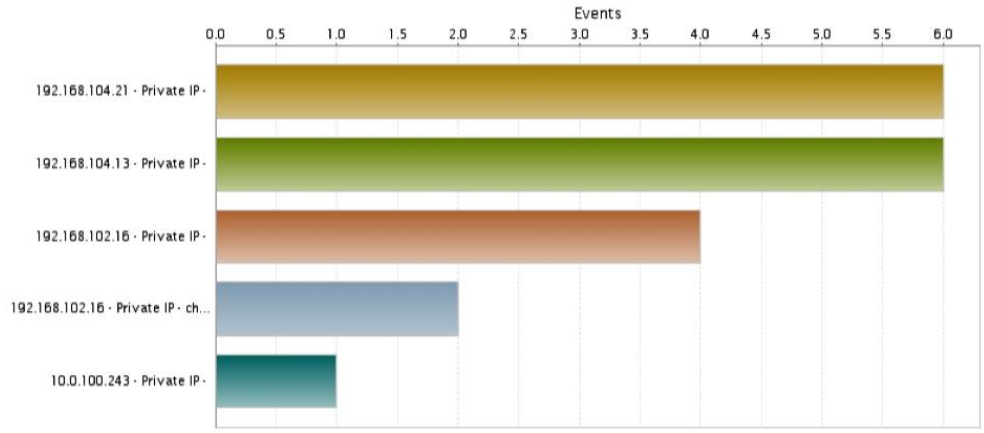
- IP sorgente
- Nome host (se disponibile)
- Numero di eventi

Elementi di attenzione:

Nella normalità dovrebbero essere pochi o nulli gli eventi individuati, in caso attività anomale è consigliata l'analisi dello stato della propria rete (ad esempio con scansioni antivirus).

3.27 Botnet – Responders: Botnet destinazioni

Botnet - Responders



	Target IP	Responder Country	Target Host	Events
1	192.168.104.21	Private IP		6
2	192.168.104.13	Private IP		6
3	192.168.102.16	Private IP		4
4	192.168.102.16	Private IP		2
5	10.0.100.243	Private IP		1
	Total:			**19**

L'analisi presenta gli oggetti verso cui le connessioni tracciate come possibile attività Botnet si sono svolte.

La tabella presenta:

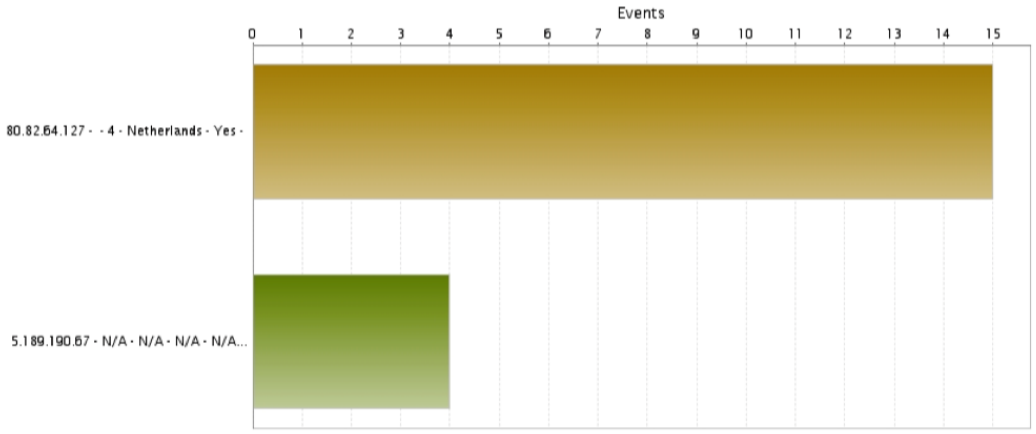
- IP destinazione
- Paese se disponibile
- Numero di eventi

Elementi di attenzione:

Quando sono presenti Ip della rete è utile verificare lo stato di protezione della postazione, in particolare come antivirus e della sua efficacia. Nei casi di persistenza in diversi report degli stessi IP è consigliata un'analisi degli stessi.

