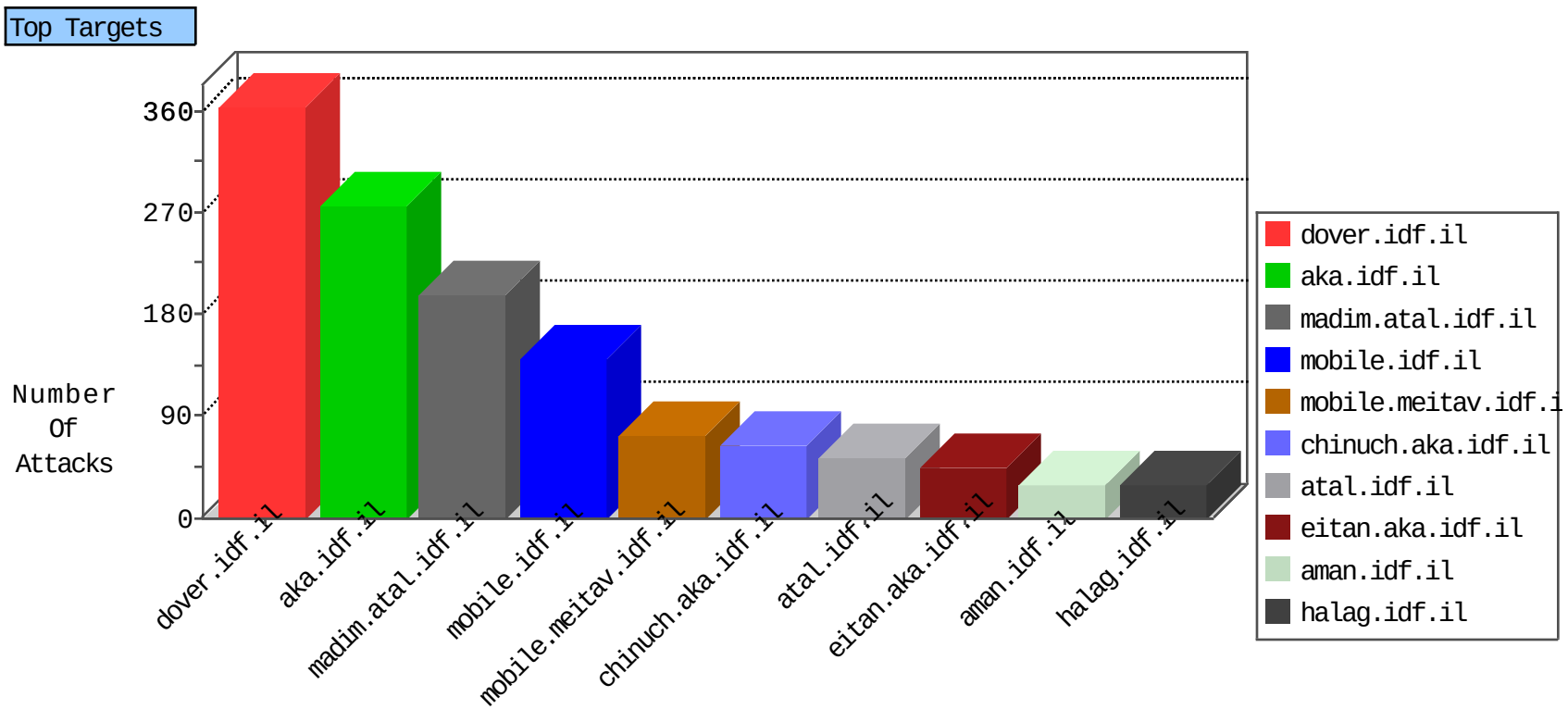
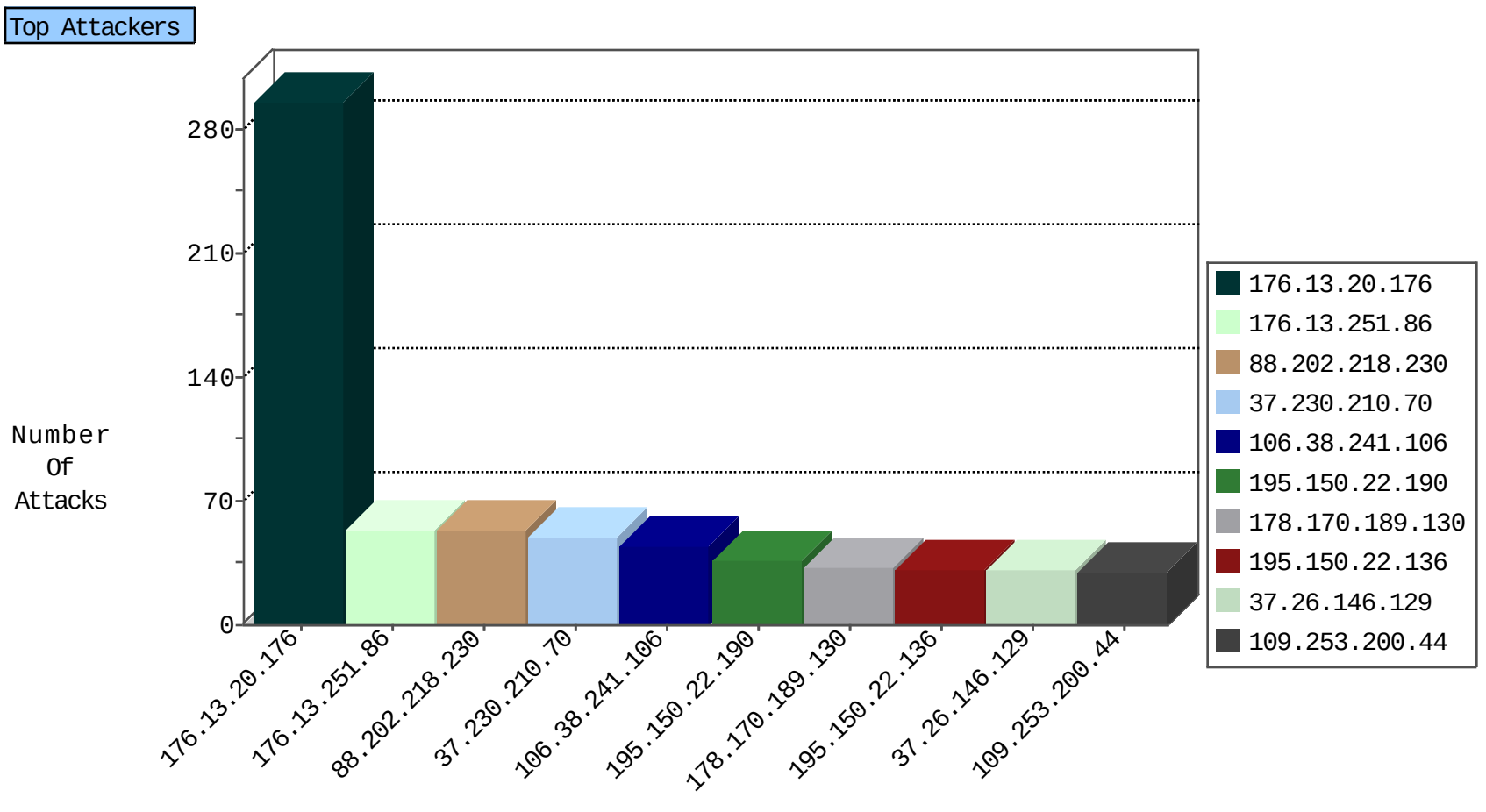
09-25-2016-20:04:08 to 09-25-2016-21:04:08

