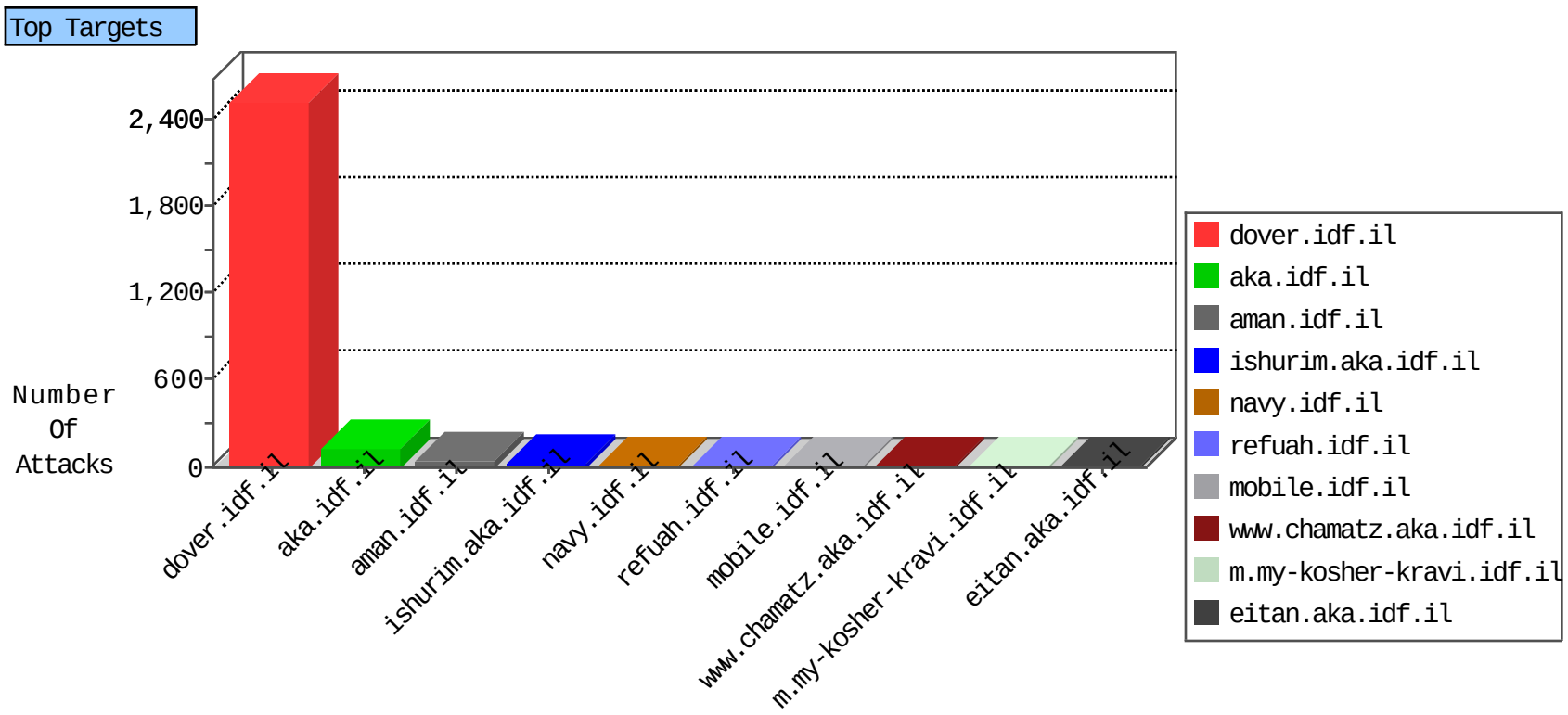
01-19-2016-01:06:48 to 01-19-2016-02:06:48

