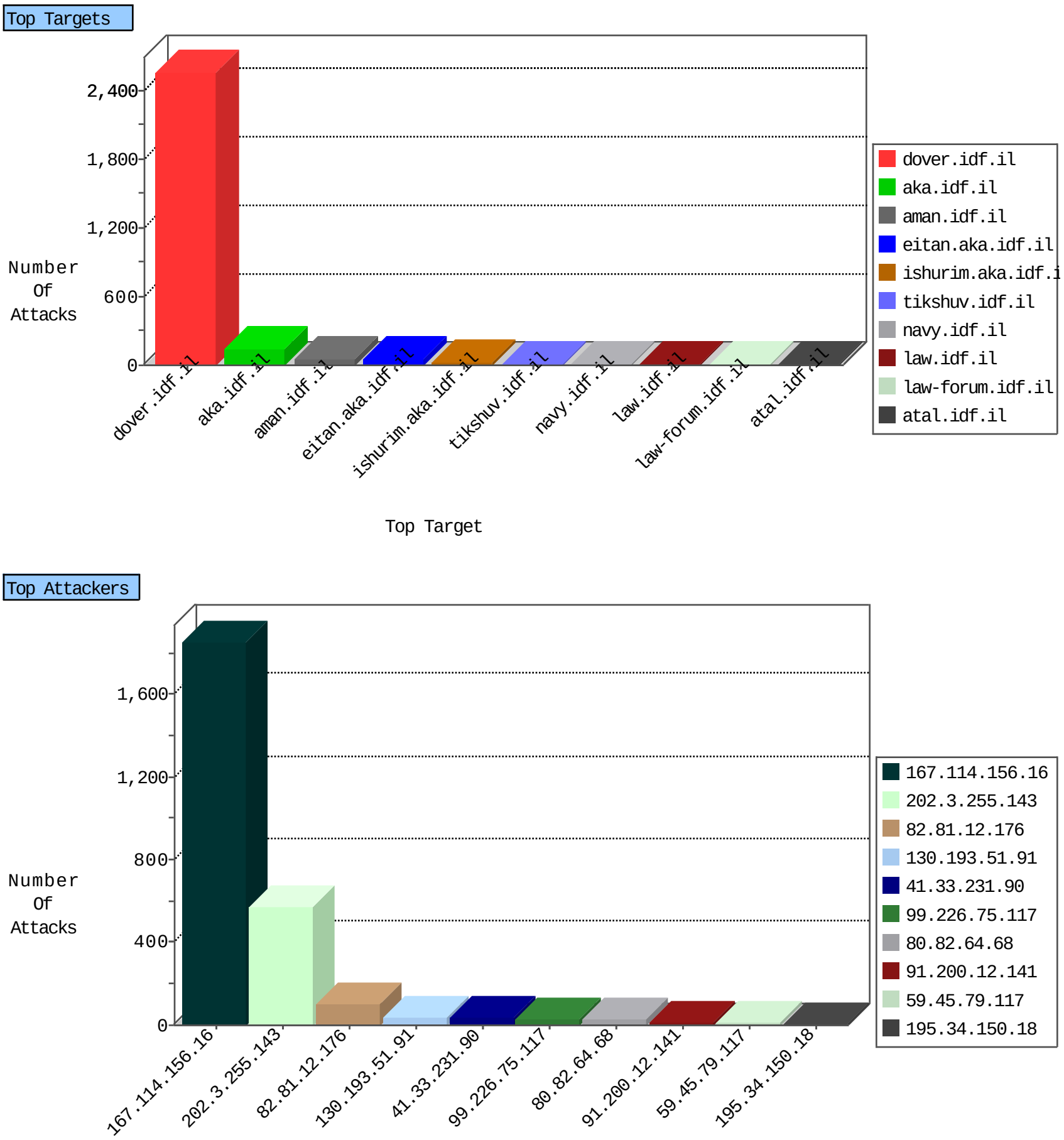
01-19-2016-04:04:09 to 01-19-2016-05:04:09

