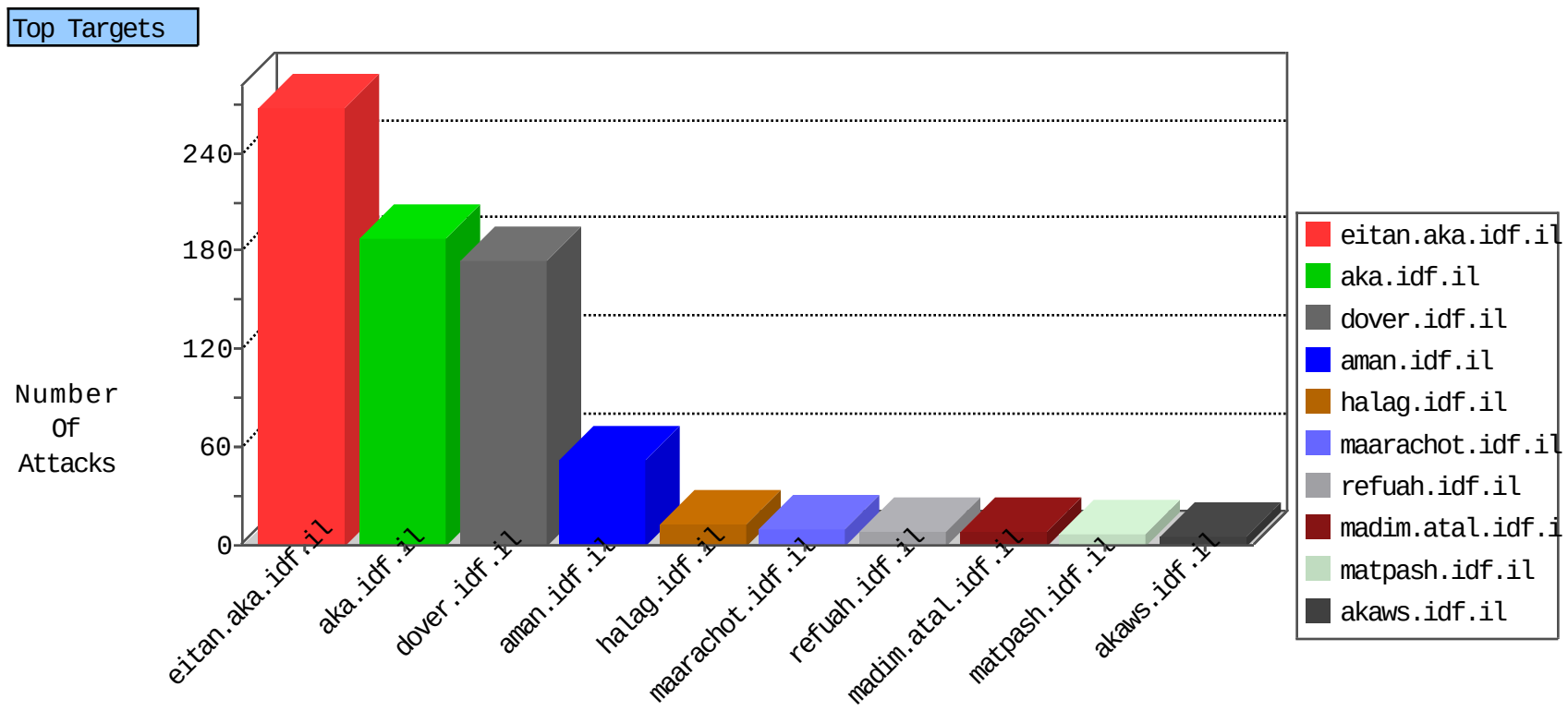
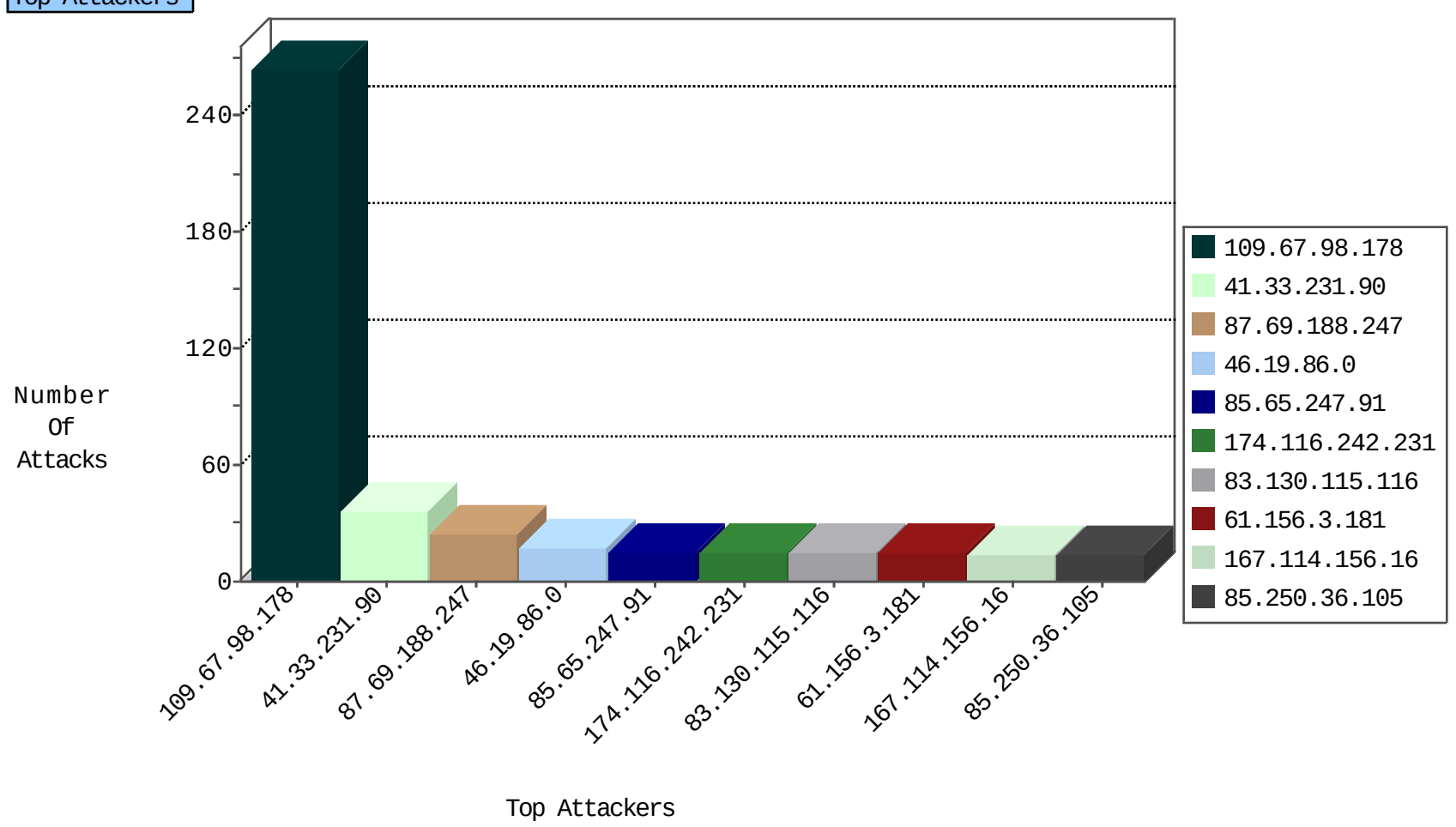
12-23-2015-02:04:07 to 12-23-2015-03:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-23-2015-02:04:07 to 12-23-2015-03:04:07

