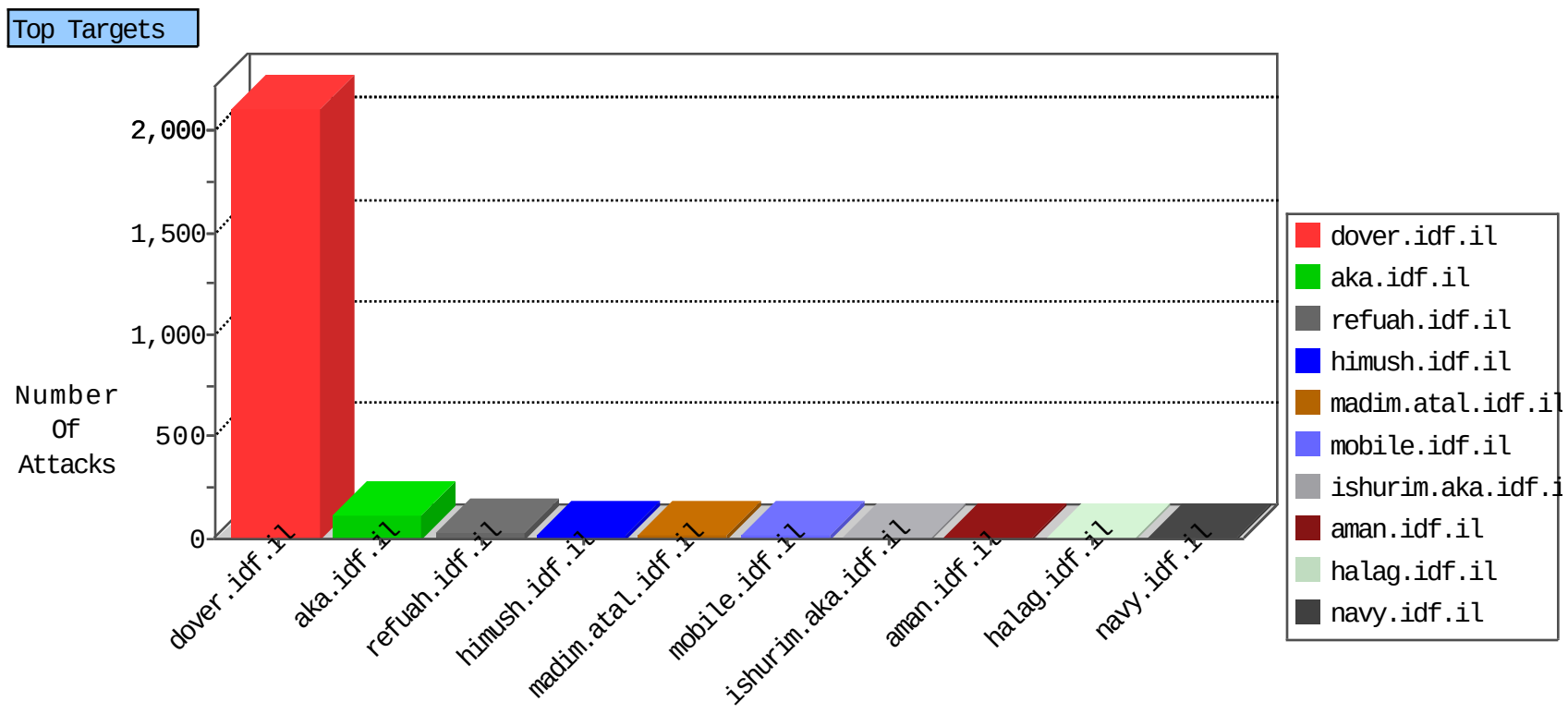
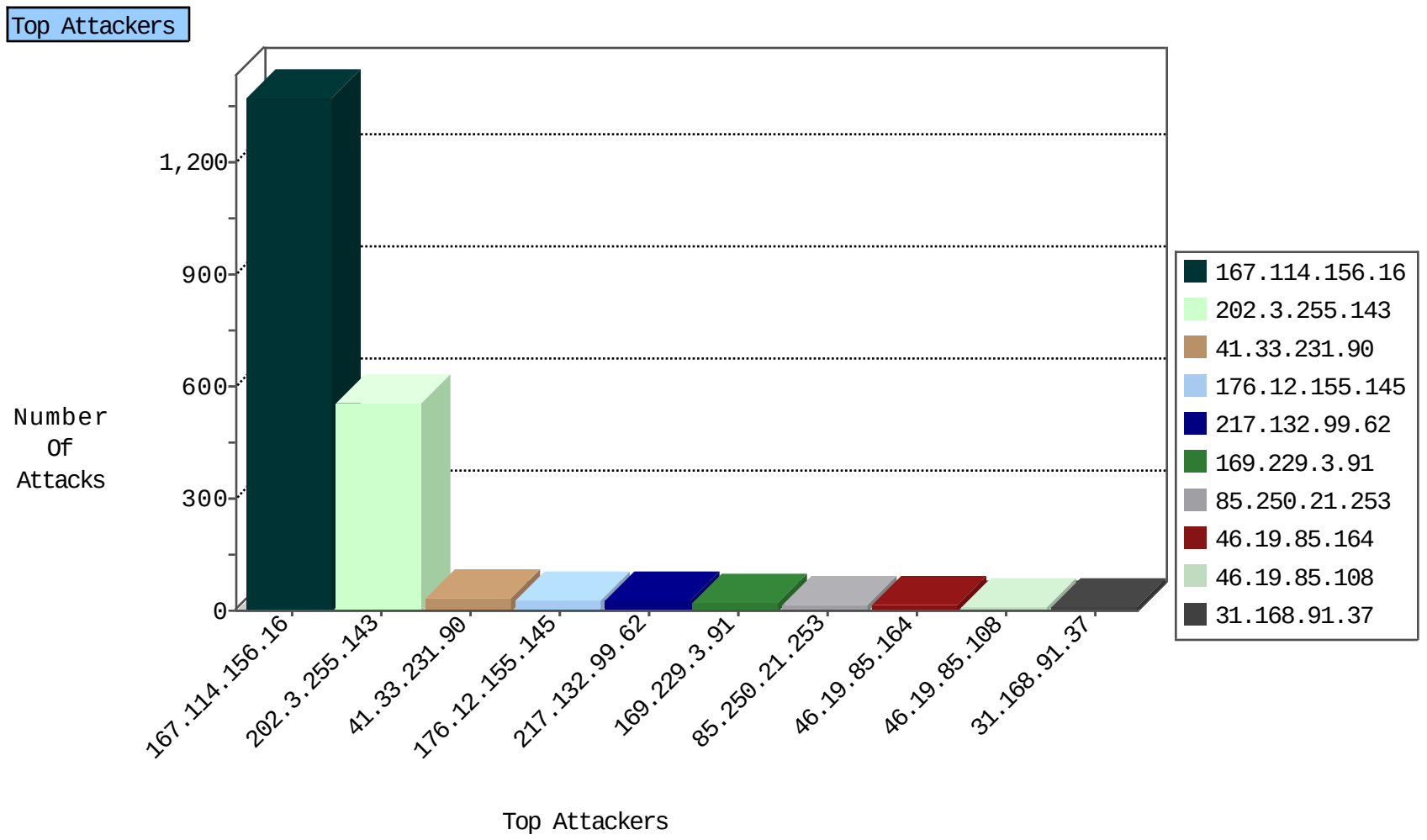
01-18-2016-00:04:06 to 01-18-2016-01:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-18-2016-00:04:06 to 01-18-2016-01:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3001
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.248.174.4	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

01-18-2016-00:04:06 to 01-18-2016-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-18-2016-00:04:06 to 01-18-2016-01:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	517
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
112.196.49.101	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.28.168	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
45.32.75.110	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 4096	1
31.210.67.78	147.237.76.197	Turkey	e.himush.idf.il	ET SCAN Potential SSH Scan	1
31.210.67.78	147.237.76.44	Turkey	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.72.14	Sweden	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
1.20.168.200	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
191.240.136.5	147.237.76.199	Brazil	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
112.196.49.101	147.237.76.199	India	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
85.250.181.16	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
31.210.67.78	147.237.76.198	Turkey	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.210.67.78	147.237.76.148	Turkey	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
31.210.67.78	147.237.76.34	Turkey	yohalan.idf.il	ET SCAN Potential SSH Scan	1
191.240.136.5	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
191.240.136.5	147.237.76.42	Brazil	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1

01-18-2016-00:04:06 to 01-18-2016-01:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
85.250.21.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
31.168.91.37	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.132.99.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
217.132.99.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.89	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.12.155.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.12.155.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
