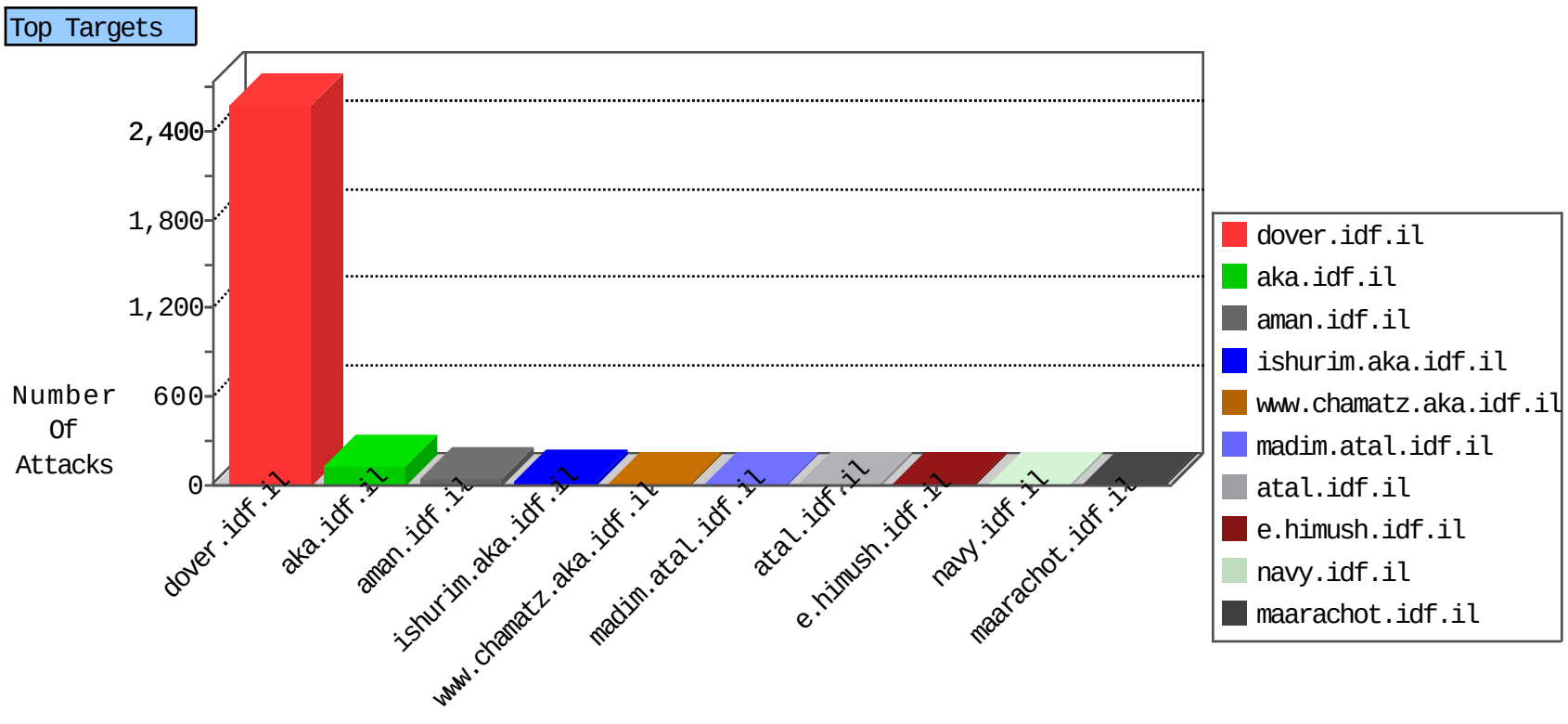
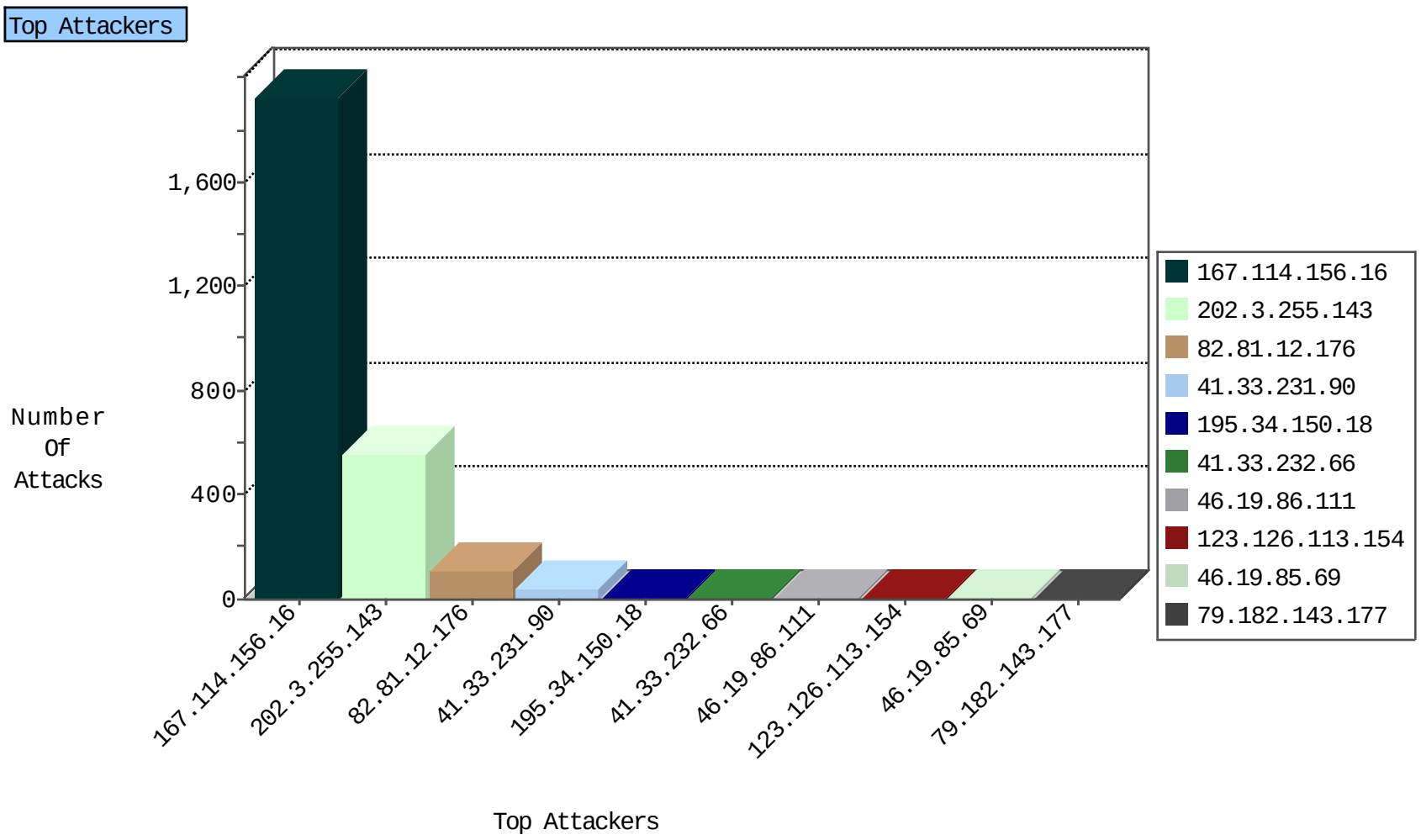
01-19-2016-02:04:05 to 01-19-2016-03:04:05