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	389
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
80.70.233.236	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
31.168.220.10	Israel	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
31.168.220.10	Israel	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
61.156.3.181	China	147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	1
31.168.220.10	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
61.156.3.181	China	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
31.168.220.10	Israel	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1

12-23-2015-02:04:07 to 12-23-2015-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.156.3.181	China	147.237.76.42	refuah.idf.il	20086: HTTP: Mueblackcat Security Scanner	Block	4
61.156.3.181	China	147.237.77.216	dover.idf.il	20086: HTTP: Mueblackcat Security Scanner	Block	4
61.156.3.181	China	147.237.76.42	refuah.idf.il	20085: HTTP: Mueblackcat Security Scanner Initial Request	Block	1
61.156.3.181	China	147.237.77.216	dover.idf.il	20085: HTTP: Mueblackcat Security Scanner Initial Request	Block	1
216.17.111.245	United States	147.237.77.234	halag.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

12-23-2015-02:04:07 to 12-23-2015-03:04:07

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	3
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
166.63.122.229	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
61.156.3.181	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
193.104.203.4	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.54.178	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
166.63.122.229	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.156.3.181	147.237.76.42	China	refuah.idf.il	ET WEB_SERVER Muieblackcat scanner	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1

12-23-2015-02:04:07 to 12-23-2015-03:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.98.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	264
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
87.69.188.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
83.130.115.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
85.65.247.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
174.116.242.231	Canada	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
85.250.36.105	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
79.176.7.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
79.179.19.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
79.176.136.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
85.250.111.90	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
185.120.126.85		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.78.62	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.115.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.19.86.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.86.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.116.177.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.0	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
176.12.146.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
66.249.69.88	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
202.141.247.2	Pakistan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.86.0	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.168	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.250.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
65.55.210.80	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
149.78.232.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
84.109.117.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.183.53.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
82.166.68.171	Israel	147.237.0.35	akaws.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
79.181.138.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
79.178.63.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.34.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.53.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3
46.19.86.0	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3
46.19.86.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	alert	3
24.45.202.126	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
84.229.158.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.168	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid sequence number	alert	2
87.68.156.138	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
46.19.85.168	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
176.13.20.0	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.69.52.102	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
85.64.216.38	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
188.37.139.65	Portugal	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
150.70.97.86	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	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
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
2.54.40.243	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
158.69.52.102	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
131.253.25.204	United States	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	1
94.242.253.92	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/shared/usercontrols/navmenu/undefined	Block	1
195.154.194.111	France	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
150.70.173.44	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
23.20.197.30	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
176.13.16.117	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
131.253.25.204	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/i/jot	Block	1
106.187.49.117	Japan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
195.154.194.111	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/wp-login.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
150.70.173.44	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
109.201.152.232	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.127.188.12	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
23.80.97.67	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
185.17.184.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
141.212.122.80	United States	147.237.76.200	eitan.aka.idf.il	Malformed URL proxytest.zmap.io:80	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
198.35.30.115	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	1
131.253.25.166	United States	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP 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
79.176.136.252	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
46.166.190.170	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
188.37.139.65	Portugal	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
150.70.97.86	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	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
198.35.30.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.228.162	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
158.69.52.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 158.69.52.102	Block	1
2.54.10.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
131.253.25.166	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/i/jot	Block	1