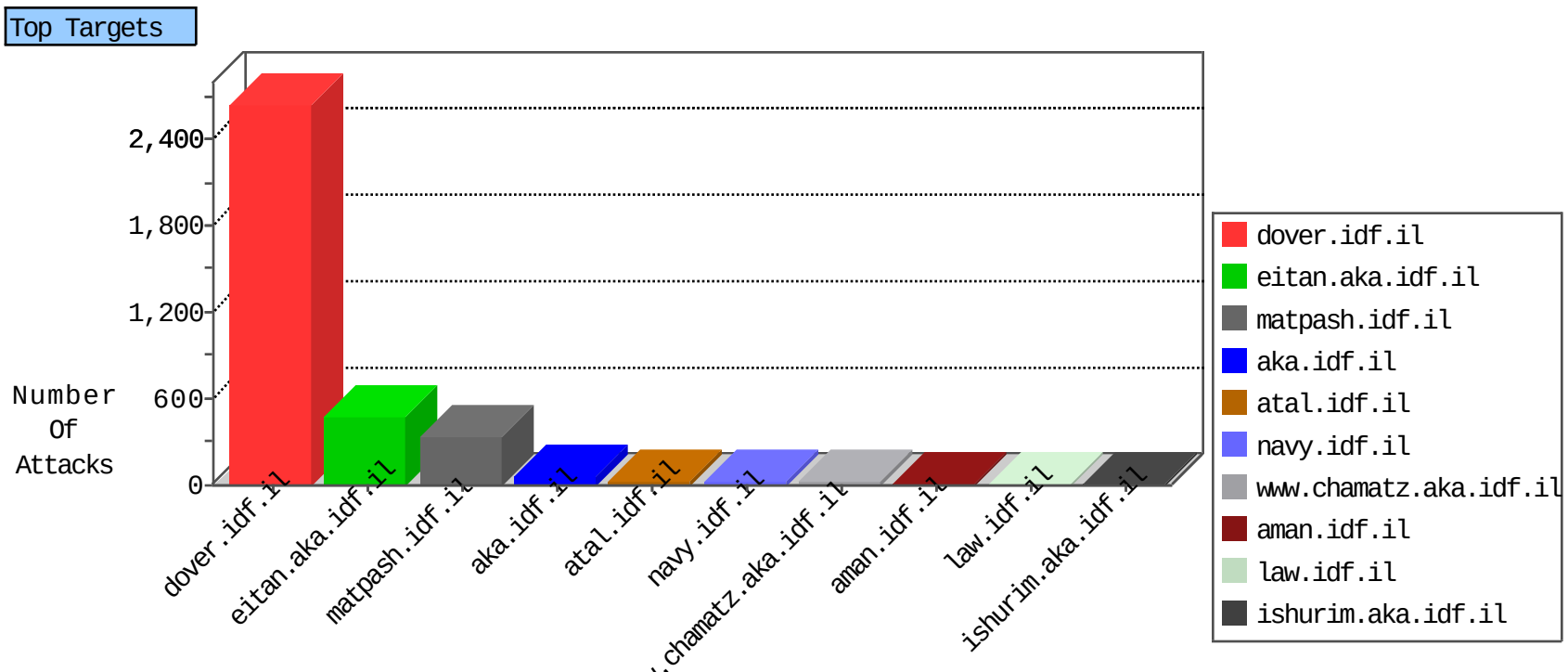
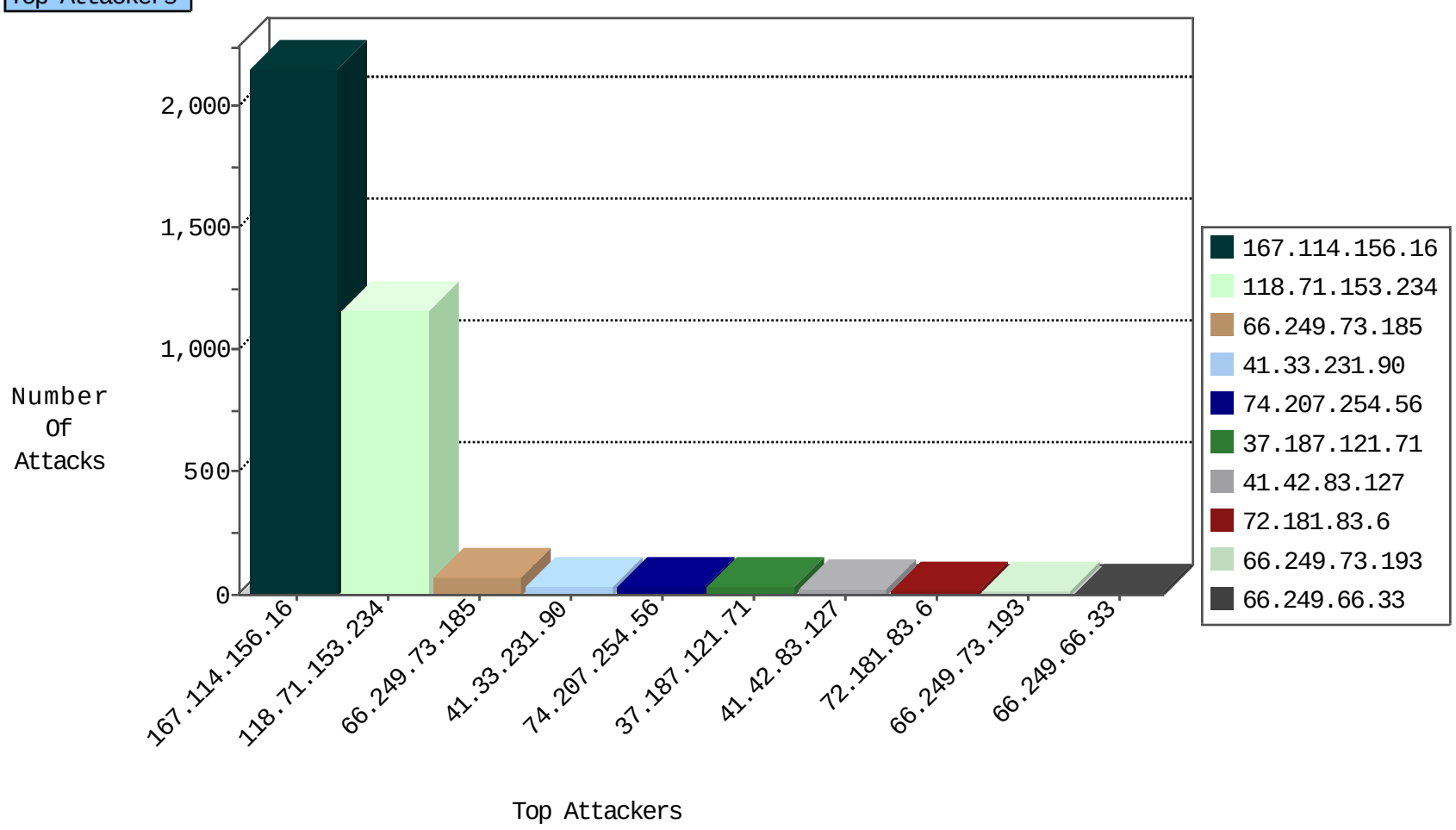
11-27-2015-04:04:08 to 11-27-2015-05:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-27-2015-04:04:08 to 11-27-2015-05:04:08

