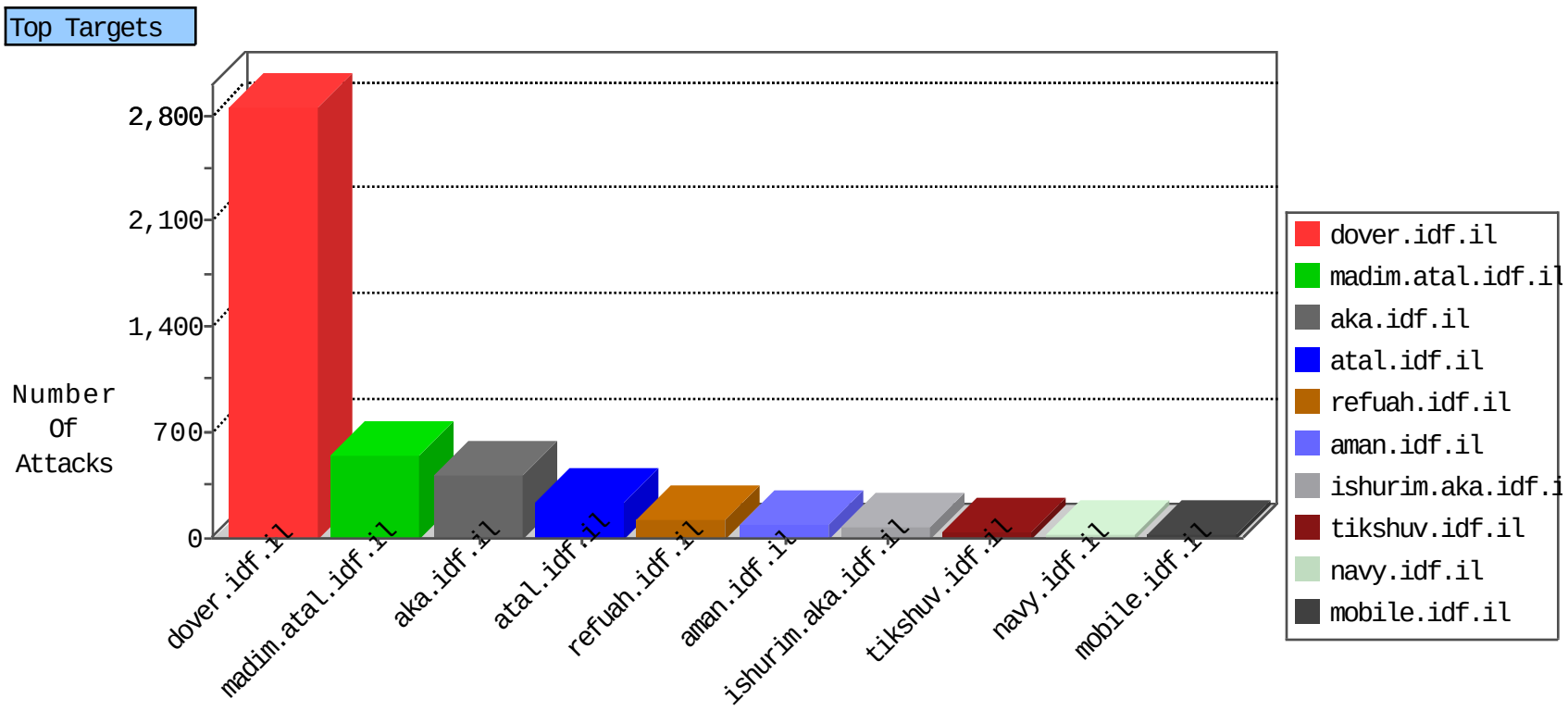
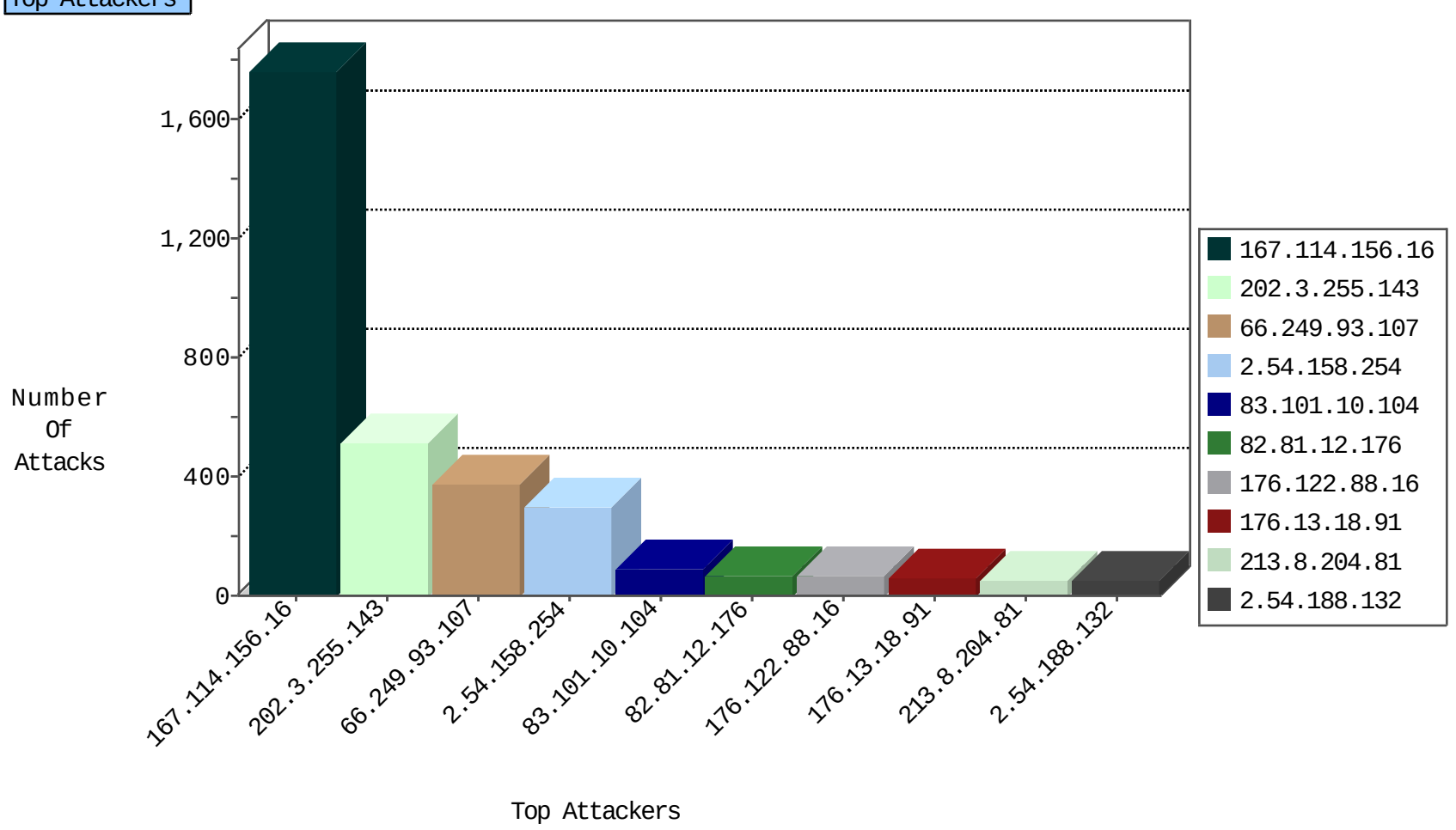
01-18-2016-22:04:07 to 01-18-2016-23:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-18-2016-22:04:07 to 01-18-2016-23:04:07

