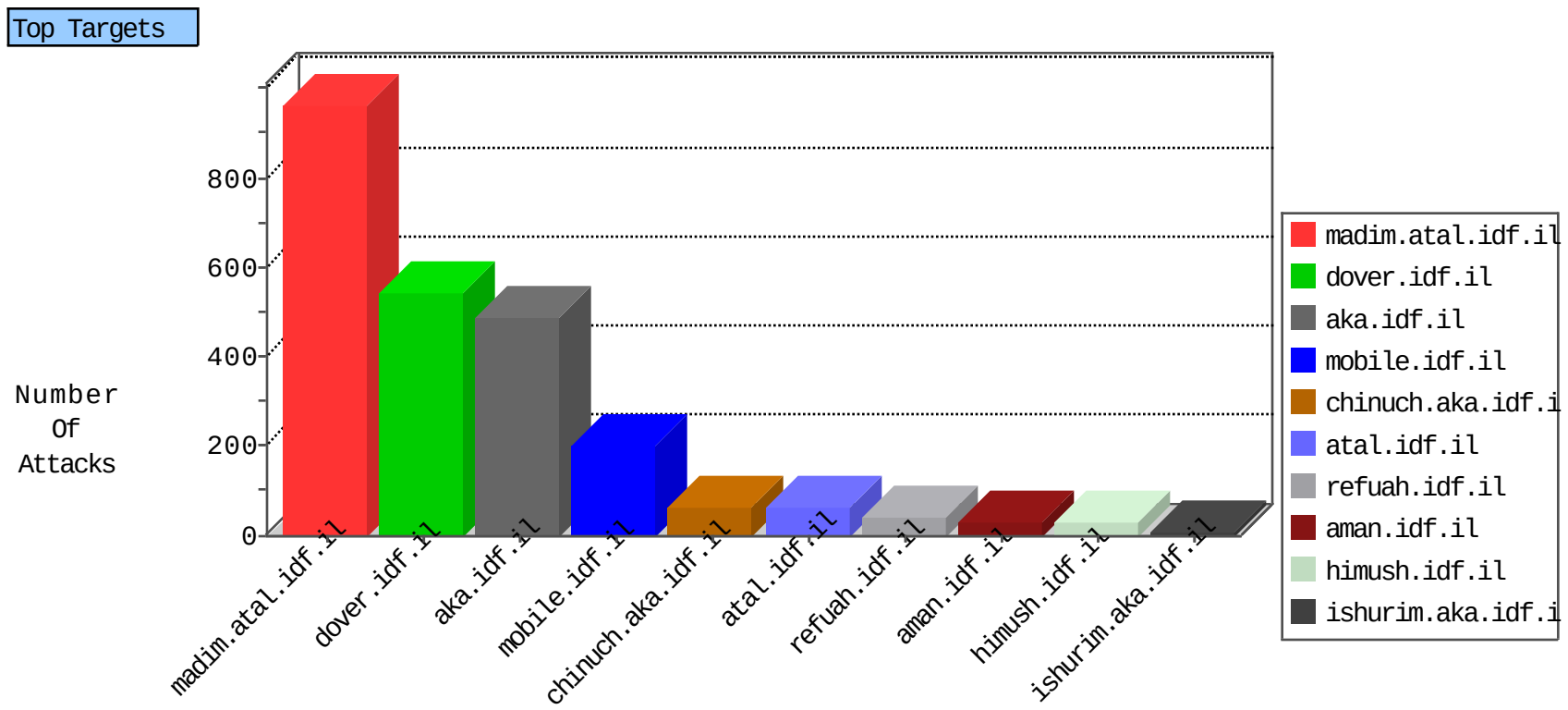
01-26-2016-22:04:04 to 01-26-2016-23:04:04

