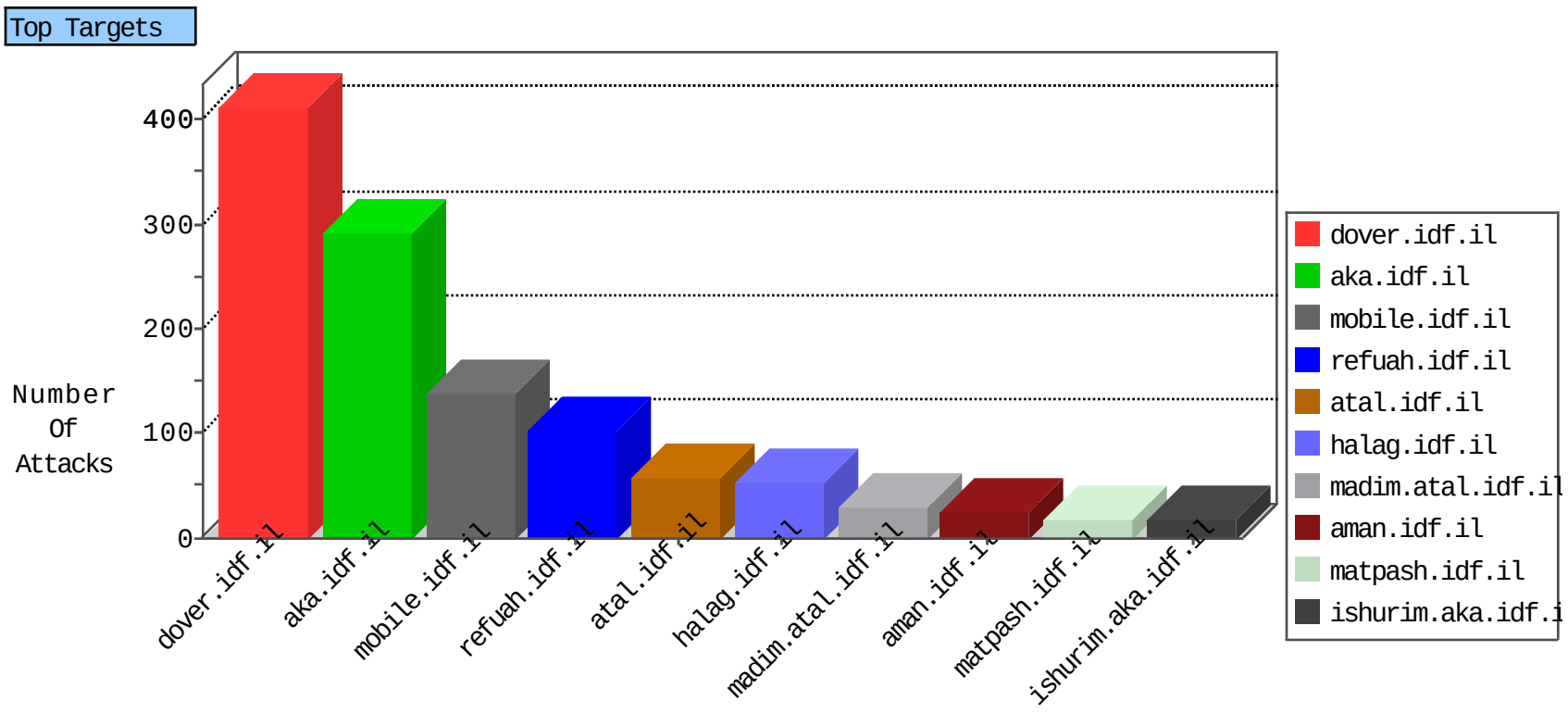
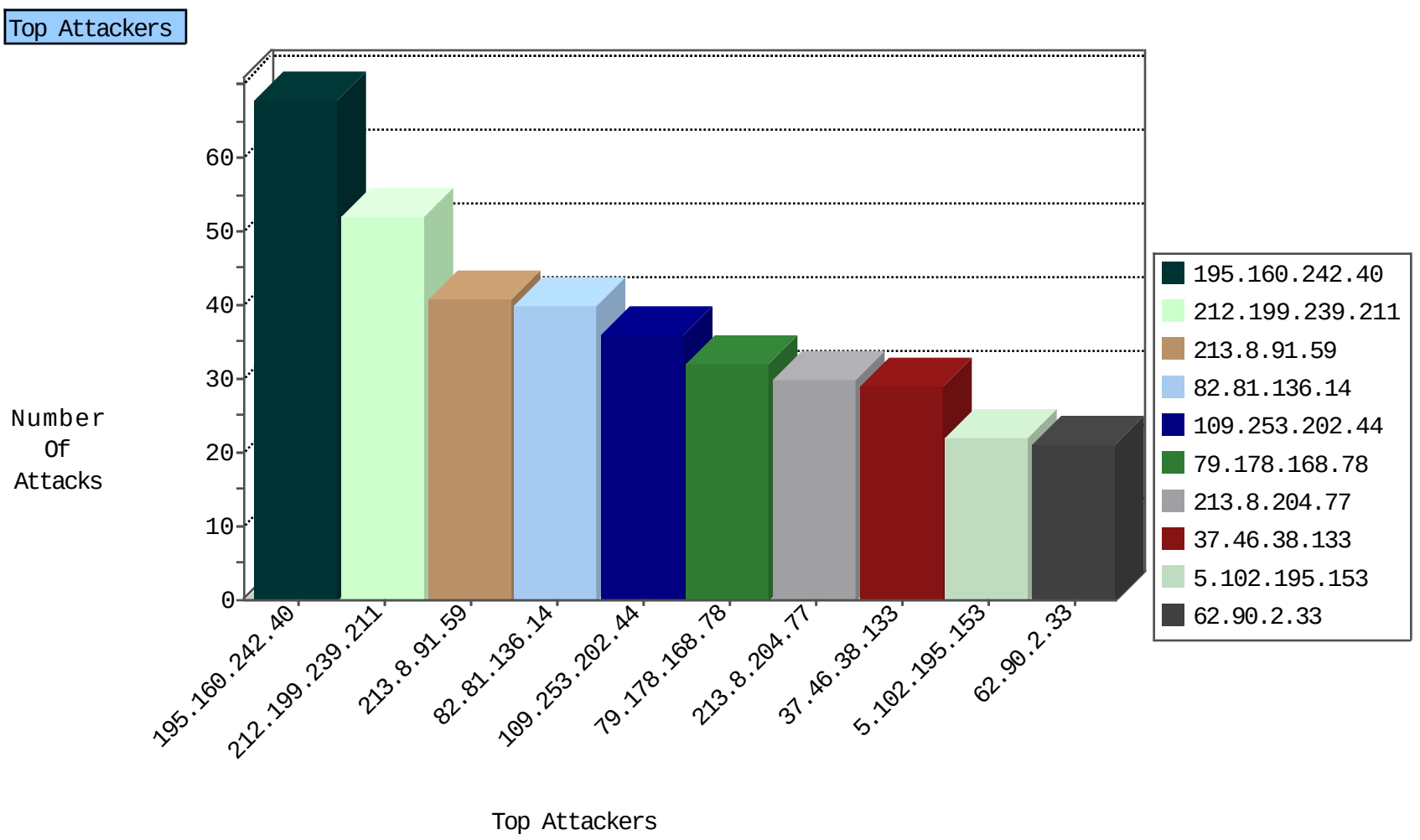
09-29-2016-16:04:00 to 09-29-2016-17:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-29-2016-16:04:00 to 09-29-2016-17:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.91.59	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
2.53.26.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
5.102.195.153	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.220.158.114	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.53.22.249	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
195.59.45.68	United Kingdom	147.237.77.216	dover.idf.il	HTTP-Triple-Headers-Flood-2	drop	2
79.177.39.64	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
192.117.188.130	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
192.54.144.229	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.228.91.142	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
217.132.158.97	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
192.69.89.173	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
58.218.200.137	China	147.237.8.46	e.chinuch.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
198.44.110.12	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1
94.102.52.10	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
217.132.158.97	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
192.117.162.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
198.44.110.12	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-29-2016-16:04:00 to 09-29-2016-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	8
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-29-2016-16:04:00 to 09-29-2016-17:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
163.172.169.150	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.194.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.162.205.49	147.237.77.121	Vietnam	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
76.168.129.148	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.225.236	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.66.169.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.17	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.34.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.46.38.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
108.168.178.253	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
89.138.169.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.246.137.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.19.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.117.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.29.40.157	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
77.138.20.225	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.140.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
109.67.151.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.65.144.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.168.178.253	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
2.53.157.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
108.168.178.253	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
84.109.144.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.72.41.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.18.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-29-2016-16:04:00 to 09-29-2016-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
212.199.239.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
213.8.204.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.178.168.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
37.46.38.133	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
82.81.136.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
62.90.2.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
82.81.136.14	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
109.253.198.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
195.160.242.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
217.132.150.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.126.69.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
185.32.179.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
120.89.103.37	Nepal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.244.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.8.91.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.102.195.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
