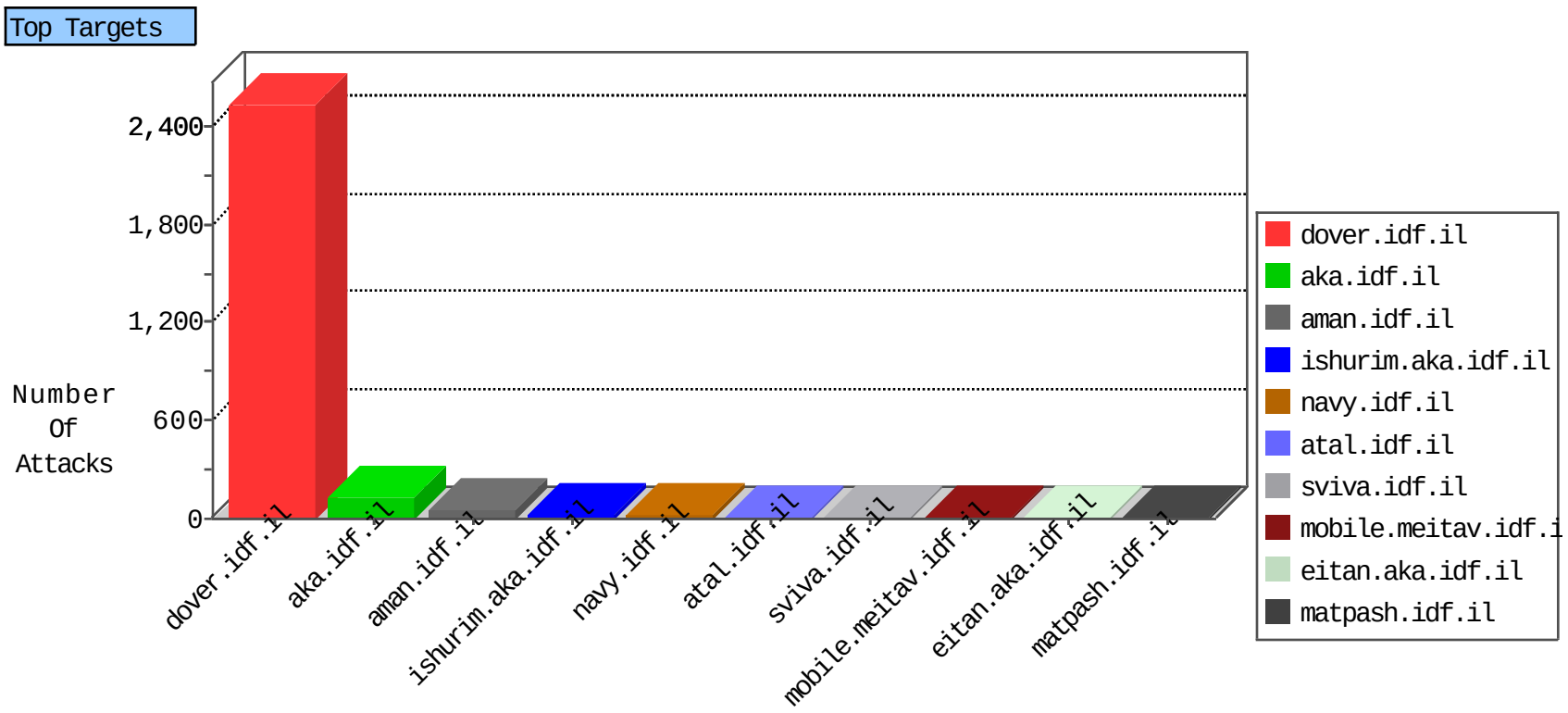
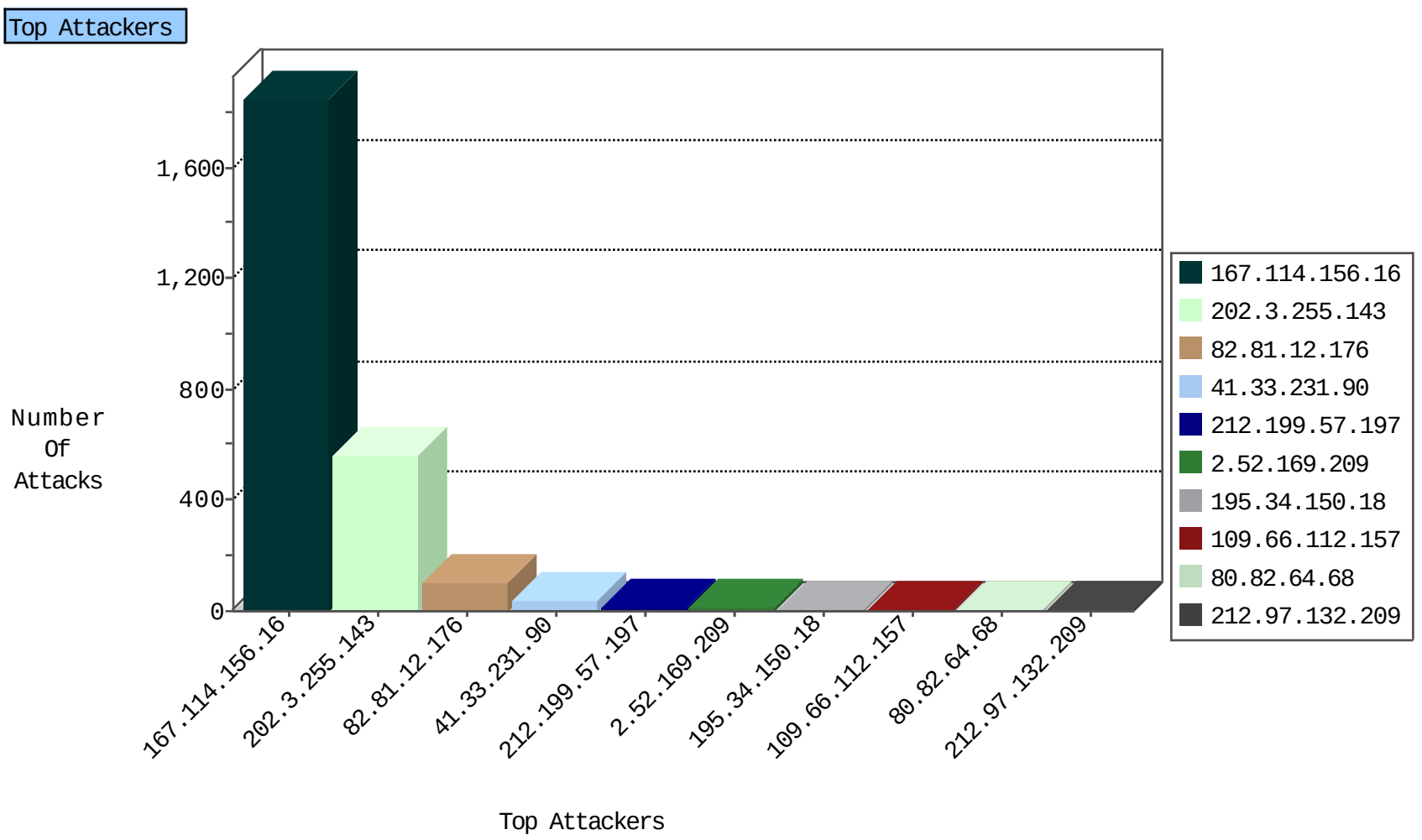
01-19-2016-03:04:08 to 01-19-2016-04:04:08

