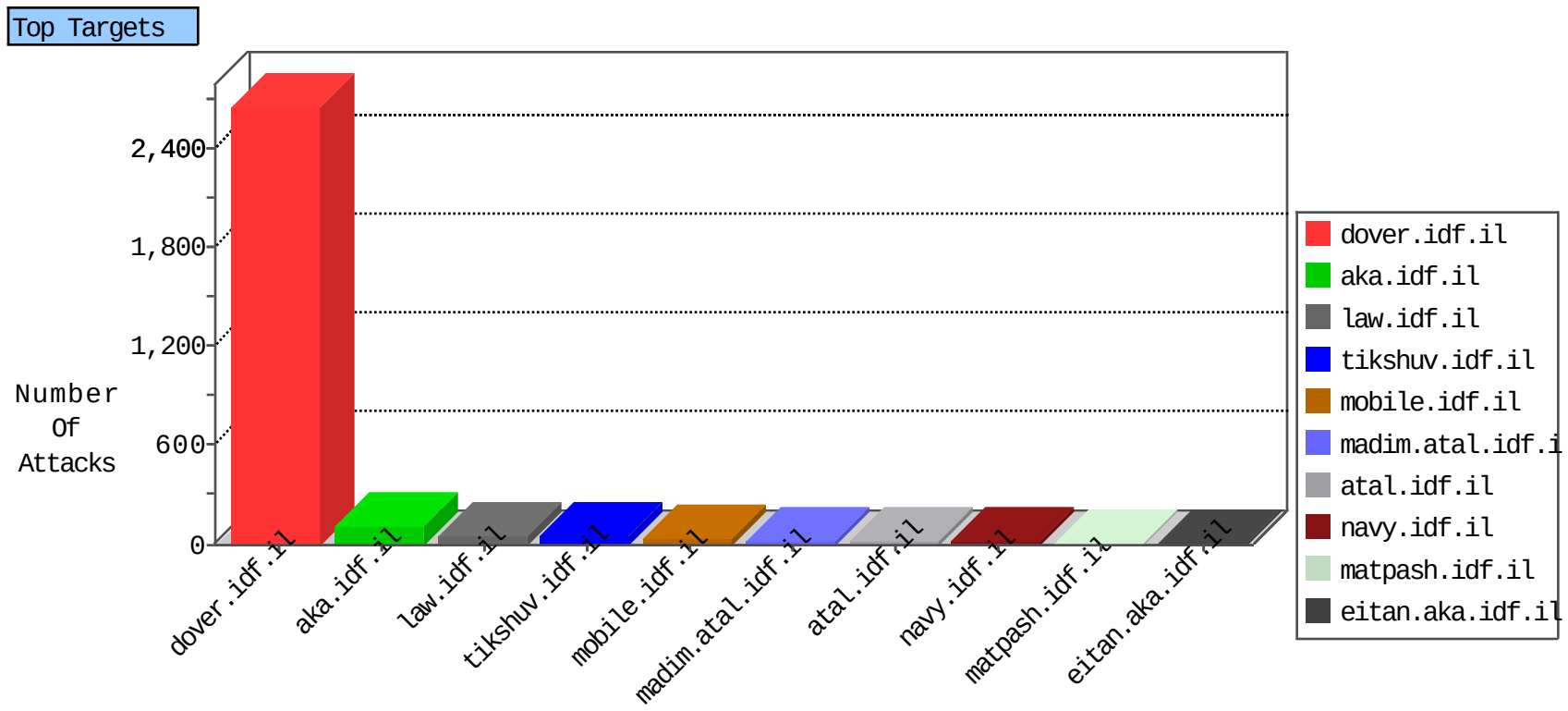
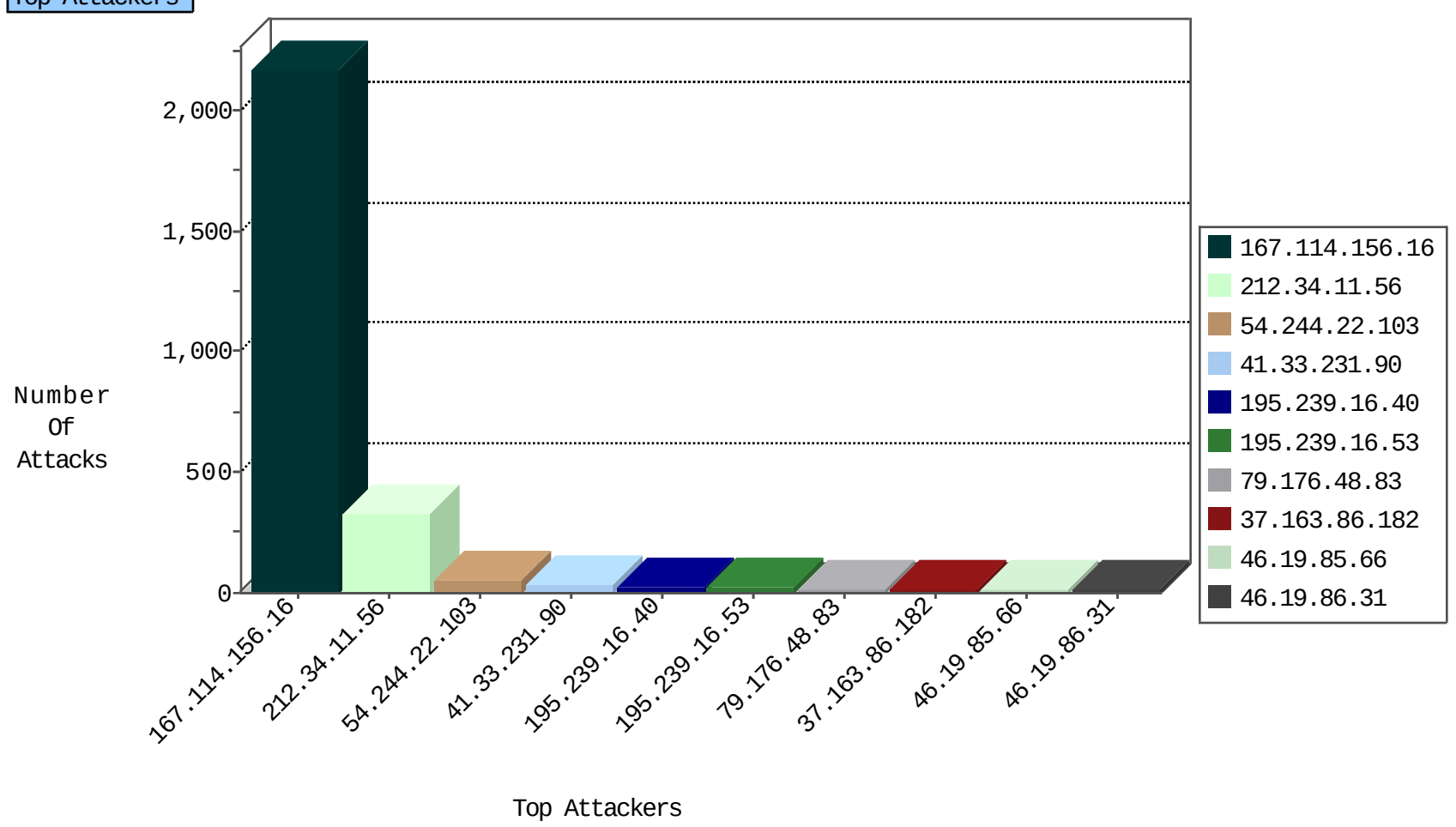
01-22-2016-23:04:08 to 01-23-2016-00:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-22-2016-23:04:08 to 01-23-2016-00:04:08