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	3306
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3025
66.249.66.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	776
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2
153.31.160.5	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
141.212.121.204	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
153.31.160.5	United States	147.237.76.176	test.ncore.idf.i	Block_Ntp_All_Net	drop	1

11-27-2015-04:04:08 to 11-27-2015-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.42.83.127	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1
95.91.45.195	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-27-2015-04:04:08 to 11-27-2015-05:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
118.71.153.234	147.237.77.216	Vietnam	dover.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	24
118.71.153.234	147.237.77.233	Vietnam	atal.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	7
118.71.153.234	147.237.77.176	Vietnam	matpash.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	7
118.71.153.234	147.237.76.86	Vietnam	navy.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	6
118.71.153.234	147.237.72.166	Vietnam	aka.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
118.71.153.234	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	4
118.71.153.234	147.237.0.34	Vietnam	tikshuv.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	3
41.42.83.127	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	3
118.71.153.234	147.237.77.74	Vietnam	law.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	3
118.71.153.234	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	3
118.71.153.234	147.237.76.200	Vietnam	eitan.aka.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	3
199.101.186.134	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
61.76.95.244	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
155.133.10.37	147.237.72.156	Poland	aman.idf.il	ET SCAN NMAP -sS window 3072	1
31.6.71.154	147.237.76.199	Poland	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
118.71.153.234	147.237.72.156	Vietnam	aman.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
212.227.141.223	147.237.0.33	Germany	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
198.23.176.210	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -sS window 1024	1
155.133.10.37	147.237.72.156	Poland	aman.idf.il	ET SCAN NMAP -sS window 4096	1
41.42.83.127	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
119.73.228.130	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
31.6.71.154	147.237.72.156	Poland	aman.idf.il	ET SCAN NMAP -sS window 1024	1