IDF Under Attack Daily Report





01-19-2016-02:04:05 to 01-19-2016-03:04:05

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	3125
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	108
74.91.28.59	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
191.188.95.73	Brazil	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
191.188.95.73	Brazil	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
104.233.70.144		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
64.94.101.246	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

01-19-2016-02:04:05 to 01-19-2016-03:04:05

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	5
136.243.103.165	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
62.210.152.89	France	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	2
188.165.15.231	France	147.237.76.30	himush.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
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-19-2016-02:04:05 to 01-19-2016-03:04:05

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	515
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	2
220.231.195.122	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
212.7.211.7	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.13.173	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.76.197	India	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
112.196.49.101	147.237.76.197	India	e.himush.idf.il	ET SCAN NMAP -f -sS	1
50.56.221.222	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
212.7.211.7	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
191.240.136.5	147.237.8.14	Brazil	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
125.227.64.115	147.237.76.197	Taiwan	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.76.197	India	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

01-19-2016-02:04:05 to 01-19-2016-03:04:05

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
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.86.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
177.135.3.3	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.182.143.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.43.222.224	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
180.76.15.140	China	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
5.22.131.59	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.26.148.186	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	2
72.188.6.213	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.30.250	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
54.176.17.88	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
180.76.15.33	China	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	1
131.253.26.232	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
191.240.136.5	Brazil	147.237.8.28	e.mobile-ks.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.169	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.22.131.59	Israel	147.237.77.216	dover.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
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
65.55.212.85	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
137.116.71.170	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.199.57.197	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
107.199.218.1	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.68	Netherlands	147.237.0.33	idf.il	drop		drop	1
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
65.55.218.50	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
183.250.126.146	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
137.116.71.170	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.230.89.51	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.30	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
168.187.173.4	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.28	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
207.46.13.84	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
185.3.147.107	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

01-19-2016-02:04:05 to 01-19-2016-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.21.147	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
187.45.195.15	Brazil	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	2
203.124.120.63	Singapore	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	2
119.18.157.130	Indonesia	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	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
37.59.49.14	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
195.74.38.67	Sweden	147.237.72.156	aman.idf.il	Distributed PHP Attempt	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
187.45.193.174	Brazil	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
86.106.93.200	Romania	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
72.29.67.54	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
213.251.182.107	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
162.144.48.184	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
112.111.184.126	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/trackback/	Block	1
50.62.208.52	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
198.20.226.241	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
93.157.99.179	Poland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
5.135.120.96	France	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
190.95.243.229	Ecuador	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=e9a7b6c5kkkkkkk_e9a7b6c5	Block	1
73.229.228.15	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
150.70.173.45	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	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
37.187.25.49	France	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
195.74.38.67	Sweden	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.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
89.161.132.102	Poland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
72.167.190.37	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
216.172.164.165	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
162.144.78.190	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
113.11.250.192	Singapore	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
50.62.208.133	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
198.20.226.241	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
93.157.99.179	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
14.1.194.250	Malaysia	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
190.95.243.229	Ecuador	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
185.61.152.8	United Kingdom	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
77.66.80.25	Denmark	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/1133-22638-he/dover.aspx.	Block	1
150.70.173.45	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
37.187.25.49	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
195.74.38.173	Sweden	147.237.72.167	ishurim.aka.idf.i	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
89.161.132.102	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
187.45.195.184	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
72.167.190.37	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
216.172.164.165	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1

01-19-2016-02:04:05 to 01-19-2016-03:04:05