3.28 Botnet – Attacks: Botnet attività

Botnet - Attacks



	Botnet IP	Threat	Severity	Country	Active	URL	Events
1	80.82.64.127		4	Netherlands	Yes		15
2	5.189.190.67	N/A	N/A	N/A	N/A	N/A	4
	Total:						**19**

Gli attacchi possibili sono tracciati in questa analisi

La tabella presenta:

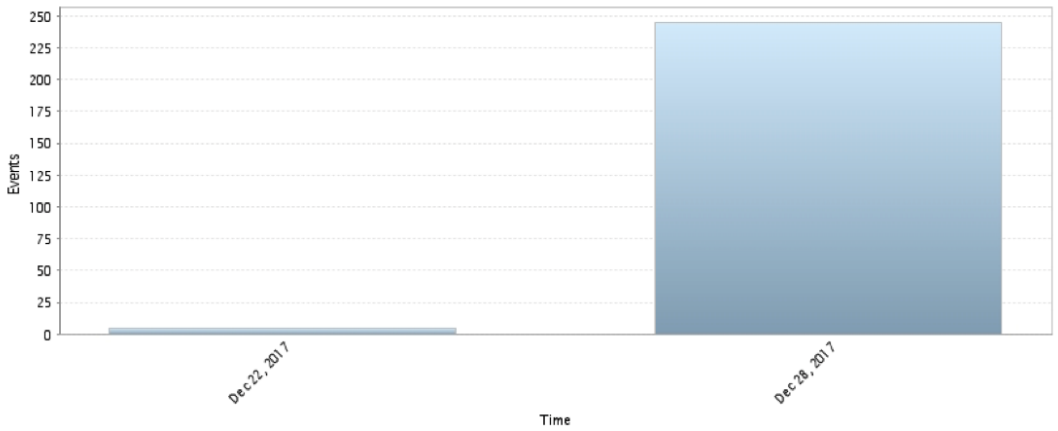
- IP Botnet
- Identificativo minaccia
- Livello di criticità
- Paese se disponibile
- STATO
- URL
- Numero di eventi

<u>Elementi di attenzione:</u>

Attacchi attivi richiedono una maggiore attenzione, richiedendo l'analisi dei target interni per verificarne lo stato.

3.29 Botnet – Timeline: Botnet attività nel tempo

Botnet - Timeline



	Time	Events
1	Dec 22, 2017	5
2	Dec 28, 2017	245
	Total:	**250**

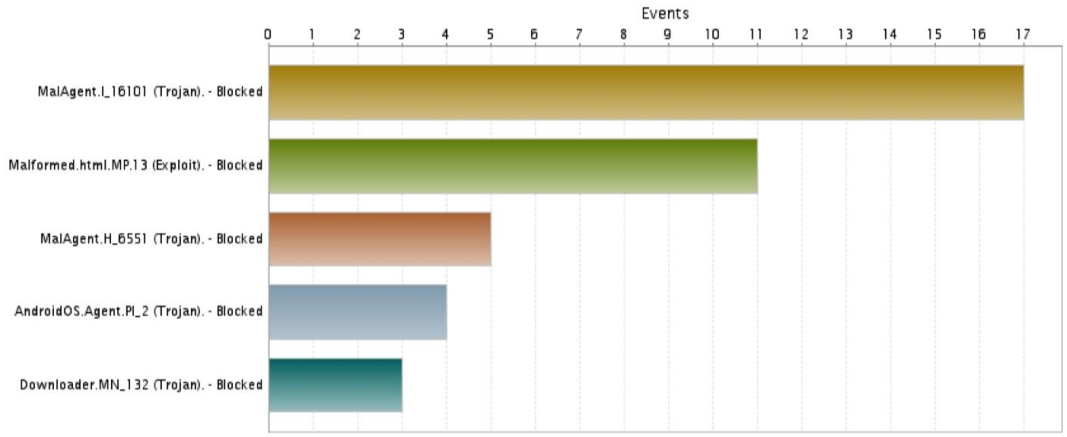
Il report evidenzia l'attività rilevata come botnet nel periodo di osservazione per numero di eventi.

Elementi di attenzione:

Solitamente avremo concentrazioni puntuali, indicando singoli attacchi o tentativi o anche di falsi postivi. In relazione con le altre analisi ci permette di avere il dettaglio dell'attività temporale, ad esempio tracciature costanti potrebbero indicare oggetti compromessi nella rete.

3.30 Gateway Viruses - Top Viruses Blocked: Virus più bloccati

Gateway Viruses - Top Viruses Blocked



	Virus	Action	Events
1	MalAgent.I_16101 (Trojan).	Blocked	17
2	Malformed.html.MP.13 (Exploit).	Blocked	11
3	MalAgent.H_6551 (Trojan).	Blocked	5
4	AndroidOS.Agent.PI_2 (Trojan).	Blocked	4
5	Downloader.MN_132 (Trojan).	Blocked	3
	Total:		**40**

Grazie ad STC i file in transito, ad esempio il download di un eseguibile o un archivio zip, sono scansionati alla ricerca di virus. Il report elenca i virus più frequentemente bloccati nei flussi di rete analizzati:

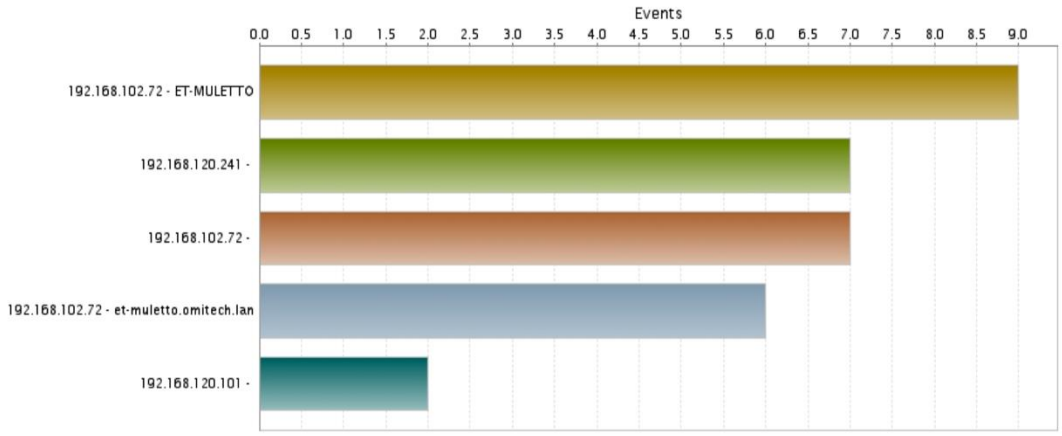
- Nome Virus individuato
- Azione intrapresa
- Numero di eventi

Elementi di attenzione:

Nel caso di un numero anomalo di eventi antivirus è consigliato verificare, grazie alle analisi successive, sorgenti e destinazioni dei file infetti. Un numero anomalo potrebbe nascere da ripetuti tentativi di scaricare un file compromesso, o nel caso di protezione STC applicata a porzioni di rete (come LAN e DMZ) o diverse sedi potrebbe essere in corso una diffusione nella rete di un virus.

3.31 Gateway Viruses - Top Targets: Antivirus principali Ip coinvolti

Gateway Viruses - Top Targets



	Target IP	Target Host	Events
1	192.168.102.72		9
2	192.168.120.241		7
3	192.168.102.72		7
4	192.168.102.72		6
5	192.168.120.101		2
	Total:		**31**

L'analisi elenca gli oggetti di rete verso cui più frequentemente era indirizzato il virus. Presentando:

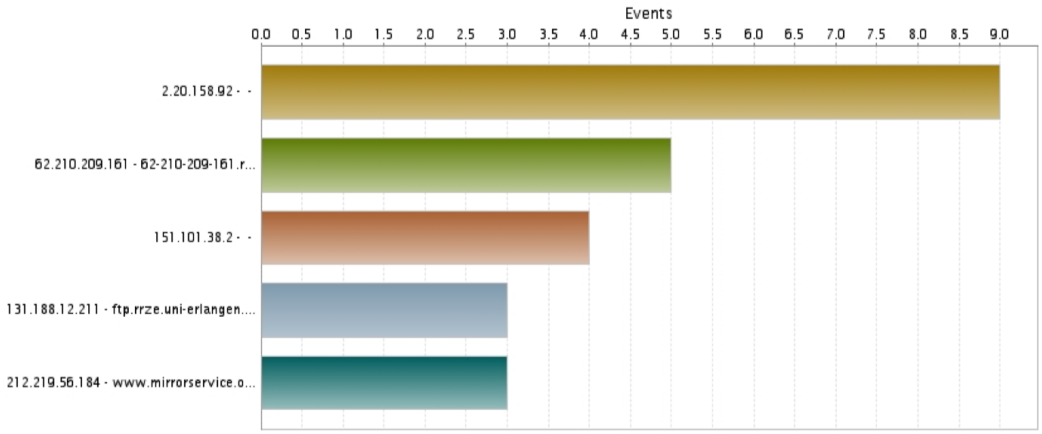
- IP indentificato
- Nome host (se disponibile)
- Numero di eventi

Elementi di attenzione:

Un numero elevato di eventi legati ad un singolo IP può avvenire quando un pc, ad esempio, ha cercato di scaricare diverse volte un file "virato". In questi casi è utile procedere con una scansione antivirus della postazione, il file bloccato potrebbe essere stato scaricato da altre reti o il numero elevato di eventi potrebbero essere il tentativo del virus di propagarsi nella rete interna.