24.96.210.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
176.12.155.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.164	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
77.125.83.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.225	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.12.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.155.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
172.58.16.26	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.225	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.126.10		147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.87.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.219	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
185.120.126.77		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.55.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.119.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.32.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.210.188.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.116.87.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.59	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.137.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.229.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.135.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.35.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
63.168.168.166	Yemen	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
199.30.25.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
176.12.155.145	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
63.168.168.166	Yemen	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.207	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.113.186.193	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.113.186.193	Block	5
80.246.137.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
217.132.99.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
46.116.87.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.22.130.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.67.162.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
41.235.248.51	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Request request version	Block	1
69.179.9.171	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.66.39	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal URL Path Encoding Ö¸>ÂŽ[[#18]]aâ‚ªÖ°v+Â°:vÖ¹â€ !Â¹Ë†dÂ¾â€˜Â£×“ÃšÆ’{×™[[#8]]#Â¦×¥5{y[[#12]]Â¨Ã›j[[#24]]Â?sÂ?Ã™Ë†Ã™Ã¼×Ÿ%[[#31]]Â-	Block	1
14.192.210.195	Malaysia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	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
84.108.248.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
171.25.193.132	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
157.55.39.79	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/undefined	Block	1
185.25.151.159	Poland	147.237.76.86	navy.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method [[#23]]/ÂžÂ¶Ã²Ye"~c7	Block	1
79.182.182.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.6	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Malformed URL Ö¸>ÂŽ[[#18]]aâ‚ªÖ°v+Â°:vÖ¹â€ !Â¹Ë†dÂ¾â€˜Â£×“Ãš}Æ’{×™[[#8]]#Â¦×¥5{y[[#12]]Â¨Ã›j[[#24]]Â?sÂ?Ã™Ë†Ã™Ã¼×Ÿ%[[#31]]Â-	Block	1
37.26.147.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.113.186.193	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
84.110.208.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.12.154.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method [[#7]]Â±	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.225	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
46.116.87.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
14.192.210.195	Malaysia	147.237.77.74	law.idf.il	PHP Attempt	Block	1
188.120.148.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/forms.aspx	Block	1
95.65.34.177	Moldova, Republic of	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in URL ×˜×€aiÖ³7f[×šÖ¸Â¾â€°~Â?e[[#28]]Â©	Block	1
66.249.75.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Unknown HTTP Request Method Ã?qÃ-Â¾[[#2]]J'Ã¾Ã?l in URL Ö¸>ÂŽ[[#18]]aâ‚ªÖ°v+Â°:vÖ¹â€ !Â¹Ë†dÂ¾â€˜Â£×“ÃšÆ’{×™[[#8]]#Â¦×¥5{y[[#12]]Â¨Ã›j[[#24]]Â?sÂ?Ã™Ë†Ã™Ã¼×Ÿ%[[#31]]Â-	Block	1
141.212.122.81	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to /x	Block	1
37.142.196.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.12.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.250.21.253	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
176.13.0.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Method Ã?qÃ-Â¾[[#2]]J'Ã¾Ã?l	Block	1
46.182.106.190	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
14.192.210.195	Malaysia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1