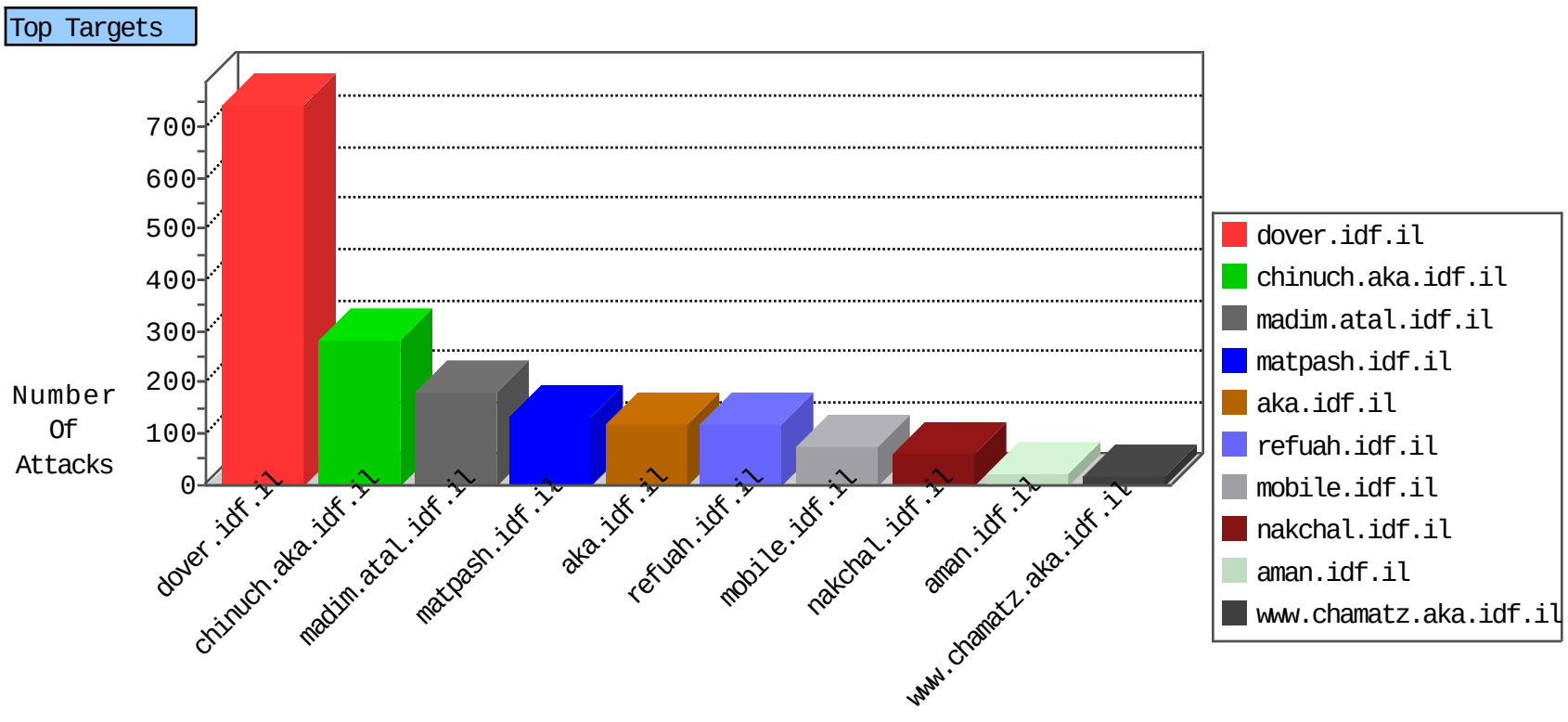
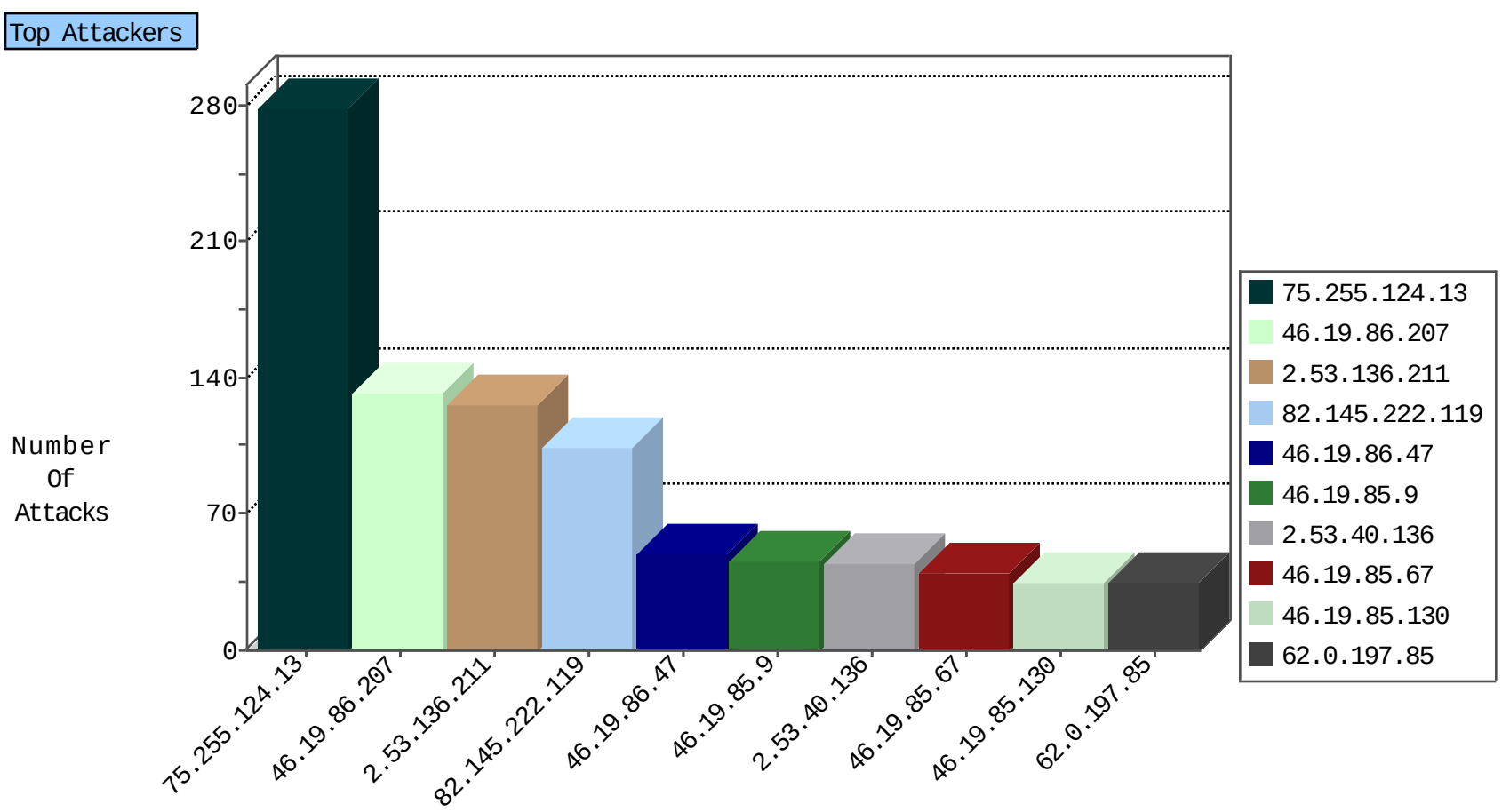
09-27-2016-09:04:01 to 09-27-2016-10:04:01

