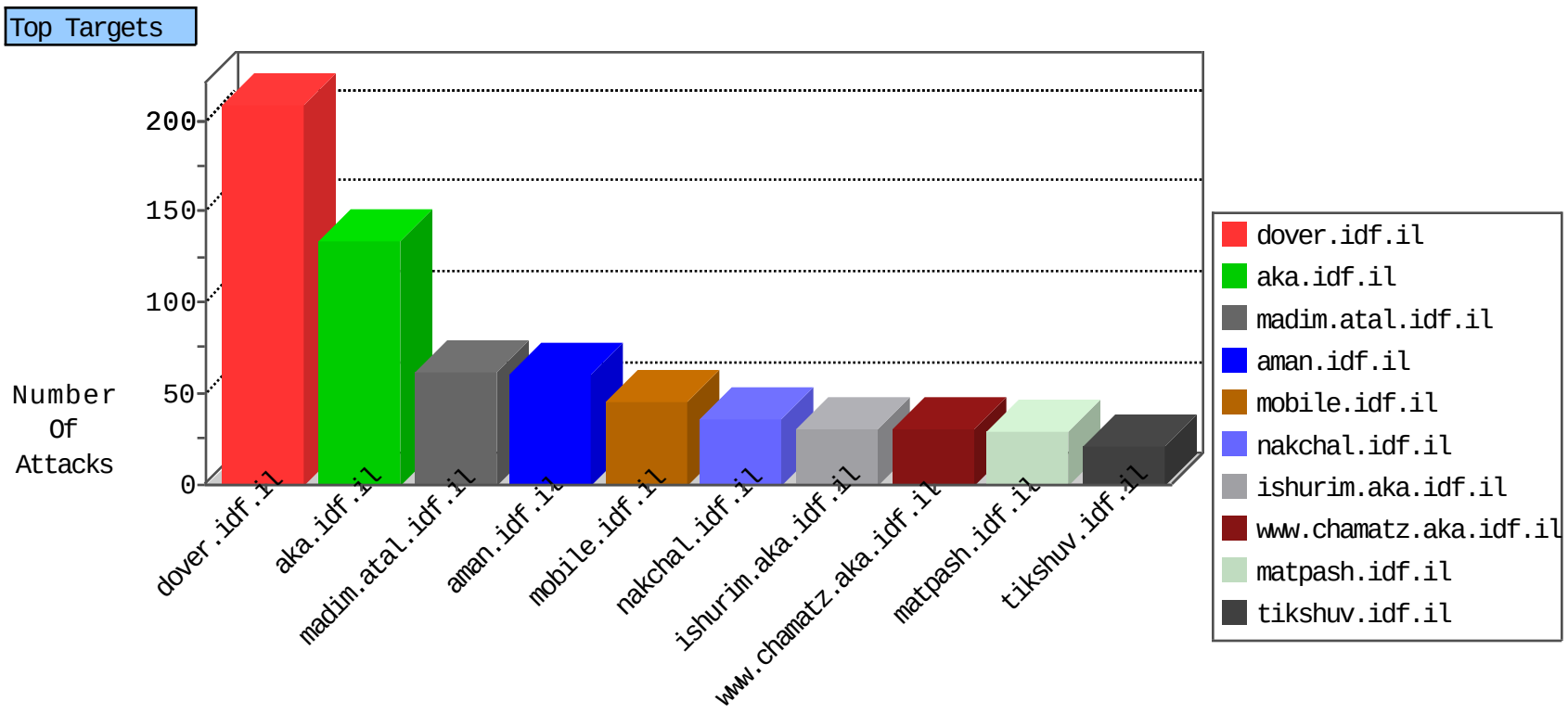
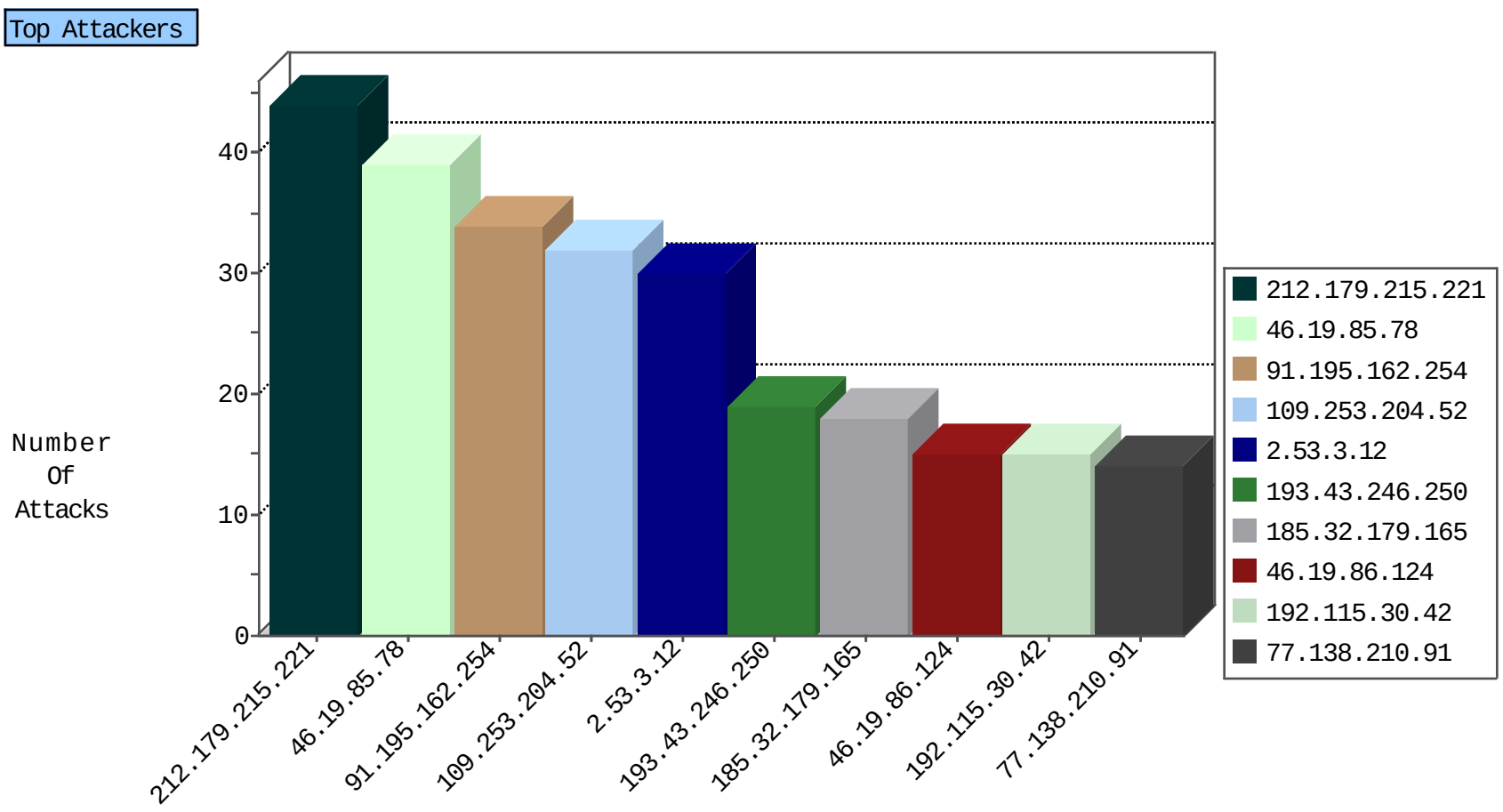
09-21-2016-10:04:08 to 09-21-2016-11:04:08

