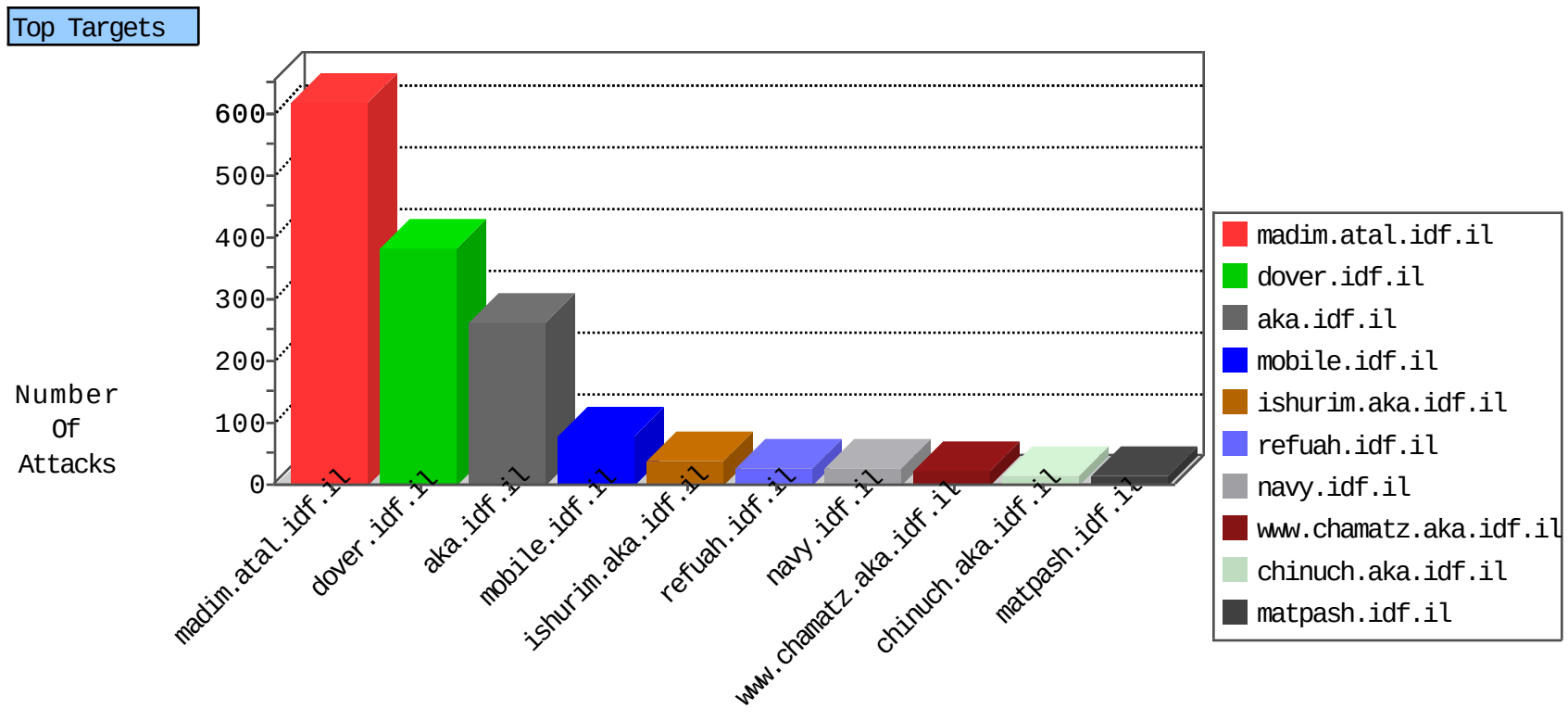
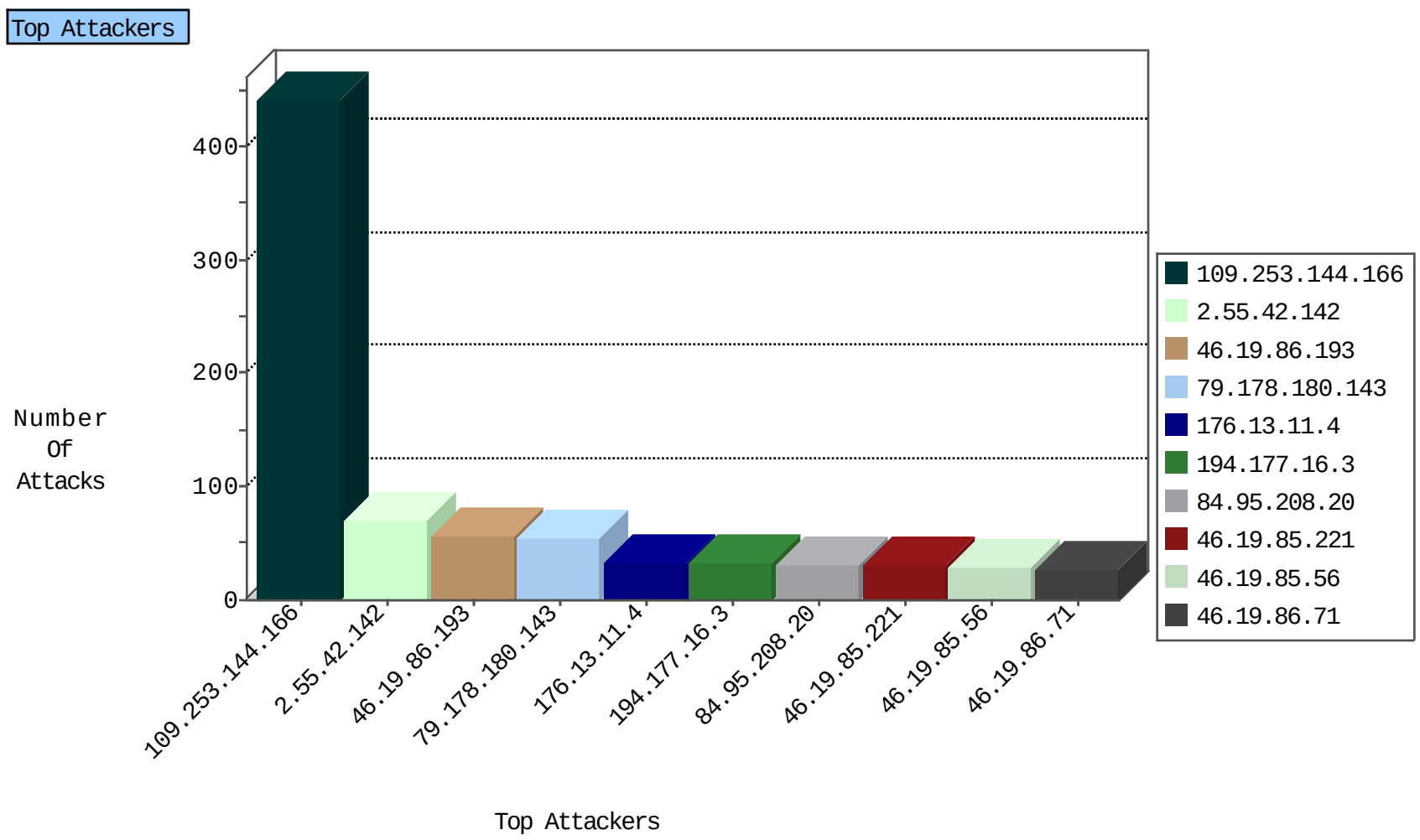
09-29-2016-10:04:07 to 09-29-2016-11:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-29-2016-10:04:07 to 09-29-2016-11:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
147.235.236.1	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	117
147.235.236.1	Israel	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	67
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	50
46.19.85.48	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
79.178.180.143	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.19.85.56	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.19.86.71	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
46.19.85.26	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.44.110.12	United States	147.237.76.200	eitan.aka.idf.i	Black List	drop	1
120.25.220.47	China	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-29-2016-10:04:07 to 09-29-2016-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.154.239.69	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
144.76.29.162	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-29-2016-10:04:07 to 09-29-2016-11:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.110.132.201	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
37.46.41.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.134.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.207.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.6.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.157.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.74.103.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.37.129.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.117.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.212.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.91.21	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
188.113.161.19	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.72.166	Ukraine	aka.idf.il	ET SCAN Potential SSH Scan	1
31.154.9.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.197.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.180.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.111.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.115.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.0.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.44.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.200.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.49.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.58.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.113.161.19	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.13.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.153.198.249	147.237.72.14		dover.idf.il(old)	ET SCAN Potential SSH Scan	1
46.19.86.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-29-2016-10:04:07 to 09-29-2016-11:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.180.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	32
46.19.85.221	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
2.55.27.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
62.0.203.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
147.236.113.13	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.147.229	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.86.20	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
207.232.28.110	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
80.246.137.107	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.166.186.249	Netherlands	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
62.0.197.105	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.20	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.12.160.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