3.32 Gateway Viruses - Top Initiators: Antivirus principali fonti

Gateway Viruses - Top Initiators



	Initiator IP	Initiator Host	User	Events
1	2.20.158.92			9
2	62.210.209.161	62-210-209-161.rev.poneytelecom.eu		5
3	151.101.38.2			4
4	131.188.12.211	ftp.rrze.uni-erlangen.de		3
5	212.219.56.184	www.mirrorservice.org		3
	Total:			**24**

L'analisi evidenzia le principali fonti antivirus individuate: la sorgente del file virato bloccato. La tabella presenta:

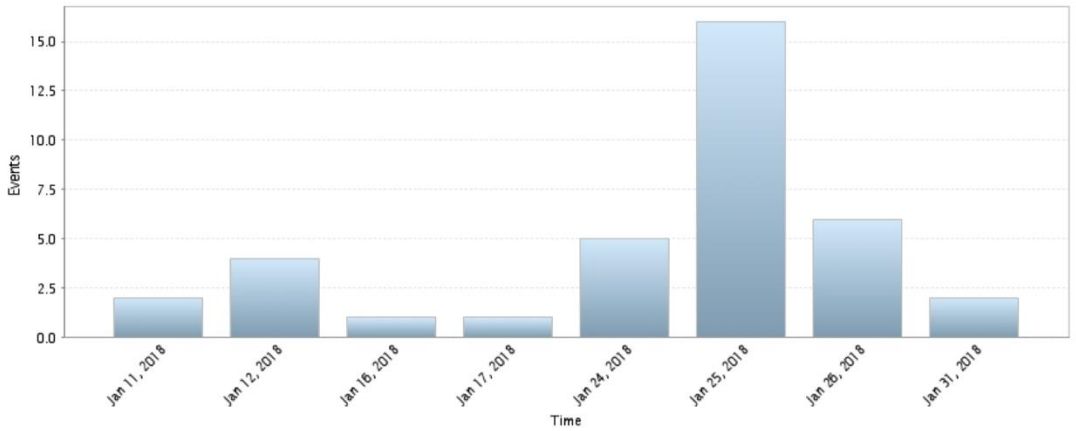
- Ip Sorgente
- Nome Host se disponibile
- Utente: solitamente vuoto
- Numero di eventi

Elementi di attenzione:

Nel caso di un numero inatteso di eventi è utile l'elenco per verificare le sorgenti, sia per intraprendere azioni correttive di sensibilizzazione degli utenti e/o blocco, e sia per verificare il motivo per cui si è tentato di traferite un file da quella sorgente.

3.33 Gateway Viruses – Timeline: Antivirus attività nel tempo

Gateway Viruses - Timeline



	Time	Events
1	Jan 11, 2018	2
2	Jan 12, 2018	4
3	Jan 16, 2018	1
4	Jan 17, 2018	1
5	Jan 24, 2018	5
6	Jan 25, 2018	16
7	Jan 26, 2018	6
8	Jan 31, 2018	2
	Total:	**37**

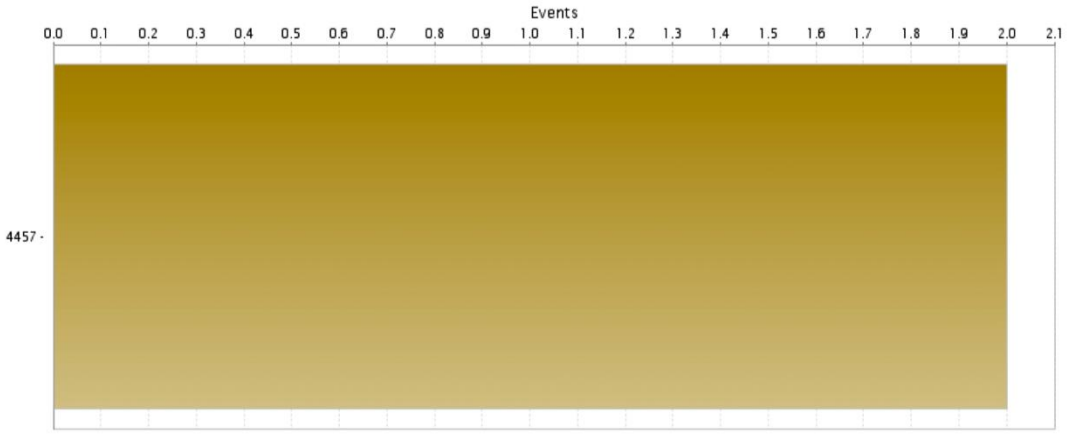
Presenta per ogni giorno il numero file bloccati dal servizio antivirus.

Elementi di attenzione:

L'analisi permette di evidenziare la presenza di anomalie, come picchi particolarmente importanti virus bloccati. Spesso avremo nell'elenco alcuni giorni con maggiore concertazione di eventi dovuto spesso al tentativo multiplo di scaricare lo stesso file virato.