IDF Under Attack
Daily Report



Top Target



Top Attackers

09-27-2016-09:04:01 to 09-27-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	34
46.19.85.226	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	9
176.13.247.134	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
2.53.133.27	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
2.53.160.17	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
213.151.58.48	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
80.246.137.101	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.116.75.198	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.210.214.163	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
37.26.149.131	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.86.0	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	2
212.143.234.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
89.139.177.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
89.248.174.4	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
46.19.85.251	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.46.41.208	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
45.32.205.113	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

09-27-2016-09:04:01 to 09-27-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-27-2016-09:04:01 to 09-27-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.207	147.237.77.176	Israel	matpash.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	58
84.94.140.177	147.237.77.226	Israel	www.chamatz.aka.idf.il	LOCAL_RULES - HTTP Request with OPTIONS method to a .doc file	3
77.125.30.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.135.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.178.42.242	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.99	147.237.77.216	Israel	dover.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
179.43.144.18	147.237.76.198	Switzerland	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.238.45	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
89.237.105.178	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
40.114.15.49	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.52.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.178.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.178.42.242	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.120.124.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.178.42.242	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.27.105.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.17	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
176.106.46.74	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
40.121.139.43	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
141.226.161.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.121.139.43	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.189.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.11.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.21.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-27-2016-09:04:01 to 09-27-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
75.255.124.13	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	278
82.145.222.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
46.19.86.207	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	60
46.19.85.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
62.0.197.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
223.24.88.44	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.47	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
46.19.86.47	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
107.167.112.139	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
107.167.99.113	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	20
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
62.0.230.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
130.245.145.167	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
46.19.85.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
176.13.245.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.55.35.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.200.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
212.25.79.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.71.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
62.0.230.1	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	10
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.221.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
176.13.236.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.115.163.105	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.207	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	6
46.19.85.145	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.10.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.168.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.29.132.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.207	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.13.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.153.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.29.211	Israel	147.237.77.179	e.mazi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.55.16.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.251.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5

09-27-2016-09:04:01 to 09-27-2016-10:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.136.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
2.53.40.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.86.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
80.178.101.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
2.53.45.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.134.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.221.110	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	2
37.26.146.196	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
176.13.5.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.80.61.179	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
194.90.216.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/alramklali/aspx	Block	1
52.198.76.213	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/web-console/serverinfo.jsp	Block	1
108.171.129.164	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
2.55.45.74	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.3.204	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
213.151.58.48	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
46.19.86.201	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
176.13.10.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
2.53.153.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.126.18.29	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
194.90.252.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/faq.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
5.29.103.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.7.3	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
80.246.130.17	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
216.72.40.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catld in aka.idf.il/main/giyus/general.aspx	None	1
46.19.86.201	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method eden0x2rd in URL	Block	1
180.76.15.9	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
2.53.162.18	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.139.36.160	France	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.24	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
8.37.70.214	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation SearchText in www.tikshuv.idf.il/938-he/tikshuv.aspx	Block	1
80.246.130.46	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9236-he/refuah.aspx	Block	1
216.72.41.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
185.3.147.181	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
2.53.185.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.9.5	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.64.89	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/m/	Block	1
157.55.39.149	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
80.246.133.222	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9331-he/refuah.aspx	Block	1
217.194.202.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1

09-27-2016-09:04:01 to 09-27-2016-10:04:01