IDF Under Attack Daily Report





01-19-2016-03:04:08 to 01-19-2016-04:04:08

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	3058
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	98
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	3
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
204.42.253.130	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	2
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.213	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1

01-19-2016-03:04:08 to 01-19-2016-04:04:08

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
62.210.152.89	France	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
91.121.221.15	France	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	2
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
91.121.221.15	France	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
176.9.131.69	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-19-2016-03:04:08 to 01-19-2016-04:04:08

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	522
212.199.57.197	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
212.199.57.197	147.237.0.19	Israel	madim.atal.idf.i	ET SCAN NMAP -sA (2)	2
193.201.227.7	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
168.62.238.153	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
162.13.88.58	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
103.23.21.188	147.237.76.176	Indonesia	test.ncore.idf.i	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
60.209.5.30	147.237.77.233	China	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.80.29.56	147.237.0.33	Vietnam	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
168.62.238.153	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
60.209.5.30	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-19-2016-03:04:08 to 01-19-2016-04:04:08

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	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.52.169.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.127.127.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
51.255.203.33	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.253	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.121.30.34	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
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	4
66.249.78.144	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.66.112.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3
109.66.112.157	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.82.64.68	Netherlands	147.237.77.235	sviva.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
91.200.12.141	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
68.180.228.112	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.194.135.73	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
93.77.123.87	Ukraine	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
128.194.135.73	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
207.46.13.88	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.225	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
128.232.110.28	United Kingdom	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
52.28.32.164	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
191.240.136.5	Brazil	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.31.77.242	Czech Republic	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.86	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
141.212.122.168	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
96.244.6.252	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
191.240.136.5	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.25.217.80	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.68	Netherlands	147.237.77.235	sviva.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
128.232.110.28	United Kingdom	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
52.28.32.164	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
193.90.12.89	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
31.162.199.206	Russian Federation	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
185.10.71.107	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.168	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.109.139.87	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
212.117.180.21	Luxembourg	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
108.168.185.134	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
191.240.136.5	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.131.109	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

01-19-2016-03:04:08 to 01-19-2016-04:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.97.132.209	Denmark	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.97.132.209	Block	5
50.62.208.133	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	2
37.142.242.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.143.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
195.74.38.121	Sweden	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
98.248.142.92	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
89.163.146.245	Germany	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
185.43.220.10	Czech Republic	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
8.37.70.44	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/dover.aspx&usg=alkjrhh6gcky1tkzmfmq9gekred5gvg8jq	Block	1
142.4.7.164	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
109.66.112.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
198.15.125.34	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
46.117.136.154	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
187.45.195.133	Brazil	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
94.23.24.84	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
216.172.189.171	United States	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
179.188.17.23	Brazil	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
88.214.162.145	Portugal	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
72.167.190.33	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	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
112.78.4.244	Vietnam	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
98.248.142.92	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
195.74.38.121	Sweden	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
89.163.146.245	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
37.187.25.49	France	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
186.202.153.13	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
8.37.70.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/dover.aspx&usg=alkjrhh3k-fndgqbbjcxcdjpvxkc8bwg7w	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/requests/	Block	1
79.172.211.136	Hungary	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
212.97.132.209	Denmark	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
109.163.234.8	Romania	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 147.237.76.42/994-9738-he/refuah.aspx	Block	1
198.20.226.241	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
46.232.178.12	Switzerland	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
187.45.195.184	Brazil	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
94.23.58.222	France	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
89.161.195.181	Poland	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
14.1.194.250	Malaysia	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
182.50.155.2	Singapore	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
72.167.190.172	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
212.85.106.38	Poland	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
128.194.135.73	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	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
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20420-he/dover.aspx	Block	1
198.1.79.36	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 PHP Attempt	Block	1

01-19-2016-03:04:08 to 01-19-2016-04:04:08