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	3036
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	69
66.249.64.92	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.35.62.85	Switzerland	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
115.238.209.209	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.207	Switzerland	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.163	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
74.91.28.60	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1

01-18-2016-22:04:07 to 01-18-2016-23:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.179	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
84.108.5.155	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
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

01-18-2016-22:04:07 to 01-18-2016-23:04:07

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	469
66.249.93.107	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	371
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
191.240.136.5	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.228.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.171.23.126	147.237.76.198	Vietnam	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
95.86.124.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
73.51.133.22	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
50.97.146.246	147.237.72.156	United States	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
201.172.81.23	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
191.240.136.5	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.13.173	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	1
113.171.23.126	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.67.205.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
73.51.133.22	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 3072	1
37.142.68.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-18-2016-22:04:07 to 01-18-2016-23:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.122.88.16	Ukraine	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	66
83.101.10.104	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	46
83.101.10.104	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	46
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
31.154.154.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
89.139.233.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
213.8.204.64	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	23
185.89.217.228		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	22
185.89.217.235		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
141.0.13.176	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.167	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
41.249.240.151	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
185.89.217.230		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
185.89.217.234		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
185.89.217.233		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
109.66.201.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.115.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.36	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.155.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.89.217.225		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
185.32.179.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.115.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
185.89.217.231		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.232		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.229		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
23.241.91.142	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
79.180.32.188	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
185.89.217.224		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
185.89.217.231		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
185.89.217.227		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
217.132.243.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.89.217.226		147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
185.89.217.228		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.46	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
79.179.195.46	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.89.217.235		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.233		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
84.108.206.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.67.34.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.102.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.229		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.227		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.234		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.186	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.182.26.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.134.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

01-18-2016-22:04:07 to 01-18-2016-23:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.158.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	139
2.54.158.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
176.13.18.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
213.8.204.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
2.54.188.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.206.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.54.158.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	43
176.13.2.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.52.141.126	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.141.126	Block	11
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.80.196.44	Block	5
85.64.151.138	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 85.64.151.138	Block	4
85.64.151.138	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 85.64.151.138	Block	4
84.109.19.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.30.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.65.149.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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	2
93.173.228.5	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 93.173.228.5	None	2
79.181.5.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
85.250.235.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
2.54.36.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.181.49.85	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
84.108.187.127	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
84.228.75.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
179.188.17.23	Brazil	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
195.74.38.98	Sweden	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	2
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	2
122.201.121.52	Australia	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
5.196.184.4	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
186.202.153.163	Brazil	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
74.91.28.60	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.tgobet.com/	Block	1
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/107170.pdf	Block	1
208.109.236.182	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
5.22.129.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
177.106.167.5	Brazil	147.237.76.86	navy.idf.il	Malformed URL dÂ±[[#27]]"Â?×£Â½â€°Ö¶Â´×š[[#1]]×¦u[[#16]]hÂŒi6zÂ¡![[#4]]Â¨×±5Â?Â¿[[#23]]ÂžÂµ×ž×˜[[#31]]â€¦Ã™×'Â-×•Â´z[[#14]][[#8]]Ã—â€¹[k^l•Ã¼Ö¹q×£Â·ÃŠ-qcË†×'pn6Â¼[[#28]]Â»v<va	Block	1
82.80.57.228	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
174.136.25.169	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
46.120.28.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
92.53.96.78	Russian Federation	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
198.20.230.169	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
79.179.10.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
162.144.75.80	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
37.122.211.142	United Kingdom	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
89.42.110.10	Romania	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
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	1
5.150.195.212	Sweden	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
84.228.171.38	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
185.32.179.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.209	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	1

01-18-2016-22:04:07 to 01-18-2016-23:04:07