IDF Under Attack Daily Report



01-19-2016-04:04:09 to 01-19-2016-05:04:09

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	3060
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	100
222.186.55.242	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
188.138.17.205	France	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
82.221.105.7	Iceland	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1

01-19-2016-04:04:09 to 01-19-2016-05:04:09

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
69.30.215.130	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
77.248.252.113	Netherlands	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	2
144.76.8.132	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
77.248.252.113	Netherlands	147.237.77.216	dover.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
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

01-19-2016-04:04:09 to 01-19-2016-05:04:09

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	531
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.92	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
108.61.228.100	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.0.15		kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
162.13.88.58	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.8.45	India	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.8.14	India	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.0.34	India	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.0.15	India	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.76.44		e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
200.75.86.68	147.237.0.19	Colombia	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
163.172.13.173	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.8.46	India	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.0.200	India	m4u.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
114.79.169.197	147.237.0.19	India	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

01-19-2016-04:04:09 to 01-19-2016-05:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
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	39
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
99.226.75.117	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
91.200.12.141	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
103.5.3.236	Philippines	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
154.121.5.230	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.82.64.68	Netherlands	147.237.77.19	law-forum.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
80.82.64.68	Netherlands	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
2.54.168.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.190.233	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	147.237.77.74	law.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.235	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.93.91.84	Germany	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.148.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.138	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.235	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
154.121.5.230	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.82.64.68	Netherlands	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
184.105.139.96	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.168	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.28	United Kingdom	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.64.68	Netherlands	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
154.121.5.230	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
80.82.64.68	Netherlands	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.76.34	yohalan.idf.il	drop		drop	1
42.99.164.100	Japan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
184.105.139.118	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.64.68	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.169	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.28	United Kingdom	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.154.146.225	France	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
80.82.64.68	Netherlands	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.74	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.64.68	Netherlands	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
42.99.164.100	Japan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
184.105.247.200	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.64.68	Netherlands	147.237.77.19	law-forum.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

01-19-2016-04:04:09 to 01-19-2016-05:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	2
187.45.195.61	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	2
122.201.121.52	Australia	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
187.45.195.61	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
198.57.194.238	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
184.168.192.107	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
37.187.25.49	France	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
195.154.146.225	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-trackback.php	Block	1
5.9.60.113	Germany	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
192.99.39.185	Canada	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-login.php	Block	1
99.226.75.117	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
217.149.52.105	Finland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
186.202.127.85	Brazil	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
80.82.64.68	Netherlands	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to alemara1.org/wp-content/themes/akhbar24/images/alemarah.jpg	Block	1
207.46.13.30	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
198.1.81.235	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
173.254.203.80	United States	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
5.196.98.204	Spain	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
195.74.38.98	Sweden	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
117.103.185.20	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
89.218.26.108	Kazakstan	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
212.85.121.222	Poland	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
184.168.192.107	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
69.195.124.97	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
199.244.88.182	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/headerupper/	Block	1
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
196.11.102.215	South Africa	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
5.149.139.125	Belgium	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
192.99.98.54	Canada	147.237.72.167	ishurim.aka.idf.i	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
186.202.127.85	Brazil	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
80.82.64.68	Netherlands	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to alemara1.org/wp-content/themes/akhbar24/images/alemarah.jpg	Block	1
207.46.13.88	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
198.1.81.235	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
173.254.203.80	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-login.php	Block	1
119.18.157.130	Indonesia	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
8.37.70.99	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19137-en/dover.aspx&usg=alkjrhise4ts0rahecdzxxuwcfyraizdkg	Block	1
195.138.85.250	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/sendtofriend.aspx?&amp	Block	1
94.23.24.84	France	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
213.251.182.102	France	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
187.45.240.114	Brazil	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
184.168.192.163	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
72.167.190.33	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
199.244.88.182	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
154.44.190.8	United States	147.237.72.167	ishurim.aka.idf.i	Distributed PHP Attempt	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1

01-19-2016-04:04:09 to 01-19-2016-05:04:09