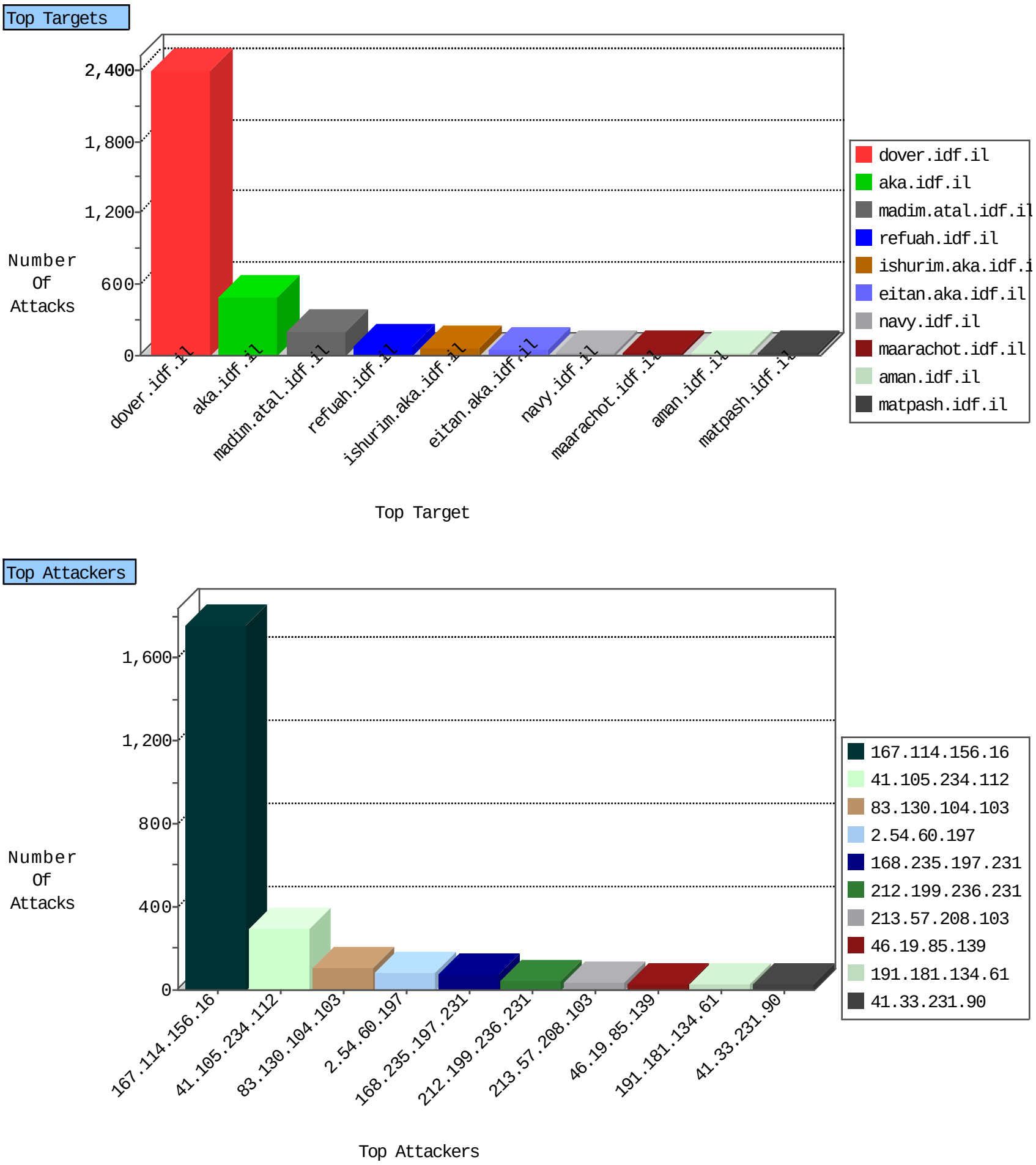
01-14-2016-16:04:08 to 01-14-2016-17:04:08

IDF Under Attack
Daily Report



01-14-2016-16:04:08 to 01-14-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8747
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3217
82.145.209.106	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
84.111.164.68	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
168.235.197.231	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
66.102.9.118	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

01-14-2016-16:04:08 to 01-14-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.45.13.150	Romania	147.237.0.34	tikshuv.idf.	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
46.4.89.35	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
185.45.13.150	Romania	147.237.0.34	tikshuv.idf.	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
122.112.77.58	China	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
172.245.224.226	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
5.254.97.75	Romania	147.237.0.34	tikshuv.idf.	10767: HTTP: Acunetix Security Scanner	Block	1
185.45.13.150	Romania	147.237.0.34	tikshuv.idf.	10767: HTTP: Acunetix Security Scanner	Block	1
5.254.97.83	Romania	147.237.0.34	tikshuv.idf.	10767: HTTP: Acunetix Security Scanner	Block	1

