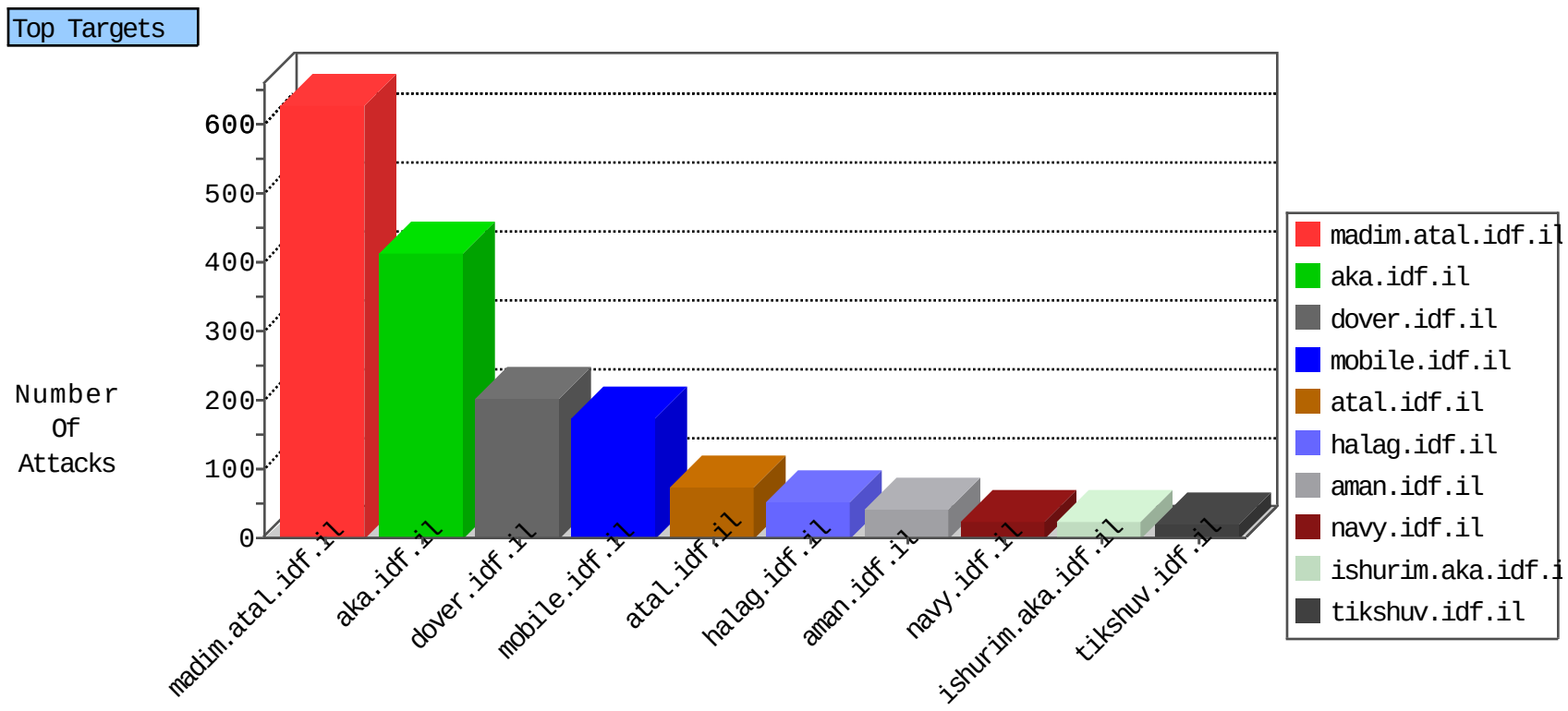
01-28-2016-17:04:03 to 01-28-2016-18:04:03

