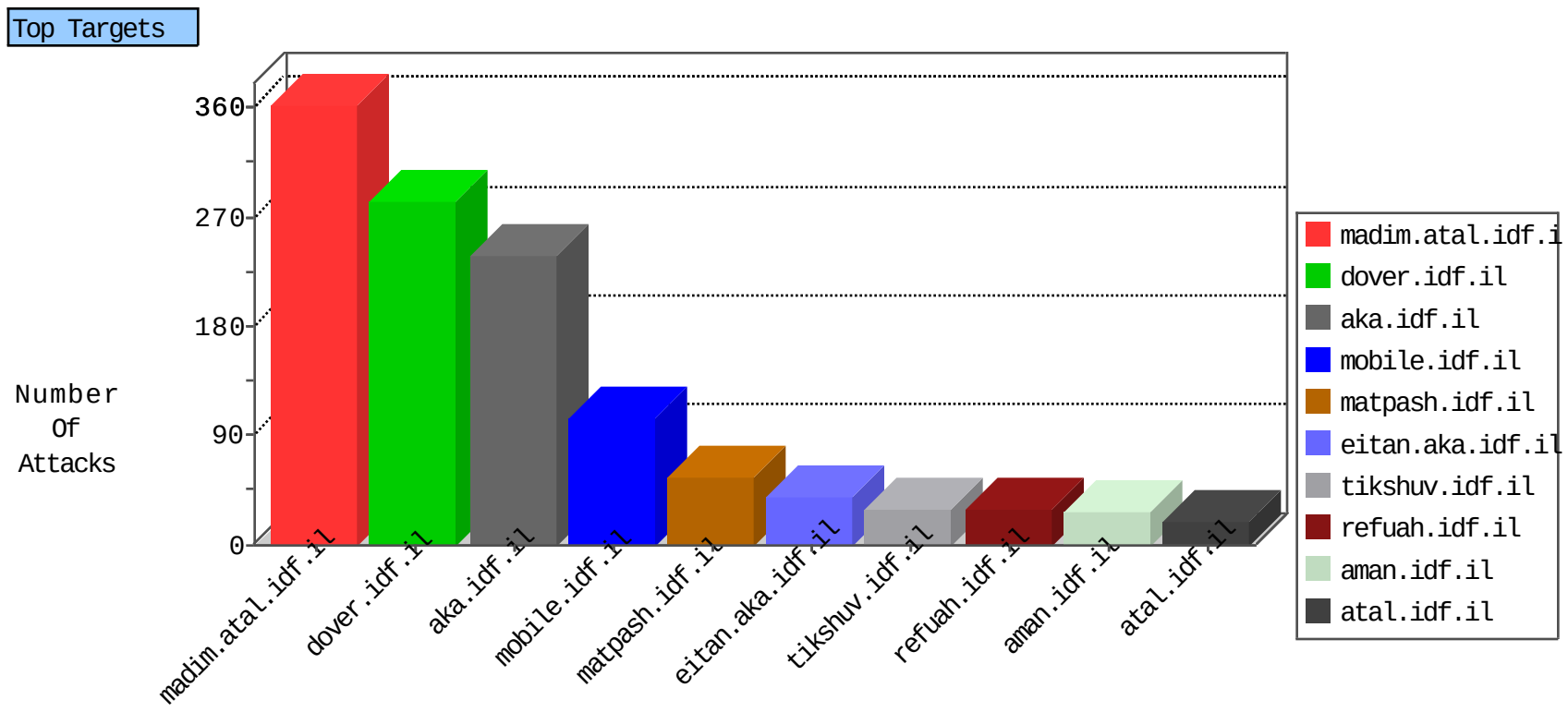
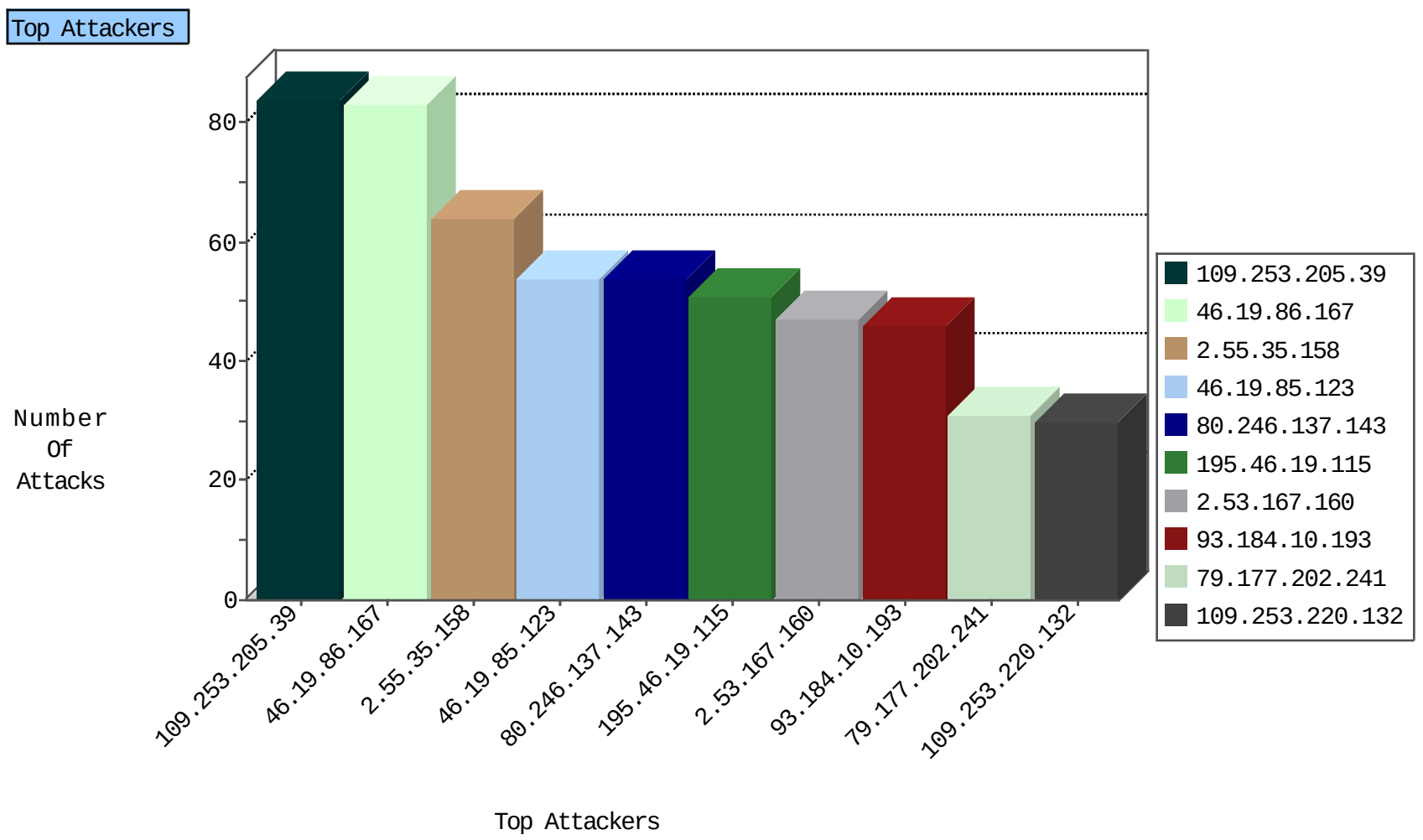
09-29-2016-22:04:04 to 09-29-2016-23:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-29-2016-22:04:04 to 09-29-2016-23:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.0.102.146	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
2.55.23.109	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
204.12.217.2	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
195.112.235.62	Russian Federation	147.237.76.86	navy.idf.il	Black List	drop	1
94.102.52.10	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
173.208.213.196	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
63.141.231.197	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	1
198.44.110.12	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
94.102.52.10	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
180.153.91.178	China	147.237.76.30	himush.idf.il	Black List	drop	1
63.141.250.154	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
117.21.248.87	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
192.187.109.60	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
79.179.119.217	Israel	147.237.76.42	refuah.idf.il	Black List	drop	1
204.12.217.3	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
173.208.207.132	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1