01-14-2016-16:04:08 to 01-14-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
79.177.199.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
208.73.207.243	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.76.177	Sweden	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
168.235.197.231	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
132.66.220.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.179.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.73.207.243	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.201	Sweden	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.23.41	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.102.76.164	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.204.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-14-2016-16:04:08 to 01-14-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.105.234.112	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	274
168.235.197.231	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	74
2.54.60.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
212.199.236.231	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.130.5.207		147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	30
46.19.85.139	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	29
46.121.139.20	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
46.19.86.69	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	24
199.203.172.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
213.57.208.103	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
213.57.208.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.86.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
2.54.60.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
62.219.165.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.60.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.60.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
191.181.134.61	Brazil	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN was acknowledged. Stripping all packet data.	drop	12
41.105.234.112	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.218	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.52.46.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
62.219.213.81	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
37.46.39.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
93.172.157.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.117.96.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.46.39.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.48.73	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.6.20	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
191.181.134.61	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.194.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
191.181.134.61	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.46.13.99	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.51.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
191.181.134.61	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.130.128.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.174	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.224	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.128.11	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
93.172.17.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
172.56.34.230	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.105.234.112	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.105.234.112	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
84.109.73.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.130.104.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
185.32.179.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.52.48.73	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 2.52.48.73	Block	11
2.54.137.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
95.86.70.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
83.130.104.103	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 83.130.104.103	Block	5
46.19.85.35	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.19.85.35	None	5
109.253.195.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.228.145.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.50.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.108.200	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.19.85.62	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
37.142.252.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.177.108.200	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.177.108.200	Block	2
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.108.200	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.177.108.200	Block	2
84.95.251.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.108.200	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.177.108.200	Block	2
79.177.108.200	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 4	Block	1
79.176.10.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.143.232.26	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/homepage.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
2.54.6.20	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.108.200	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method [[#0]]4Â˜qÂ¥`Ã-#Ã¯Â¶Ã¢Â¯UÂ?!*Â€ Ã¸md[[#5]]ÂšÃº[[#4]]Ã‘=^Â§Ã?Â,\fÃžwÃ-Â?Ã¥Â½[[#19]]Ã¾Ãµ`EÃ²Ãƒ [[#6]]0Ã¥#wÂ?Ã,Â¾Â¥Â²ÃƒÃ•6Â¼Ã¶[[#22]]Â?LÃ?Ã¬Â˜Œ5T3Ã?Â† [[#17]]Ã¼Ã¸Â¶Nl&Â-Â°Ã?Ãš in URL â€˜dÃ»)Ã·yÂŽ6Ö¹[[#22]]i[[#24]]â,ªq	Block	1
46.117.96.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.177.108.200	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.177.108.200	Block	1
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
84.108.173.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.108.200	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name c[[#29]]c}]fÂ–ÂªÃ€˜SÃŸ [[#19]]Ã…[[#23]]mÂ¢Â²Â¶Â²_Ã±b•Ã…Â-Ã…Â’ÂœÃ¸Â°Â™[[#12]]Â™ ,Â®[[#30]]Â’EU8 WÂ£RÃ?Â†Âž-ÂœÂ¨nÃ™ÃžÂ®8[[#14]]&Ã£Ã®Ã‹Ã§Ãƒ Ã°4$mÃ?;[[#6]]Â°9Â±Ã»ÃŒ[[#8]]Â¤llÃ¥rdÃ¤[[#14]]DÃ›Âª!\'Ã¸/Â€ ,[[#29]][[#31]][Ã«Â?[[#2]]\Ã‰	Block	1
213.8.204.86	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
185.45.13.150	Romania	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
2.54.129.237	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.178.173.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.135.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.108.200	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at Â‡PÃ§Â·Ã‘6Ã¡Ã© [[#6]][[#3]][[#16]]2[[#2]]&Ã®[[#7]]Â•Â«CC+Â?ÃªCYÃ‡Ã€ MTaDl[[#19]]yÃƒ4EÂ Ã˜Ã€V$Â‹Ã˜Ãœ~Ã˜Z[[#29]]ÂœÃ-Â˜JÂºw-ÂŸÃ„ Â¿Ã?Ã‰qÂ™Â?WHEÃ’Ã˜Â‹Ã…ÃŒÂ½ÃŸÂ¢Â°Â°ÃŒ [[#28]]Â«Ã²5[[#25]]Â,Â?Ã^hÂ´ ÂŸ JÂ¦Â¦-[[#8]]R3Â¦zÃ©b[[#5]]Ã?Â¥[[#0]][[#5]]Ã¢0[[#27]]Â‘%Â¿Ã‰ WwW,Ã£Ã¿Â³Â¤ Â^Â£Â?)Ã±Â”[[#27]]3fgEÃ¸•Â¡#Âš y/ÃµÃ¡[[#21]]Ã¶%Â½Ã¯3Â¥AÂœÃ¯Â®Â»3bÂ„=Âž Â²!Â£Ã?Â´'Ã«ÃºM0Ã‡Ã®{Â†FÂ¦Â½Â?	Block	1
79.177.108.200	Israel	147.237.72.166	aka.idf.il	Malformed URL â€˜dÃ»)Ã·yÂŽ6Ö¹[[#22]]i[[#24]]â,ªq;&Ö·z×¤[[#30]]~Ë† 1[[#22]][[#24]]hÃ»Â½×¡rnnâ,¬z$4ÂœlÂ¹Â£ gkÂ¢â€?Â?×³×´Â®ÃŠ [[#16]]Â¶[[#7]]h[[#0]]Ö±â€™Ö¶Ã¼}d7cÂ§×´c[[#22]]ÂŽ8Â«fl6Â§d×, [[#0]]•Â©Öµ[[#12]]Ö·×šÂŽ[[#27]]tÖ¿Ö¼[[#4]]ÂŸÂŠÖ±iÂ?×³&×‘itÂž Ö¶t"Â§jâ„¢[[#5]][[#11]]3	Block	1
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
87.69.87.39	Israel	147.237.0.16	my-kosher-kravi.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
79.176.171.231	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.176.171.231	Block	1
194.90.251.18	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
31.168.103.115	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 31.168.103.115	Block	1
2.54.6.20	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.166.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.213.81	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.253.208.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1