79.177.202.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.117.56.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
79.176.20.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.126.69.23	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
109.253.202.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.2.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.202.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.130.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.12.160.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.225.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.91.244	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.167.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.166.186.249	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
109.253.202.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.138.87.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.202.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.202.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.91.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
217.132.150.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.107	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.132.150.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

09-29-2016-16:04:00 to 09-29-2016-17:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.174.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
77.139.87.46	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	5
185.32.179.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.34.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.137.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	3
2.53.19.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.81.18	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
31.168.244.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.138.164.106	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Malformed URL	Block	1
46.19.86.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
201.173.19.131	Mexico	147.237.77.234	halag.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
108.161.241.26	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
189.219.236.45	Mexico	147.237.72.166	aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
189.219.236.45	Mexico	147.237.72.166	aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
77.138.218.192	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
207.46.13.52	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
201.166.217.35	Mexico	147.237.76.200	eitan.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
157.55.39.214	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
188.120.148.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
77.138.35.222	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk	Block	1
212.199.239.211	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
176.13.225.126	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unknown HTTP Request Method	Block	1
46.121.67.16	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
201.173.19.131	Mexico	147.237.77.235	sviva.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
109.64.169.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
189.219.236.45	Mexico	147.237.72.167	ishurim.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
185.32.179.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
207.182.140.210	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in URL	Block	1
37.46.38.133	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
201.172.121.200	Mexico	147.237.0.34	tikshuv.idf.il	Redundant HTTP Headers Content-Type	Block	1
166.137.252.97	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
82.81.136.14	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
189.218.169.28	Mexico	147.237.76.31	nakchal.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
77.138.116.89	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
177.238.133.136	Mexico	147.237.76.39	mobile.meitav.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1
61.8.244.132	Australia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
201.173.26.29	Mexico	147.237.0.15	kosher-kravi.idf.il	Redundant HTTP Headers Content-Type	Block	1
201.160.40.118	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1

09-29-2016-16:04:00 to 09-29-2016-17:04:00