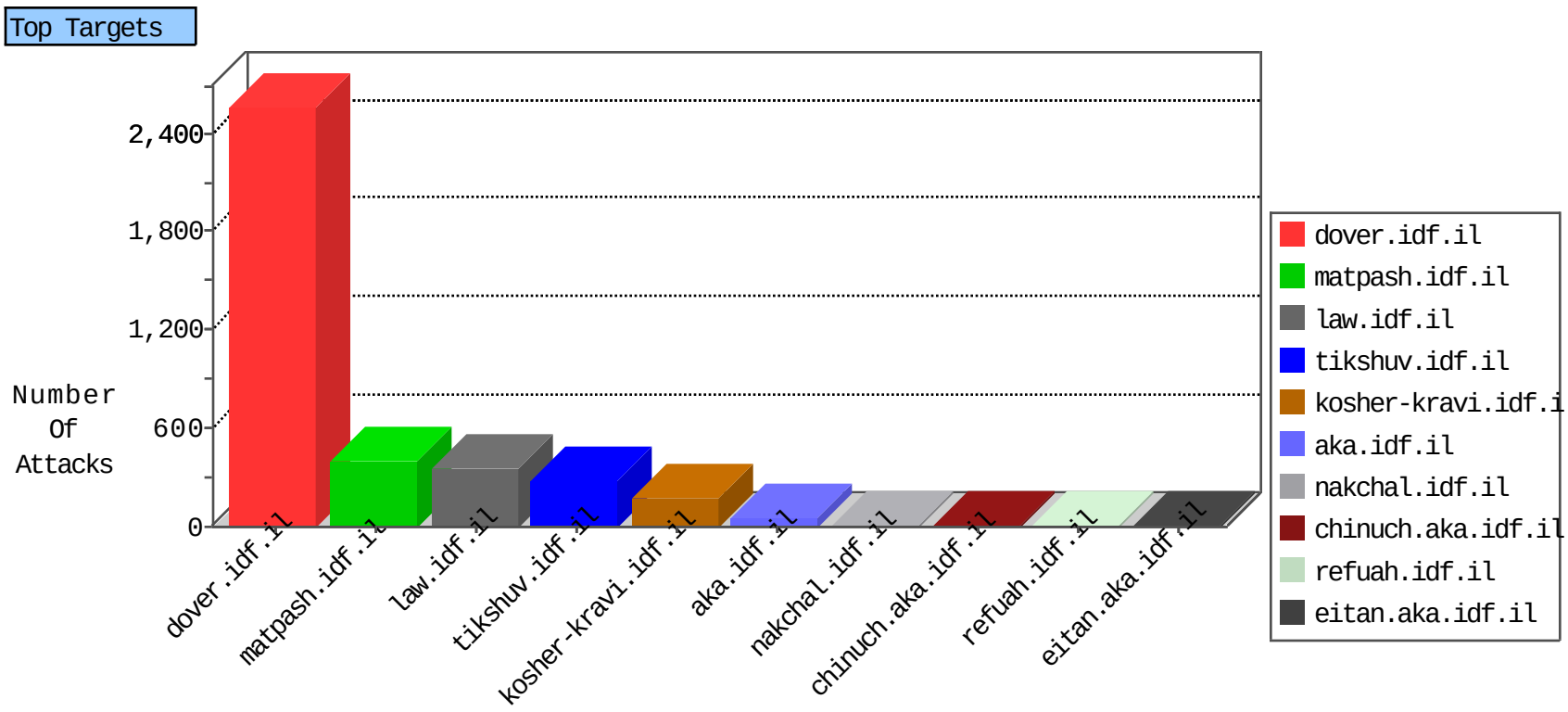
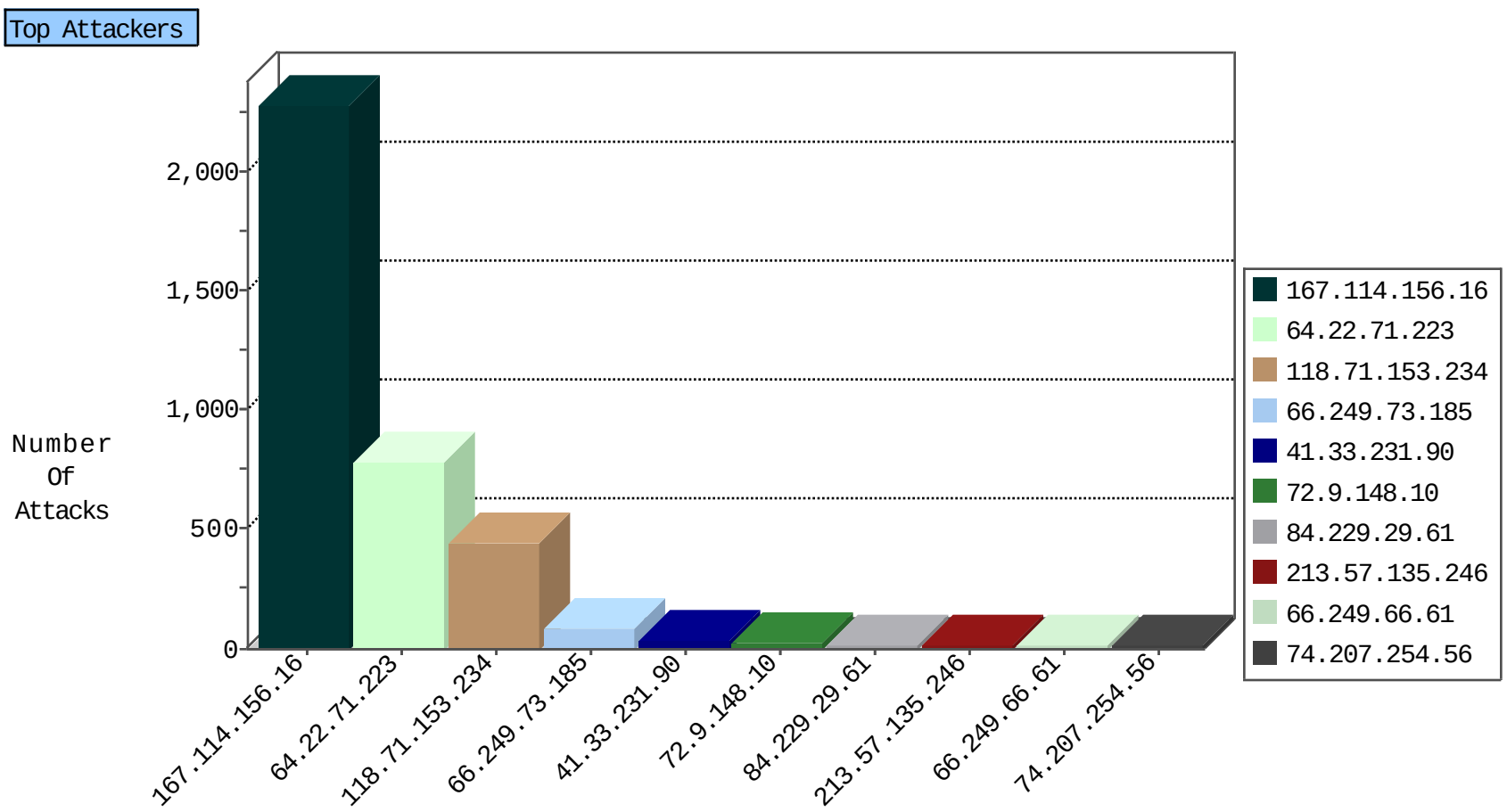
11-27-2015-05:04:01 to 11-27-2015-06:04:01