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	3045
212.34.11.56	Jordan	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1431
64.31.132.129	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
42.112.10.66	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
146.185.239.100	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1
115.239.228.10	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Http	drop	1
42.112.10.87	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
74.91.28.58	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
142.54.160.212	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
42.112.10.92	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
190.233.72.123	Peru	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.61	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
42.112.10.65	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
142.54.160.213	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
42.112.10.93	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
190.233.72.123	Peru	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
104.233.70.144		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-22-2016-23:04:08 to 01-23-2016-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.223.211.30	Spain	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	4
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
178.175.142.50	Moldova, Republic of	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.207	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-22-2016-23:04:08 to 01-23-2016-00:04:08

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	4
66.249.66.77	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
177.240.201.201	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
169.50.77.72	147.237.8.45	Switzerland	e.eitan.idf.i	ET SCAN NMAP -sS window 1024	1
189.195.212.52	147.237.76.34	Mexico	yohalan.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.240.201.201	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

01-22-2016-23:04:08 to 01-23-2016-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	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
212.34.11.56	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
79.176.48.83	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.155.199	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.31	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.147.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.34.11.56	Jordan	147.237.77.216	dover.idf.il	SYN Attack		reject	7
212.34.11.56	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.178.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.182.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.87.220	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
196.217.184.36	Morocco	147.237.77.216	dover.idf.il	drop		drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.120.131.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
108.217.100.49	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
89.217.250.125	Switzerland	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.163.86.182	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.176.204.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.163.86.182	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.178.162.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.163.86.182	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.230.26.56	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.131.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.163.86.182	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
37.46.38.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.110.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.163.86.182	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.67.199.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.8.83	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.98.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.29.222	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
157.55.39.253	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.15.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
188.120.148.197	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
173.48.107.248	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2

01-22-2016-23:04:08 to 01-23-2016-00:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.142.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
37.142.68.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
212.34.11.56	Jordan	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	4
212.34.11.56	Jordan	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	4
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.34.11.56	Jordan	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	3
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.125.87.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.13	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
197.160.25.27	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	1
46.19.85.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.254	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/edim/fund/Ã£â€”Ã¢â‚¬Ë œÃ£â€”Ã¢â‚¬Â?Ã£â€”Ã¢Â§Ã£â€”Ã¥Â¾Ã£â€”Ã¢â‚¬Â?	Block	1
130.193.51.51	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.128	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	1
66.220.158.116	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.66	Block	1
157.55.39.250	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/misrot.aspx	Block	1
92.139.158.61	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
197.160.25.27	Egypt	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
167.88.118.169	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
150.199.118.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
82.166.242.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
189.202.227.196	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.66.33	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.66	Block	1
157.55.39.251	United States	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/kamlar/contact/default.asp	Block	1
41.233.88.92	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
217.73.208.105	Italy	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.178.151.126	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
167.88.118.169	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
64.19.78.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.245	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/reports/waterreport34.pub	Block	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
5.22.131.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.34.11.56	Jordan	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
84.108.69.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
191.178.26.87	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.66	Block	1
157.55.39.253	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/general.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
41.233.88.92	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
79.178.151.126	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1

01-22-2016-23:04:08 to 01-23-2016-00:04:08