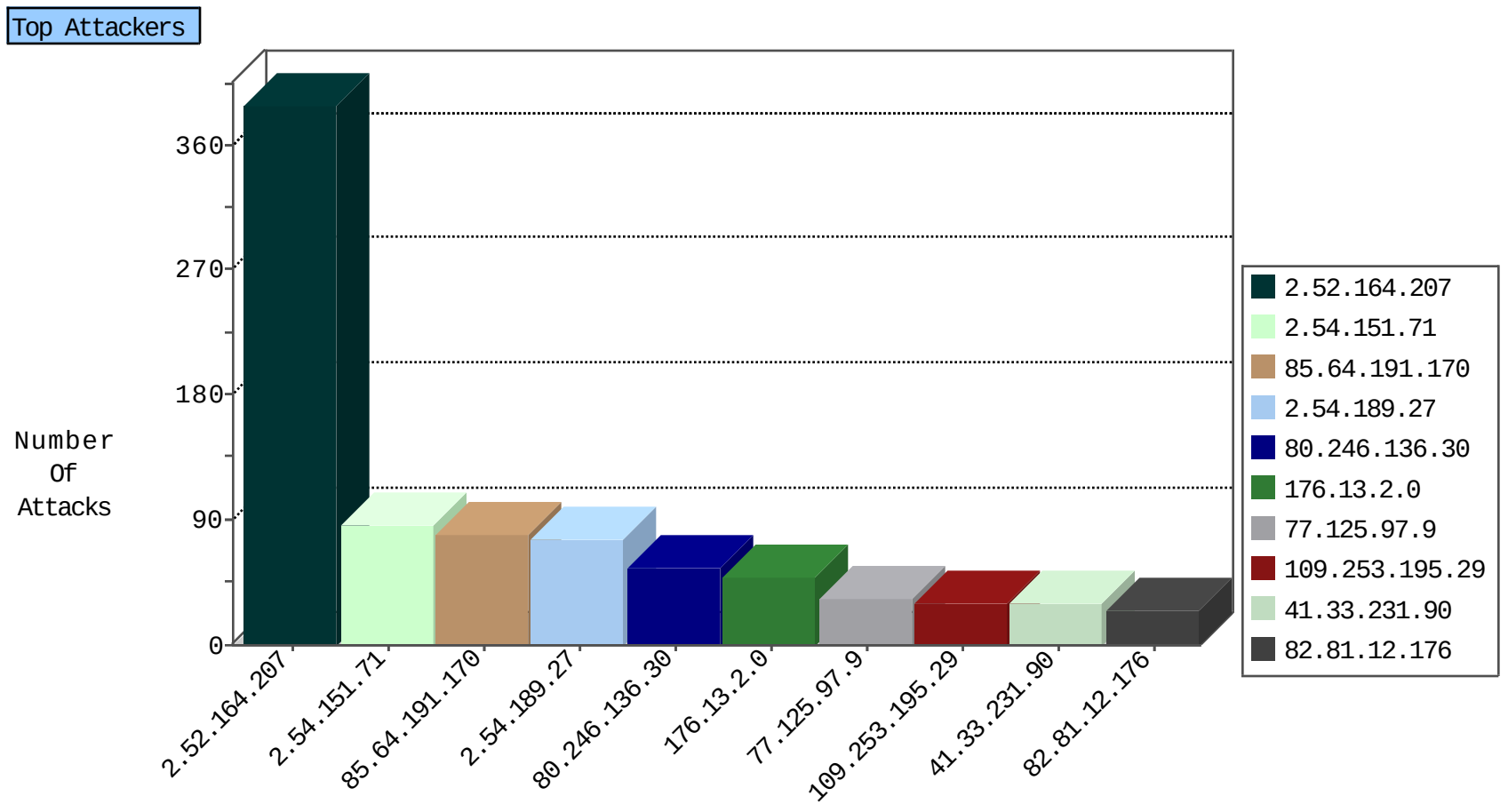
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-28-2016-17:04:03 to 01-28-2016-18:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	24
109.67.179.166	Israel	147.237.76.86	navy.idf.il	L4 Source or Dest Port Zero	drop	9
109.67.179.166	Israel	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
183.60.48.25	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
108.59.4.197	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
108.59.4.197	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
108.59.4.197	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
108.59.4.197	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
108.59.4.197	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
108.59.4.197	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

01-28-2016-17:04:03 to 01-28-2016-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.236.201.28		147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	12
212.225.165.62	Spain	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	2
123.149.205.53	China	147.237.72.166	aka.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1

01-28-2016-17:04:03 to 01-28-2016-18:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
104.236.201.28	147.237.72.166		aka.idf.il	Tehila - Perl LWP with fake user agent	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.64.102	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
84.229.249.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.64.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.178	Sweden	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.51.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
172.98.200.237	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
40.122.124.70	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.154.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.183.51.251	147.237.77.170	Switzerland	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.126.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
83.228.71.58	147.237.77.216	Bulgaria	dover.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.187	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
59.189.161.117	147.237.0.34	Singapore	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.105.134.220	147.237.77.234	Sweden	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.182.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.255.168.17	147.237.72.166	Czech Republic	aka.idf.il	portscan: TCP Distributed Portscan	1
40.122.124.70	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
149.88.14.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.206.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.216.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.24.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.183.51.251	147.237.77.234	Switzerland	halag.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.139.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.77.233	Ukraine	atal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

01-28-2016-17:04:03 to 01-28-2016-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.2.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
77.125.97.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.13.4.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.195.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.156.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.217	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
109.253.139.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
31.168.216.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.18.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.22.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.164.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.147.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.154.150.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
2.54.189.27	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
164.138.121.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.54.189.27	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.189.27	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
2.54.189.27	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.54.189.27	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
176.13.10.156	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
89.139.154.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.10.156	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
147.235.8.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
147.235.8.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
31.154.150.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
109.67.38.37	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.192.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.165.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.129.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.51.212	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.172.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.195.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.189.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.125.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.100	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.189.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.186.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.154.157.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.189.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
31.154.157.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

01-28-2016-17:04:03 to 01-28-2016-18:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.164.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	215
2.52.164.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
2.54.151.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
85.64.191.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
80.246.136.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
2.52.164.207	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.52.164.207	Block	48
2.54.191.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
213.111.233.25	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
109.253.156.203	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
213.111.233.25	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.111.233.25	Block	5
109.186.150.125	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
95.86.70.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.183.118.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
164.138.121.176	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.177.170.249	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
109.253.139.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.1.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.64.200.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.139.154.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.154.94.10	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	2
176.13.2.0	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.210.186.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.136.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.3.144.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMai in www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	None	1
46.19.85.14	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
149.88.39.82	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.126.98.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.69.87	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-he	Block	1
208.115.111.74	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to chimush.atal.idf.il/templates/news/null	Block	1
87.69.14.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.0.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
109.253.141.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
2.54.145.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
105.157.18.69	Morocco	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
46.120.182.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.111.233.25	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
46.19.85.14	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method ;q=0.6,en;q=0.4 in URL	Block	1
81.218.48.37	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/resource/userfollowresource/create/	Block	1
157.55.39.10	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.176.10.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1444-he/atal.aspx	Block	1
109.66.28.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-28-2016-17:04:03 to 01-28-2016-18:04:03