3.34 Spyware - Top Spyware Detected: pincipali spyware individuati

Spyware - Top Spyware Detected



	Spyware	Priority	Events
1	4457		2
	Total:		**2**

Uno spyware è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di pubblicità mirata.
L'analisi elenca i principali spyware individuati nel periodo.
La tabella presenta:

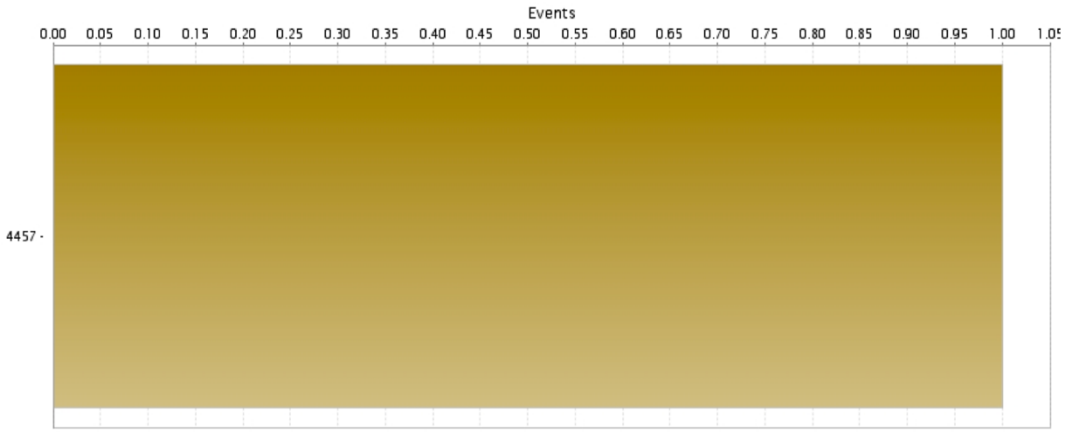
- Nome dello spyware (o ID numerico)
- Priorità
- Numero di Eventi

Elementi di attenzione:

L'analisi permette di evidenziare la presenza di attività spyware. Nel caso di attività rilevata questa sarà (nella configurazione di default) bloccata dal servizio, ma è utile verificare successivamente quali oggetti della nostra rete sono stati coinvolti.

3.35 Spyware - Top Spyware Blocked: pincipali spyware bloccati

Spyware - Top Spyware Blocked



	Spyware	Priority	Events
1	4457		1
	Total:		**1**

L'analisi elenca i principali spyware bloccati nel periodo, solitamente contiene gli stesso oggetti individuati, dato che il servizio blocca tale attività malevola.
La tabella presenta:

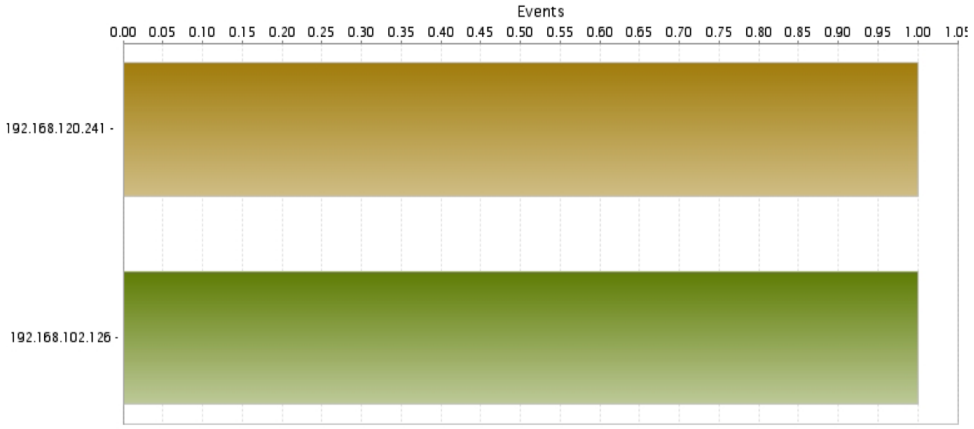
- Nome dello spyware (o ID numerico)
- Priorità
- Numero di Eventi

Elementi di attenzione:

Nel caso di attività rilevata questa sarà (nella configurazione di default) bloccata dal servizio, ma è utile verificare successivamente quali oggetti della nostra rete sono stati coinvolti.

3.36 Spyware - Top Targets: Priciapali obbiettivi spyware

Spyware - Top Targets



	Target IP	Target Host	Events
1	192.168.120.241		1
2	192.168.102.126		1
	Total:		**2**

L'analisi elenca gli oggetti verso cui le connessioni o tentativi di attività spyware si è svolta. La tabella presenta:

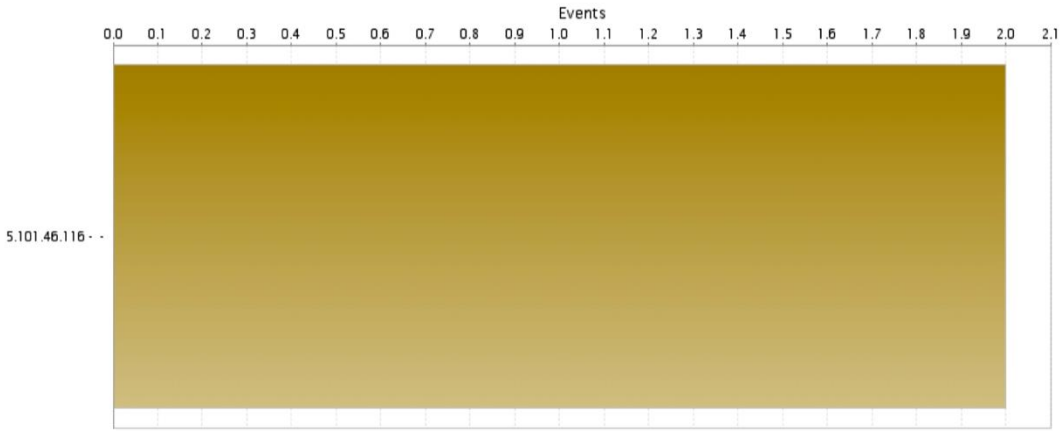
- Target IP: identificativo Ip dell'oggetto verso cui è stata fatta l'attività
- Nome dell'Host: se disponibile
- Numero di Eventi

Elementi di attenzione:

Un numero minimo di attività spyware, a seguito di navigazione o normale attività di rete è possibile. Nel coso il report presenti una numerosità importante o anomala è utile analizzare i target della propria rete con strumenti appositi antivirus o anti malware.

3.37 Spyware - Top Initiators: principali sorgenti spyware

Spyware - Top Initiators



	Initiator IP	Initiator Host	User	Events
1	5.101.46.116			2
	Total:			**2**

L'analisi elenca gli oggetti da cui le connessioni o tentativi di attività spyware sono state individuate.

La tabella presenta:

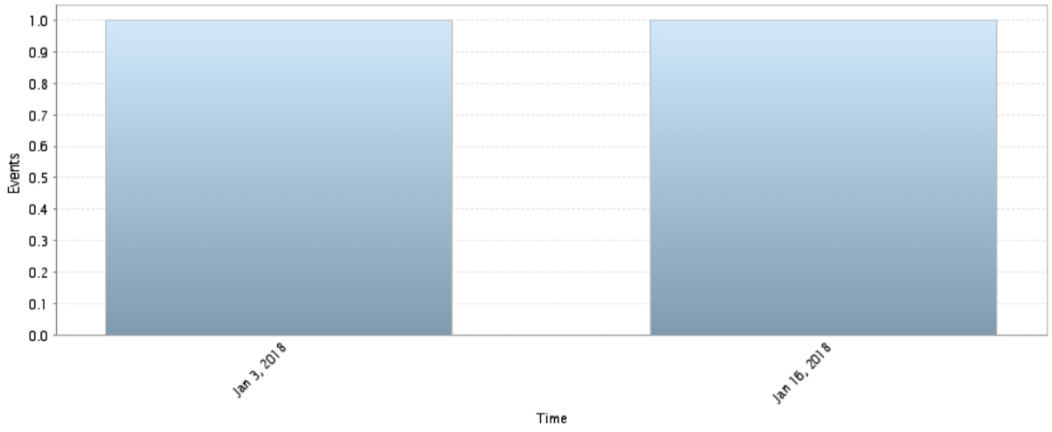
- IP Inizializzatore: identificativo Ip dell'oggetto verso cui è stata fatta l'attività
- Nome dell'Host: se disponibile
- Utente: solitamente vuoto
- Numero di Eventi

Elementi di attenzione:

Importante è verificare la sorgente dell'attività malevola per indentificare se è un oggetto noto (ad esempio un sito normalmente usato dall'azienda) potenzialmente compromesso o un falso positivo.

