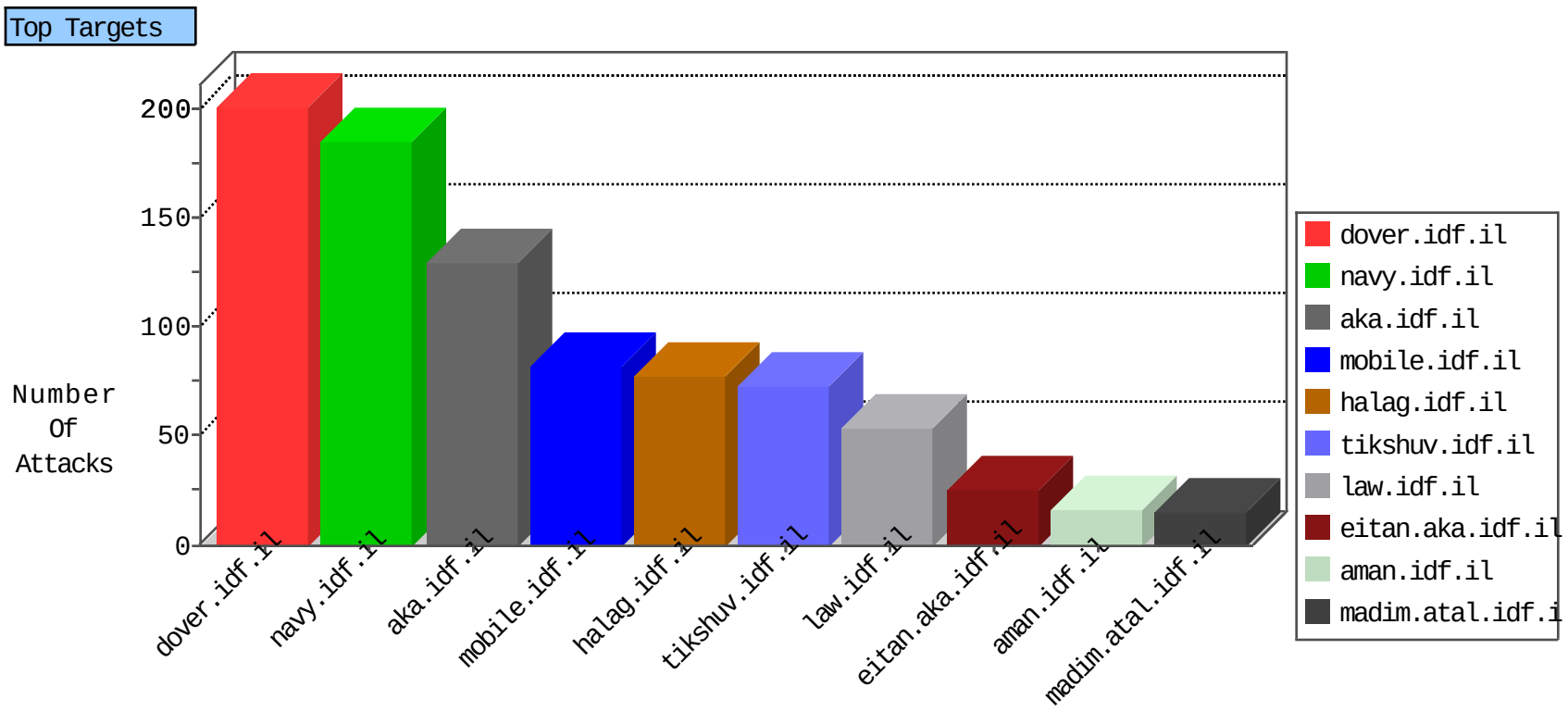
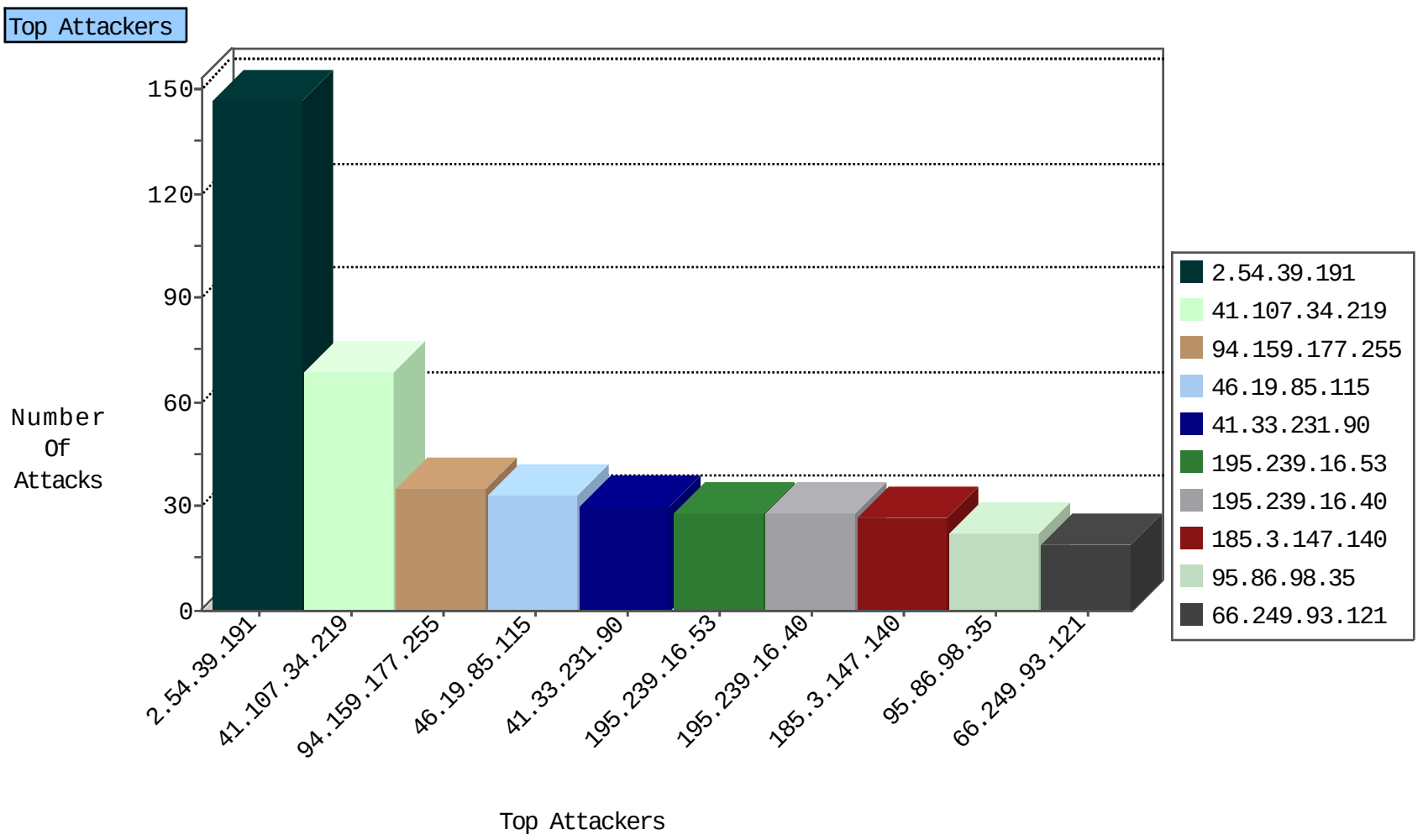
02-25-2016-23:04:06 to 02-26-2016-00:04:06