IDF Under Attack Daily Report





09-21-2016-10:04:08 to 09-21-2016-11:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
47.8.60.167	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
66.249.93.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
195.93.234.8	Israel	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	3
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Black List	drop	1
123.249.3.155	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
173.208.150.114	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1

09-21-2016-10:04:08 to 09-21-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
36.110.147.67	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
2.55.27.87	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-21-2016-10:04:08 to 09-21-2016-11:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.64.245.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
31.13.163.43	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
217.132.9.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.45.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.190.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.164.11.206	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
195.34.78.195	147.237.77.216	Gibraltar	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
54.164.11.206	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
164.52.227.101	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 4096	1
128.232.110.28	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -f -sS	1
123.249.3.155	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
2.55.176.53	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.41.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.215.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.164.11.206	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
207.232.46.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.164.11.206	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
193.34.57.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.5.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.83.120.230	147.237.76.34	Senegal	yohalan.idf.il	ET SCAN Potential SSH Scan	1
164.52.227.101	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 2048	1
125.65.83.162	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
123.249.3.155	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.53.58.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.76.44	Ukraine	e.refuah.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

09-21-2016-10:04:08 to 09-21-2016-11:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.195.162.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
2.53.3.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.32.179.165	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
193.43.246.250	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.78	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.78	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
182.56.163.6	India	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	8
5.22.134.89	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.253.89.45	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.0.240.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
217.194.207.24	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
80.246.139.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.130.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.53.16.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.215	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.76.98.42	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
84.109.75.165	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.115.30.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.115.30.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.115.30.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.76.98.42	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.176.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.149.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.253.89.45	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.179.215.221	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.134.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.179.215.221	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.196	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.166.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.177	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.108.37.57	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.108.127.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
147.236.238.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
5.22.134.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.176.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.134.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.23.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.149.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
85.130.176.140	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

09-21-2016-10:04:08 to 09-21-2016-11:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.204.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
192.116.232.69	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	10
77.138.210.91	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	8
176.13.227.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
77.138.210.91	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
87.152.48.80	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 87.152.48.80	Block	3
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.10.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.202.180	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
176.13.7.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
185.89.217.227	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
115.119.113.194	India	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sites/home/default.asp	Block	1
46.19.85.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
213.57.243.74	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method	Block	1
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version _pk_ses.118.fd1c=*	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
77.138.6.132	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
132.68.49.109	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim	Block	1
46.19.85.167	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.41.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.94.229.51	Belarus	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.101	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Malformed URL _pk_id.118.fd1c=2381425f7808ab7d.1474442892.1.1474442892.1474442892.;	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
77.138.36.133	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.36.133	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method	Block	1
2.53.50.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
87.152.48.80	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
80.178.98.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
109.253.205.119	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method %2C%22%22%2C1474442892%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; in URL _pk_id.118.fd1c=2381425f7808ab7d.1474442892.1.1474442892.1474442892.	Block	1
204.79.180.40	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
77.138.36.133	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	NULL Character in Method	Block	1
2.55.166.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
91.205.154.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
80.246.139.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/</font	Block	1
176.13.233.37	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
109.253.215.79	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1

09-21-2016-10:04:08 to 09-21-2016-11:04:08