3.38 Spyware – Timeline: attività spyware nel periodo

Spyware - Timeline



	Time	Events
1	Jan 3, 2018	1
2	Jan 16, 2018	1
	Total:	**2**

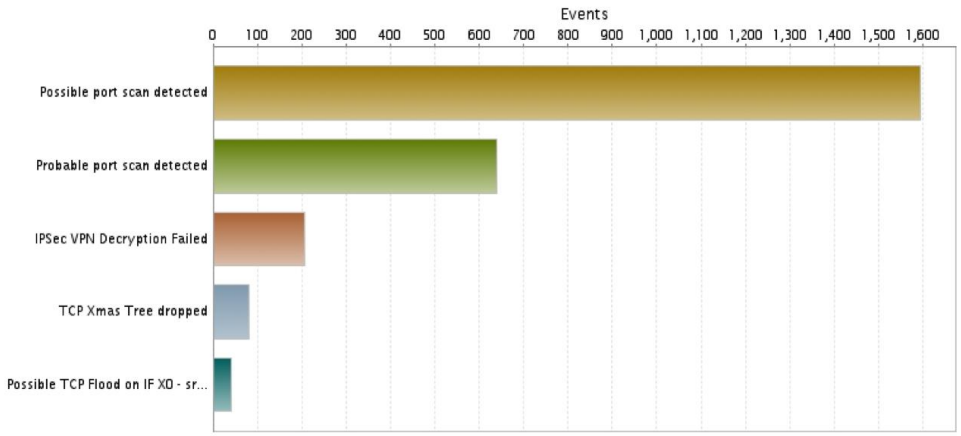
Presenta per ogni giorno il numero connessioni bloccati dal servizio anti spyware.

Elementi di attenzione:

L'analisi permette di evidenziare la presenza di anomalie, come picchi particolarmente importanti di attività spyware bloccata.

3.39 Attacks - Top Attempts: principali tentativi di attacco

Attacks - Top Attempts



	Attack	Events
1	Possible port scan detected	1,593
2	Probable port scan detected	641
3	IPSec VPN Decryption Failed	208
4	TCP Xmas Tree dropped	80
5	Possible TCP Flood on IF X0 - src: 192.168.102.125:57381 dst: 192.168.120.101:7070	42
	Total:	**2,564**

STC analizza I flussi di rete e blocca eventuali tendativi di attacco verso le reti protette.
La tabella presenta:

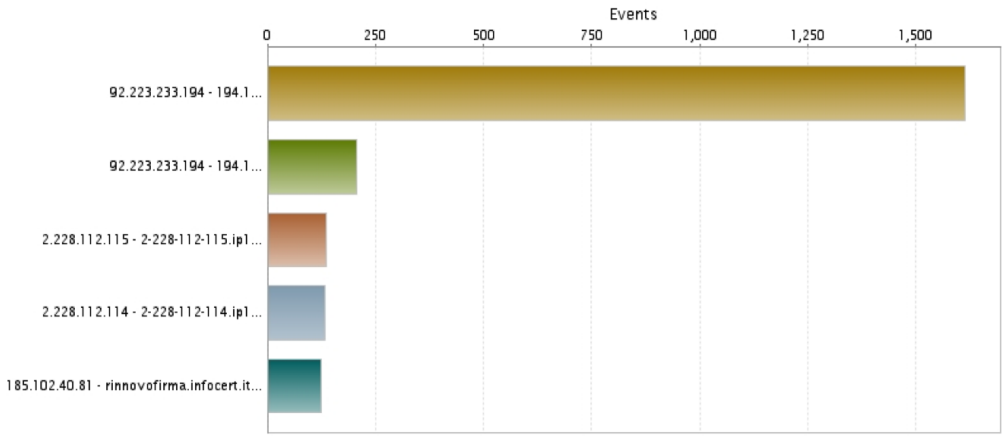
- Tipologia Attacco
- Numero di Eventi

Elementi di attenzione:

È solitamente normale individuare tentavi di attacco. Spesso possono essere eventi innocui come la scansione dei nostri Ip pubblici per individuare porte aperte. Innocui perché non sono veri attacchi, ma attività svolta da "robot" alla ricerca di punti di attacco successivo. La misura ci permette di avere un migliore lettura delle successive analisi.

3.40 Attacks - Top Targets: principali obiettivi di attacco

Attacks - Top Targets



	Target IP	Target Host	Target MAC	Events
1	92.223.233.194	194.192-28.233.223.92.in-addr.arpa	c0:ea:e4:86:5b:31	1,614
2	92.223.233.194	194.192-28.233.223.92.in-addr.arpa		208
3	2.228.112.115	2-228-112-115.ip191.fastwebnet.it	c0:ea:e4:86:5b:30	137
4	2.228.112.114	2-228-112-114.ip191.fastwebnet.it	c0:ea:e4:86:5b:30	133
5	185.102.40.81	rinnovofirma.infocert.it	c0:ea:e4:86:5b:30	124
	Total:			**2,216**

Le attività anomale e classificate come attacco sono divise in destinazioni e sorgenti, questi vista evidenzia i principali "attaccati".