62.219.225.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.94.199.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
212.179.21.194	Israel	147.237.8.27	e.madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.15.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.55.142.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.178.180.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.148	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.71	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
46.19.85.175	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	5
79.178.180.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.132.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.210.180.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
80.179.40.62	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
62.0.221.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.197.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.108.43.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.0.197.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.224.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.170.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

09-29-2016-10:04:07 to 09-29-2016-11:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.144.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	442
2.55.42.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
46.19.86.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
176.13.11.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
185.3.147.205	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	15
37.26.149.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
176.13.238.47	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	4
46.19.86.238	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	3
37.26.148.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
62.90.255.56	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
80.246.137.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.202.114	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
124.170.209.173	Australia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
2.53.180.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	2
109.253.145.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
176.13.243.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9711-he/refuah.aspx	Block	1
109.253.201.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
37.26.149.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.142	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/global.js	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.93.87	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/2796.jpg	Block	1
84.111.233.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dover.aspx	Block	1
213.151.48.138	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
194.90.200.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/scrollstrech.gif	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
10.30.10.166	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
176.13.17.58	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/60931.pdf	Block	1
62.90.255.56	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
213.8.204.72	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
2.53.61.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Method 6&[[#30]]§×ÞyÚMýÔæÉÙáXdwæÎ#³—ï–'[[#19]]ÿ[[#25]]°œÚL<Nm69QBS;}ü°	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2065-he/cogat.aspx	Block	1
66.249.66.238	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/m/	Block	1
94.244.90.230	Lithuania	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.118.19	Block	1

09-29-2016-10:04:07 to 09-29-2016-11:04:07