11-27-2015-04:04:08 to 11-27-2015-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
118.71.153.234	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	426
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	156
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
118.71.153.234	Vietnam	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
72.181.83.6	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	9
100.100.85.117		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
37.187.121.71	France	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
2.52.134.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.4.176	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.146.220	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.187.121.71	France	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.187.121.71	France	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
37.187.121.71	France	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
118.71.153.234	Vietnam	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
109.67.99.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.89		147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
118.71.153.234	Vietnam	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
37.187.121.71	France	147.237.8.45	e.eitan.idf.il	drop	First packet isn't SYN	drop	3
173.88.238.81	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.187.121.71	France	147.237.8.46	e.chinuch.idf.il	drop	First packet isn't SYN	drop	3
37.187.121.71	France	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.201.138.10	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
199.30.25.255	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
107.181.178.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.105	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.122.72	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.216	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.123.6.153	Moldova, Republic of	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.140	United States	147.237.0.35	akaws.idf.il	drop		drop	1
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
141.212.122.87	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.166.170.6	Lithuania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.67	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.96	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
172.56.31.8	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.135	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.72	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.227	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
118.71.153.234	Vietnam	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
176.123.6.157	Moldova, Republic of	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.141	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.94	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

11-27-2015-04:04:08 to 11-27-2015-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
118.71.153.234	Vietnam	147.237.77.176	matpash.idf.il	Distributed Abnormally Long Request	Block	314
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
118.71.153.234	Vietnam	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 118.71.153.234	Block	34
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	15
41.42.83.127	Egypt	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.42.83.127	Block	13
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 118.71.153.234	Block	9
118.71.153.234	Vietnam	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 118.71.153.234	Block	7
118.71.153.234	Vietnam	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 118.71.153.234	Block	5
118.71.153.234	Vietnam	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 118.71.153.234	Block	5
118.71.153.234	Vietnam	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 118.71.153.234	Block	5
74.207.254.56	United States	147.237.76.86	navy.idf.il	Multiple Illegal HTTP Version from 74.207.254.56	Block	4
118.71.153.234	Vietnam	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 118.71.153.234	Block	4
118.71.153.234	Vietnam	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 118.71.153.234	Block	4
74.207.254.56	United States	147.237.76.86	navy.idf.il	Multiple Abnormally Long Request from 74.207.254.56	Block	4
118.71.153.234	Vietnam	147.237.77.226	www.chamatz.aka.idf.il	Distributed Abnormally Long Request	Block	3
118.71.153.234	Vietnam	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 118.71.153.234	Block	3
40.77.167.91	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
74.207.254.56	United States	147.237.76.42	refuah.idf.il	Multiple Abnormally Long Request from 74.207.254.56	Block	3
74.207.254.56	United States	147.237.76.42	refuah.idf.il	Multiple Illegal HTTP Version from 74.207.254.56	Block	3
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	2
74.207.254.56	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Abnormally Long Request from 74.207.254.56	Block	2
74.207.254.56	United States	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 74.207.254.56	Block	2
37.26.147.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
74.207.254.56	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Illegal HTTP Version from 74.207.254.56	Block	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
74.207.254.56	United States	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 74.207.254.56	Block	2
74.207.254.56	United States	147.237.77.233	atal.idf.il	Multiple Abnormally Long Request from 74.207.254.56	Block	2
74.207.254.56	United States	147.237.77.233	atal.idf.il	Multiple Illegal HTTP Version from 74.207.254.56	Block	2
118.71.153.234	Vietnam	147.237.76.200	eitan.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
74.207.254.56	United States	147.237.77.176	matpash.idf.il	Multiple Illegal HTTP Version from 74.207.254.56	Block	1
54.209.59.210	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/5/3895.pdf&quot	Block	1
31.193.51.17	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
74.207.254.56	United States	147.237.76.31	nakchal.idf.il	Multiple Abnormally Long Request from 74.207.254.56	Block	1
118.71.153.234	Vietnam	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/clientscripts/jquery/2.74	Block	1
66.249.73.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17858-he/dover.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
141.212.122.64	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /x	Block	1
84.111.65.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.42.83.127	Egypt	147.237.77.216	dover.idf.il	Multiple signatures from 41.42.83.127	Block	1
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Parameter Type Violation searchText in www.idf.il/1500-en/dover.aspx	Block	1
207.46.13.177	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
5.102.246.130	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.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
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
184.105.247.195	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/2799.jpg	Block	1
74.207.254.56	United States	147.237.76.31	nakchal.idf.il	Multiple Illegal HTTP Version from 74.207.254.56	Block	1
66.249.73.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20050-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
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1

11-27-2015-04:04:08 to 11-27-2015-05:04:08