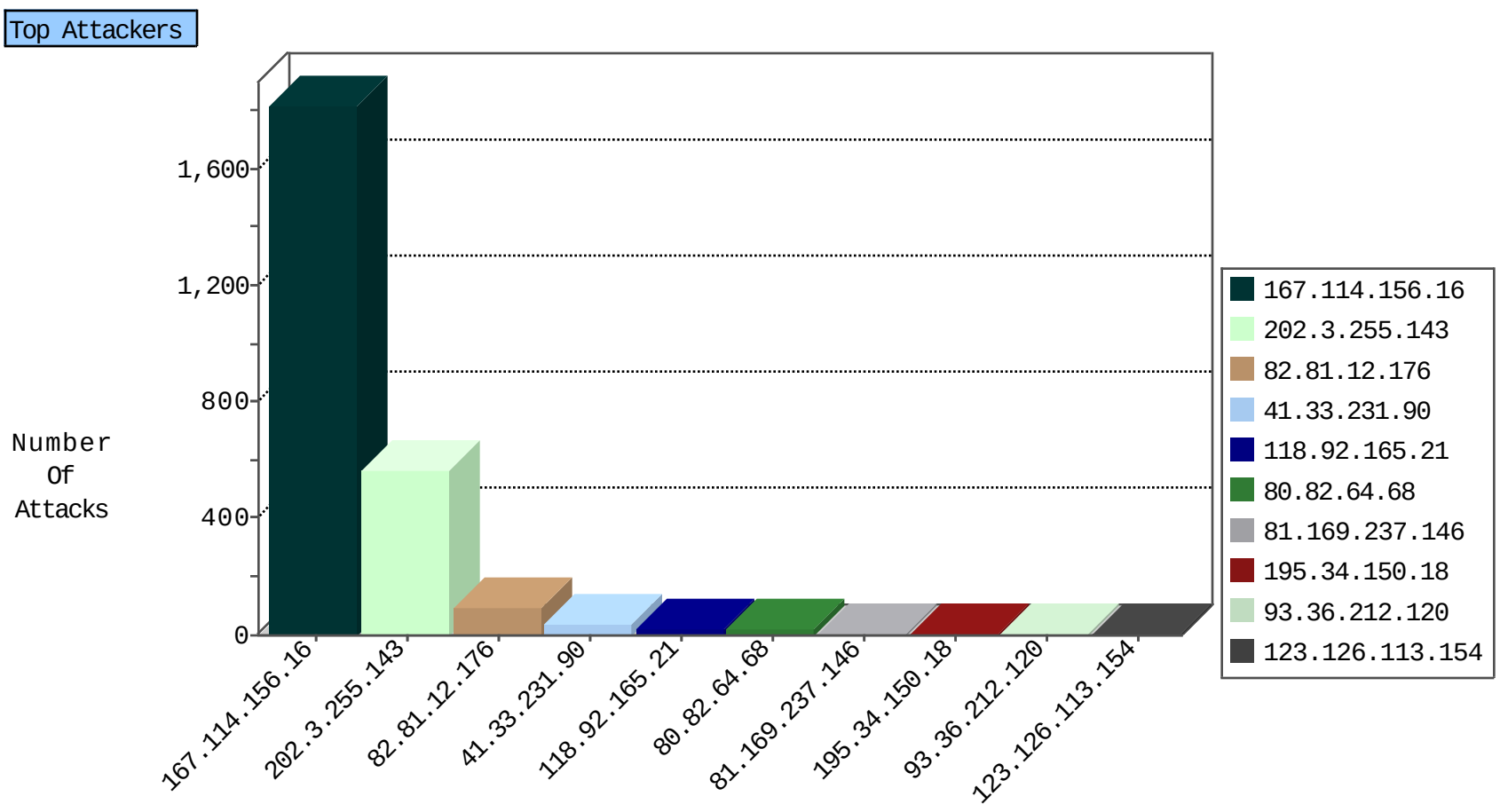
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-19-2016-01:06:48 to 01-19-2016-02:06:48

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	3016
66.249.78.79	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	415
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	96
185.130.5.231		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
89.46.102.242	Romania	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.210	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1

01-19-2016-01:06:48 to 01-19-2016-02:06:48

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	7
65.55.210.150	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.238	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-19-2016-01:06:48 to 01-19-2016-02:06:48

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	527
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
222.174.5.28	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.214.65.50	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
115.214.65.50	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
80.82.64.68	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
222.174.5.28	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.214.65.50	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1

01-19-2016-01:06:48 to 01-19-2016-02:06:48

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
118.92.165.21	New Zealand	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12
118.92.165.21	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.208.36.71	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
93.36.212.120	Italy	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.69.49.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.46.39.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
131.253.25.139	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.121.138.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.54.198	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.22.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.97.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.198	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	3
79.182.19.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.82.64.68	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
49.197.14.209	Australia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.82.64.68	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
37.75.215.122	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.172.173.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.22.131.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.76.109.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	2
185.3.147.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.193.111	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.80.155.130	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
80.82.64.68	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
192.254.250.164	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.82.64.68	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.171	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
128.232.110.28	United Kingdom	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
91.189.176.230	Norway	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
80.82.64.68	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
137.226.113.7	Germany	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.29.153.220	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
193.90.12.89	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.82.64.68	Netherlands	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.172	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.173.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
80.246.136.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
79.96.145.135	Poland	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
50.87.133.172	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
187.45.195.61	Brazil	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
208.80.155.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar	Block	2
93.172.173.131	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 93.172.173.131	Block	2
154.127.59.254	Mauritius	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
5.9.15.27	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
186.202.127.122	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
122.201.121.52	Australia	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
212.85.121.222	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
50.62.208.133	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	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
41.36.57.156	Egypt	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
187.45.193.205	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
89.161.198.15	Poland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
162.144.93.104	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
66.46.167.71	Canada	147.237.72.156	aman.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/1133-22461-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/1133-22638-he/dover.aspx.	Block	1
93.36.212.120	Italy	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
50.62.177.176	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
198.20.226.241	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
79.96.162.17	Poland	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
5.150.195.212	Sweden	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
186.202.127.122	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
122.201.121.52	Australia	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
213.201.31.253	Spain	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
207.46.13.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/17471.jpg	Block	1
94.136.40.100	United Kingdom	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
46.12.140.219	Greece	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
89.161.198.15	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
72.167.190.37	United States	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
162.247.72.199	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/navy/	Block	1
66.46.167.71	Canada	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
212.85.106.38	Poland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	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
93.157.99.179	Poland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
50.62.208.40	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
200.73.116.212	Chile	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
187.45.193.166	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
80.82.64.68	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to alemara1.org/wp-content/themes/akhbar24/images/alemarah.jpg	Block	1
5.196.184.4	France	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
154.44.190.8	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1