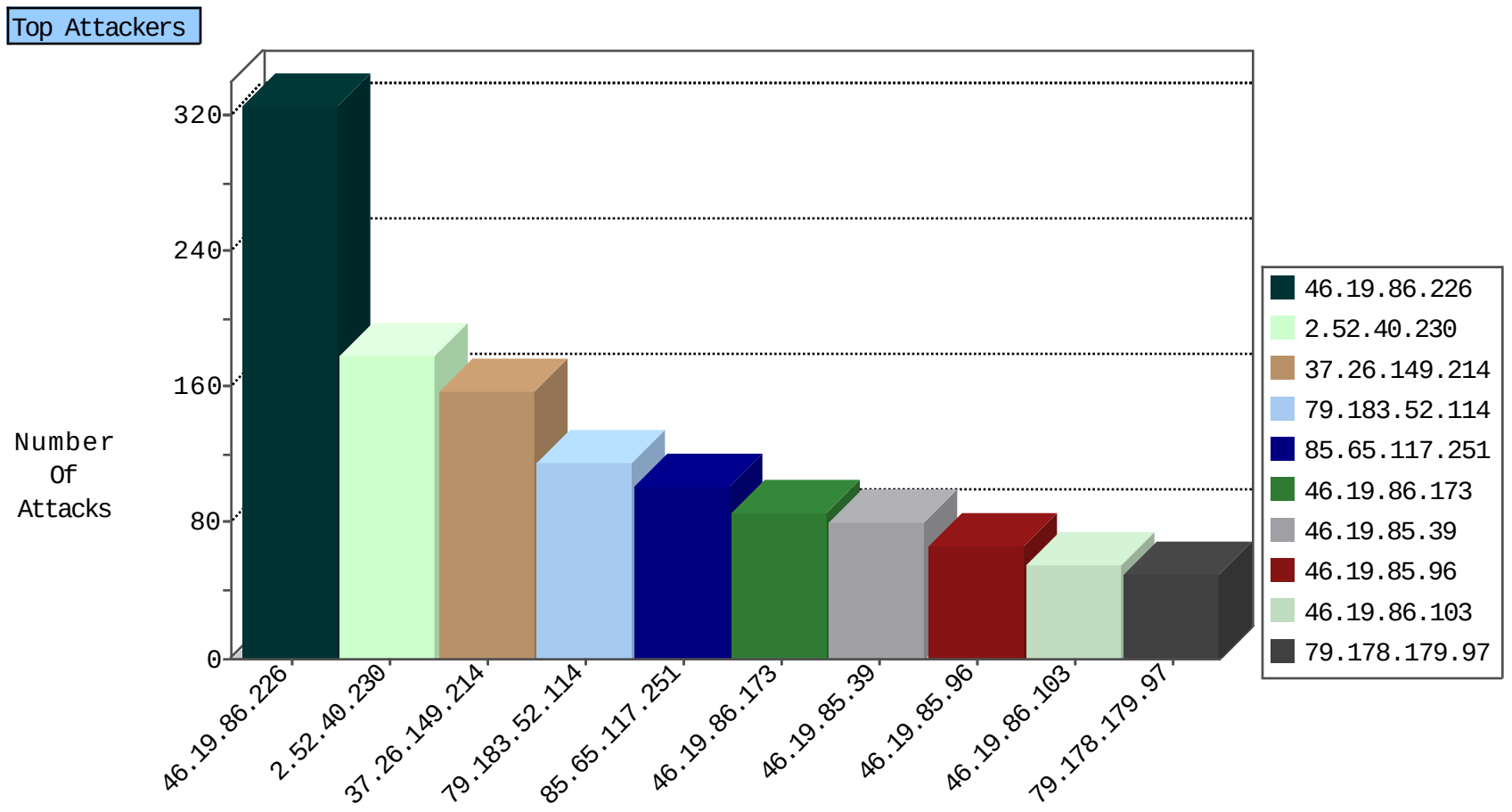
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-26-2016-22:04:04 to 01-26-2016-23:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
181.228.123.107	Argentina	147.237.72.166	aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
89.163.132.132	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
23.239.64.15	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
89.163.132.132	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
89.163.132.132	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
89.163.132.132	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
113.163.32.60	Vietnam	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
89.163.132.132	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
23.239.64.15	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
113.163.32.60	Vietnam	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
89.163.132.132	Germany	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

01-26-2016-22:04:04 to 01-26-2016-23:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.97	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

01-26-2016-22:04:04 to 01-26-2016-23:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.225	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
111.50.66.45	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
85.250.248.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	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
61.244.49.137	147.237.0.35	Hong Kong	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
199.203.240.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
190.124.35.115	147.237.77.235	Nicaragua	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
46.121.87.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
190.124.35.115	147.237.77.235	Nicaragua	sviva.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.65.9.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
84.229.134.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
79.180.197.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
212.252.193.52	147.237.77.212	Turkey	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.0.17	Hong Kong	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
190.124.35.115	147.237.77.235	Nicaragua	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
180.150.177.188	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.8.45	United Kingdom	e.eitan.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

01-26-2016-22:04:04 to 01-26-2016-23:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	53
37.26.149.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	53
37.26.149.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	52
46.19.85.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
109.67.148.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.86.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
79.178.179.97	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
46.19.85.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
46.19.85.96	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
149.78.18.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.130.225	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
85.64.56.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.228	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.176.166.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.96	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
80.246.130.225	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
84.228.15.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.96	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
2.52.179.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.96	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.96	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
46.19.85.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.120.125.32		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.210.186.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.96	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.187.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.50.93	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.142.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.178.179.97	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.166.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.230	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
95.86.102.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

01-26-2016-22:04:04 to 01-26-2016-23:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	176
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	147
79.183.52.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
2.52.40.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
85.65.117.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.86.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
2.52.40.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	75
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
82.81.65.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
2.54.49.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.54.45.231	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	29
85.65.117.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.86.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
109.253.221.26	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	8
77.127.78.27	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 77.127.78.27	None	8
213.57.176.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.32.179.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.229.134.91	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.229.134.91	Block	6
176.13.21.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.229.134.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
46.19.86.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.97.16	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 95.86.97.16	Block	3
2.54.45.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.102.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.60.103	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
95.86.102.6	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 95.86.102.6	Block	2
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.18.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.125.140.97	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
95.86.102.6	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
66.220.158.106	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.108.17.226	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.86.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.78.180.75	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
109.64.165.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.175.61	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
31.13.102.109	Ireland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.142.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
95.86.97.16	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.78.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
41.199.130.230	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
109.253.220.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.78.27	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding uQ1M1.yl^AXO	None	1
5.29.78.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl40$ctl07$ctl03$ddlQuestion in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
95.86.105.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

01-26-2016-22:04:04 to 01-26-2016-23:04:04