La tabella presenta:

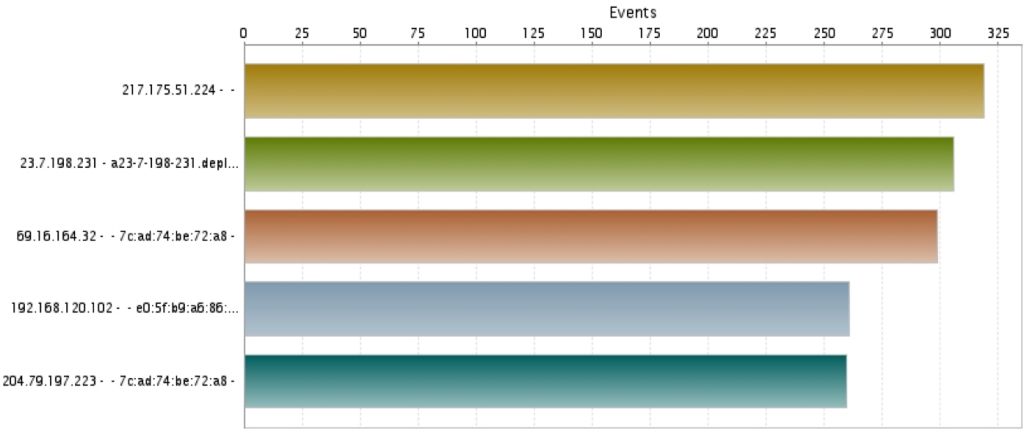
- Target IP: identificativo Ip dell'oggetto verso cui è stata fatta l'attività
- Nome dell'Host: se disponibile
- Mac Address se disponibile
- Numero di Eventi

Elementi di attenzione:

Se il target è un nostro Ip è utili verificare che sia correttamente aggiornato e con le ultime patch applicativi installati, questo perché gli attacchi solitamente sfruttano vulnerabilità note.

3.41 Attacks - Top Initiators: principali sorgenti di attacco

Attacks - Top Initiators



	Initiator IP	Initiator Host	Initiator MAC	User	Events
1	217.175.51.224				319
2	23.7.198.231	a23-7-198-231.deploy.static.akamaitechnologies.com	7c:ad:74:be:72:a8		306
3	69.16.164.32		7c:ad:74:be:72:a8		299
4	192.168.120.102		e0:5f:b9:a6:86:d6		261
5	204.79.197.223		7c:ad:74:be:72:a8		260
	Total:				**1,445**

Le attività anomale e classificate come attacco sono divise in destinazioni e sorgenti, questi vista evidenzia i principali "attaccanti".

La tabella presenta:

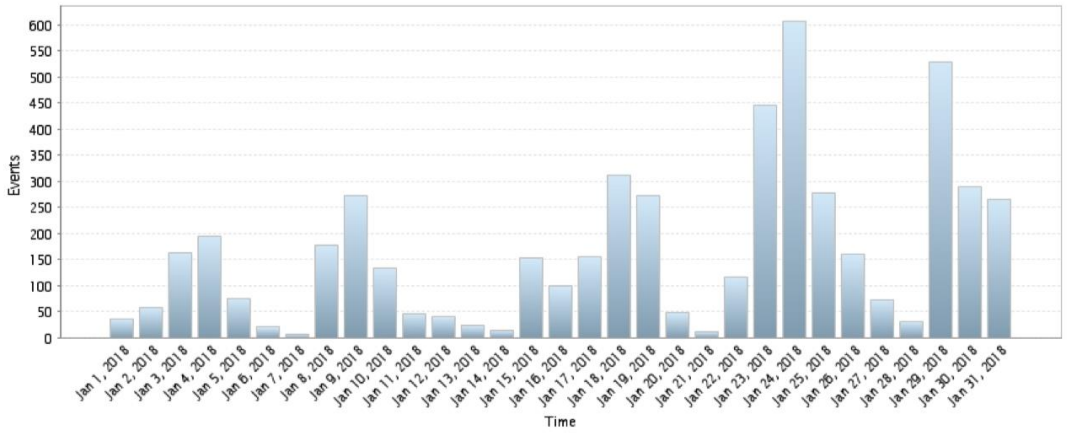
- Sorgente IP: identificativo Ip dell'oggetto da cui è stata fatta l'attività
- Nome dell'Host: se disponibile
- Mac Address se disponibile
- Numero di Eventi

Elementi di attenzione:

Se la sorgente è un nostro Ip è utili verificare che sia correttamente aggiornato e con le ultime patch applicativi installati, questo perché gli attacchi solitamente sfruttano vulnerabilità note, e potrebbe essere una macchina compromessa.

3.42 Attacks – Timeline: attacchi nel periodo

Attacks - Timeline



	Time	Events
1	Jan 1, 2018	36
2	Jan 2, 2018	58
3	Jan 3, 2018	162
4	Jan 4, 2018	195
5	Jan 5, 2018	76
6	Jan 6, 2018	21

Presenta per ogni giorno il numero connessioni bloccati dal servizio.

Elementi di attenzione:

L'analisi permette di evidenziare la presenza di anomalie, come picchi particolarmente importanti di attività bloccata. In relazione con le sorgenti e destinazioni è possibile individuare il periodo di attività e predisporre le eventuali contromisure.