IDF Under Attack Daily Report





02-25-2016-23:04:06 to 02-26-2016-00:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.107.34.219	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	69
198.23.190.39	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
213.136.78.48	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
199.115.117.12	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
213.136.78.48	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
199.115.117.12	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
213.136.78.48	Germany	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
208.100.26.228	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1

02-25-2016-23:04:06 to 02-26-2016-00:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.88.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
85.64.2.84	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.178.98.15	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.4.32.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
185.120.126.37		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.116	Italy	147.237.77.226	www.chamatz.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
61.135.189.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.55	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-25-2016-23:04:06 to 02-26-2016-00:04:06

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	4
66.249.93.113	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.121	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
107.6.130.113	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
93.174.95.73	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
211.215.19.235	147.237.8.28	Korea, Republic of	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
40.113.118.99	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
211.215.19.235	147.237.8.14	Korea, Republic of	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.8.50	Sweden	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.8.239	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
108.61.228.113	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.255.65.207	147.237.8.27		e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
211.215.19.235	147.237.8.46	Korea, Republic of	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
40.113.118.99	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
211.215.19.235	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
40.113.118.99	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
208.80.155.214	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
193.105.134.220	147.237.76.200	Sweden	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
180.150.177.188	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
112.119.253.142	147.237.0.33	Hong Kong	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-25-2016-23:04:06 to 02-26-2016-00:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.39.191	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	147
94.159.177.255	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
185.3.147.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	13
176.13.12.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
95.86.114.253	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	11
5.29.160.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
94.230.86.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.120.226.203	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.253.145.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.216.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.54.187.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
85.64.33.146	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.27.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.179.220	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.13.21.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
70.195.194.150	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.234.253	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.33.146	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.43.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.146.164	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.146.188	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
94.230.86.153	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.93.189	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.6	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
217.132.195.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.137.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.189.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.244.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.126.10.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.8.239	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
23.81.154.194	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.29.69.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.41.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
194.90.37.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.51.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.69.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-25-2016-23:04:06 to 02-26-2016-00:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.206.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
23.81.154.194	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.166.244.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	2
109.67.27.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.117.183.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.121.123.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.123.29	Block	2
93.170.253.196	Czech Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.170.253.196	Block	2
93.170.253.196	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17607-en/dover.aspx'	Block	1
197.39.129.69	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.114.253	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7972-he/eitan.aspx&sa=u&ved=0ahukewjfq-oq9jplahui_xikhw0ydbwqfggjmae&usg=afqjcnfjrck0lo43ek8mbxpz8kw4tkgawq	Block	1
66.249.83.161	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 95.86.98.35	Block	1
5.22.130.239	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
208.115.113.87	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
149.88.185.19	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
87.71.29.148	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 95.86.98.35	Block	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version £¤ZîS>«#011^qnÀ[[#0]]äÄ:•’fC#èaPG	Block	1
37.26.146.164	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
94.159.177.255	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
198.58.102.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
97.91.157.117	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.178.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 95.86.98.35	Block	1
46.19.86.163	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.29.88.246	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.170.253.196	Czech Republic	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
62.90.179.220	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at [[#18]]&sOš½úPºìõ¬òéë7ü`Ö[[#6]]Ot6ÒjRyŸä#012±GTµúç'ë[[#3]]ìðDçë‰úÔí¡ÆÑ×ƒŽ¦“çù¤“Câdmž N-ƒ[[#0]]_á¥öù@ì?p#yj©5 9¾TBpqa\},a²Zï•~-[[#2]]°,[[#30]]_¥ªF,,ú#AÎIÇcº[[[#18]][[#11]]n1Š’[[#2]][[#19]]ò1Þ[[#16]]8ÏÝŽ¬[[#18]]{lè¤ÞòË4é¹,&ÐßúsRÑºî2…ÈÒKJnæ£n+Ÿ08%#012ü[[#27]]Þ¢¦eâ–•Ûê[[#30]]¢X[[#15]]©´%’Xýo[[#11]]NûöÄP±’[[#4]][[#8]]b=ú@	Block	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding ¨Ú[[#23]]ɔ]b[[#6]][[ʎ#7]]6q†ɔɔ[[91#]]ɽ[[62#]]¨[[#6]][[#7]]yɪɪnkɲb˜ɤgg%(…^[[#30]][[#26]]:un[[#14]]zd[[#2]]¶²¨'`…v¸Œ4ɾe‡.ʬ[[#20]][[#29]]Ý[[#6[[¶ɔ]]#5-µ]]’n»´¸±”[[8#]]@[[6#]]Ê°^jßû[[#14]]ɾ6¯vt;¸¥ˈƴ[[#25]]@9y*(¡`v –	Block	1
37.142.64.106	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
94.230.86.153	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
199.30.24.104	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.124.39	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 95.86.98.35	Block	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name [[#18]]&sOš½úPºìõ¬òéë7ü`Ö[[#6]]Ot6ÒjRyŸä#012±GTµúç'ë[[#3]]ìðDçë‰úÔí¡ÆÑ×ƒŽ¦“çù¤“Câdmž N-ƒ[[#0]]_á¥öù@ì?p#yj©5 9¾TBpqa\},a²Zï•~-[[#2]]°,[[#30]]_¥ªF,,ú#AÎIÇcº[[[#18]][[#11]]n1Š’[[#2]][[#19]]ò1Þ[[#16]]8ÏÝŽ¬[[#18]]{lè¤ÞòË4é¹,&ÐßúsRÑºî2…ÈÒKJnæ£n+Ÿ08%#012ü[[#27]]Þ¢¦eâ–•Ûê[[#30]]¢X[[#15]]©´%’Xýo[[#11]]NûöÄP±’[[#4]][[#8]]b=ú@	Block	1
93.170.253.196	Czech Republic	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/404.aspx'	Block	1
185.3.147.140	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
65.55.210.196	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
40.77.167.84	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
95.86.98.35	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1

02-25-2016-23:04:06 to 02-26-2016-00:04:06