IDF Under Attack Daily Report





09-25-2016-20:04:08 to 09-25-2016-21:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.81.157	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
2.53.47.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

09-25-2016-20:04:08 to 09-25-2016-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	36
51.255.1.68	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
212.68.146.35	Israel	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
213.251.184.38	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
216.119.125.34	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
69.163.163.224	United States	147.237.77.176	matpash.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-25-2016-20:04:08 to 09-25-2016-21:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.68.146.35	147.237.77.233	Israel	atal.idf.il	SQL Injection - Select From	9
95.155.221.167	147.237.76.38	Sweden	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	3
216.119.125.34	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
222.186.56.199	147.237.72.166	China	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
217.26.17.53	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
185.56.82.22	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.199	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
77.139.196.91	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
45.63.28.148	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 4096	1
209.95.50.84	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
185.129.148.230	147.237.0.33	Latvia	idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.22	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.56.82.22	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.199	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.32.30.116	147.237.77.61	China	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.56.199	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.56.199	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.93.156	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	1
45.63.28.148	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
210.212.207.80	147.237.76.86	India	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.80.155.222	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.129.148.230	147.237.0.16	Latvia	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.22	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-25-2016-20:04:08 to 09-25-2016-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.20.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	58
176.13.20.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	45
176.13.20.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	43
88.202.218.230	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
176.13.20.176	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
195.150.22.190	Poland	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.20.176	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
176.13.20.176	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	25
31.154.241.53	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
176.13.20.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.26.146.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.94.76.17	Croatia	147.237.77.233	atal.idf.il	drop	SAM rule	drop	17
88.202.218.230	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
176.13.20.176	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
195.150.22.136	Poland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
156.57.211.97	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
31.210.188.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.195.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
37.26.146.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
185.24.207.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.20.176	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.71.48.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
83.130.215.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
79.182.137.130	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
37.26.146.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
86.30.13.177	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
130.180.211.15	Ukraine	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
80.179.19.81	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
213.57.46.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
207.46.13.14	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
74.208.192.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.249	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
62.219.34.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
195.150.22.136	Poland	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.53.177.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.145.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
37.230.210.70	Russian Federation	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	5
156.57.211.97	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
177.185.192.98	Brazil	147.237.77.233	atal.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
178.170.189.130	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
109.64.62.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.20.176	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
178.170.189.130	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5

09-25-2016-20:04:08 to 09-25-2016-21:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.251.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
125.116.209.49	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 125.116.209.49	Block	14
85.64.64.103	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	7
109.253.209.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	7
37.26.146.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
176.13.4.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
125.116.209.49	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
77.125.84.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
31.210.188.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
213.151.35.218	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
79.177.189.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
176.13.17.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.35.218	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.35.218	Block	3
176.13.228.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.235.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.102.242.213	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.102.242.213	Block	2
109.226.48.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	2
176.13.20.176	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
109.253.195.146	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
62.219.34.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
70.215.23.56	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	1
46.19.85.143	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
199.203.186.155	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.139.160	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.121.222	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
84.108.87.238	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.108.87.238	Block	1
37.26.146.155	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.87.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
77.125.43.44	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Parameter Encoding	None	1
46.19.86.210	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.68.41.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail/giyus	Block	1
5.102.242.213	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
207.46.13.14	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.108.87.238	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
77.139.66.245	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
109.253.145.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.87.238	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
41.36.64.168	Egypt	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
185.3.147.211	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.87.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
125.116.209.49	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
77.125.43.44	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	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
87.69.98.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/yahash2015/lobby.aspx	Block	1
84.108.87.238	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-login.php	Block	1
31.154.241.53	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.139.90.36	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-25-2016-20:04:08 to 09-25-2016-21:04:08