IDF Under Attack Daily Report





11-27-2015-05:04:01 to 11-27-2015-06:04:01

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	3703
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
141.212.121.206	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
173.242.125.211	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

11-27-2015-05:04:01 to 11-27-2015-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

11-27-2015-05:04:01 to 11-27-2015-06:04:01

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	20
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
89.178.15.14	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
123.203.156.53	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
118.71.153.234	147.237.77.176	Vietnam	matpash.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
46.228.207.18	147.237.0.200	Germany	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

11-27-2015-05:04:01 to 11-27-2015-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
64.22.71.223	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	318
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	88
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
213.57.135.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
64.22.71.223	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
118.71.153.234	Vietnam	147.237.77.176	matpash.idf.il	HTTP Format Sizes	'Referer' header length exceeded maximum allowed length	monitor	9
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.34.98		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.75.77.200	Czech Republic	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.125.73.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.73.201	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
157.55.39.112	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.75.77.174	Czech Republic	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.99	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
207.46.13.137	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
62.219.115.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.75.77.123	Czech Republic	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
109.66.179.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.217.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
209.126.230.71	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
64.233.172.163	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.91	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
64.233.172.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
40.77.167.21	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.67	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
209.126.230.71	United States	147.237.0.35	akaws.idf.il	drop		drop	1
46.19.86.32	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.108	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.89.107	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
80.246.133.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.94	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.80	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
216.218.206.83	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.57.57.11	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.90	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.70	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
209.126.230.71	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.32	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

11-27-2015-05:04:01 to 11-27-2015-06:04:01

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	369
64.22.71.223	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	267
64.22.71.223	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 64.22.71.223	Block	169
64.22.71.223	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	9
118.71.153.234	Vietnam	147.237.77.176	matpash.idf.il	Parameter Type Violation __EVENTVALIDATION in www.cogat.idf.il/938-he/cogat.aspx	Block	9
37.59.232.247	France	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	5
37.59.232.247	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.59.232.247	Block	4
46.116.106.18	Israel	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	3
46.116.106.18	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	3
64.22.71.223	United States	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
81.7.14.25	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
64.22.71.223	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	2
37.26.149.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	2
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
84.229.29.61	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.229.29.61	Block	1
74.207.254.56	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
142.4.218.201	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
2.50.17.207	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.229.29.61	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/scriptresource.axd	Block	1
64.5.53.237	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	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
74.207.254.56	United States	147.237.0.34	tikshuv.idf.il	Multiple Abnormally Long Request from 74.207.254.56	Block	1
41.108.175.12	Algeria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Parameter Type Violation __VIEWSTATEGENERATOR in www.idf.il/1116-en/dover.aspx	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
85.250.67.204	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/xmlrpc.php	Block	1
84.229.29.61	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	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
74.207.254.56	United States	147.237.76.42	refuah.idf.il	Illegal HTTP Version + "?SearchText=" + escape($(" HTTP/1.1	Block	1
173.230.156.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
2.50.17.207	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
68.180.228.170	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69859.jpg	Block	1
84.229.29.61	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
207.46.13.90	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/70400.jpg	Block	1
84.229.29.61	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
74.207.254.56	United States	147.237.0.34	tikshuv.idf.il	Multiple Illegal HTTP Version from 74.207.254.56	Block	1
41.108.175.12	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
118.71.153.234	Vietnam	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
66.249.73.143	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1362-16540-he/dover.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.229.29.61	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
209.126.230.71	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /	Block	1
46.116.106.18	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
197.135.219.96	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1

11-27-2015-05:04:01 to 11-27-2015-06:04:01