09-29-2016-22:04:04 to 09-29-2016-23:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.4.148	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-29-2016-22:04:04 to 09-29-2016-23:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
178.74.20.27	147.237.77.170	Norway	maarachot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	4
61.240.144.65	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
180.213.5.205	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.65.161.106	147.237.77.19	Pakistan	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
180.97.106.37	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
58.65.161.106	147.237.77.19	Pakistan	law-forum.idf.il	ET SCAN NMAP -f -sS	1
2.55.3.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
114.216.131.108	147.237.76.86	China	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.65.117.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
201.73.83.242	147.237.0.33	Brazil	idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
180.97.106.161	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.65.161.106	147.237.77.19	Pakistan	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.37	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.172.91.20	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
164.70.7.41	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
115.74.128.130	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.32.107.194	147.237.77.235	Italy	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
80.246.130.86	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
61.240.144.65	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

09-29-2016-22:04:04 to 09-29-2016-23:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.202.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	31
109.253.220.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.171.49	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	25
173.161.193.57	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.177.154.119	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
79.179.170.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
107.167.109.87	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
93.184.10.193	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	18
93.184.10.193	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
195.46.19.115	Greece	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
195.46.19.115	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.178.194.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.46.19.115	Greece	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
41.169.18.58	South Africa	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.46.19.115	Greece	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.90	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.90	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
176.13.228.71	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
109.253.138.63	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
31.222.97.5	Spain	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
107.178.194.113	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.15.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.147.131	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.17.217	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.15.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.102.146	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
195.46.19.115	Greece	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.15.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.228.71	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.184.10.193	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
95.218.51.12	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.246.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.138	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
79.181.36.149	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.245.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
93.184.10.193	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	5
31.222.97.5	Spain	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.15.8	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
72.69.192.138	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.15.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
176.13.246.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
141.0.12.5	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4

09-29-2016-22:04:04 to 09-29-2016-23:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.205.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
46.19.86.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
2.55.35.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
80.246.137.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.53.167.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
77.139.41.103	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
80.179.91.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.240	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	5
5.29.242.233	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	4
77.139.103.137	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/iturim/asp/displayallsoldiers.asp	Block	4
80.246.137.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.226.28.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.116.23	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	3
2.53.167.160	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
77.139.193.252	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/faq/default.asp	Block	2
188.120.148.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
50.192.147.82	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
84.154.138.217	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
77.138.162.100	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
157.55.39.177	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
54.71.10.1	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/web-console/serverinfo.jsp	Block	1
85.65.1.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.22.172	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.76.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
188.120.154.60	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
46.19.86.246	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method f45 in URL	Block	1
5.29.135.236	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
157.55.39.200	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
46.19.86.89	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
94.32.107.194	Italy	147.237.77.235	sviva.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.180.231.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.175	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
188.120.154.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/home/home.asp	Block	1
109.253.216.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.116.125.9	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
176.13.246.169	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in 147.237.72.166/main/giyus/general.aspx	Block	1
109.67.130.77	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.202.98	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
77.138.56.236	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
110.170.10.178	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.117.30.165	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
81.18.207.100	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
31.154.81.74	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.64.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58604&docid=73552	Block	1
79.183.91.15	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.13.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1

09-29-2016-22:04:04 to 09-29-2016-23:04:04