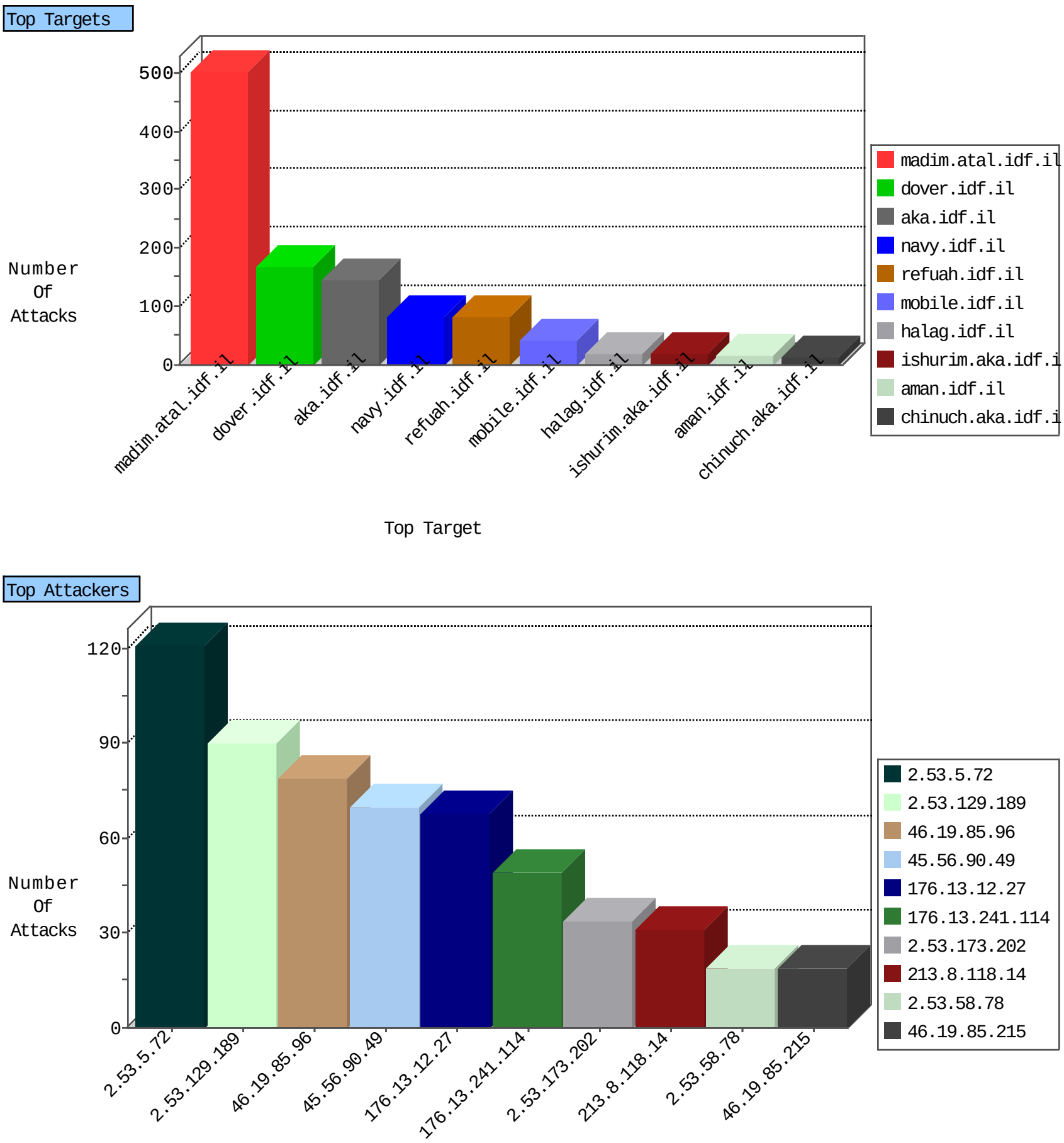
09-04-2016-14:04:09 to 09-04-2016-15:04:09

IDF Under Attack Daily Report



09-04-2016-14:04:09 to 09-04-2016-15:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	131
46.19.86.88	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	36
176.106.41.217	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	25
46.117.58.255	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
134.147.203.115	Germany	147.237.76.197	e.himush.idf.il	Black List	drop	2
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1
119.142.214.147	China	147.237.77.121	e.navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-04-2016-14:04:09 to 09-04-2016-15:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.187.94.250	Egypt	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	3
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.126.68.101	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
188.138.1.119	Germany	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-04-2016-14:04:09 to 09-04-2016-15:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
45.79.71.122	147.237.77.234	United States	halag.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
92.29.68.241	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.118.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.2.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.55.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.117.182.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.124	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
185.72.177.20	147.237.8.45	Romania	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
50.116.123.135	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
107.15.44.175	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.217.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 4096	1
2.53.30.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.194.4.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.251.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
81.218.68.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.241.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.107.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.23.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.137.171.55	147.237.76.42	Canada	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.65.80.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-04-2016-14:04:09 to 09-04-2016-15:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
213.8.118.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	21
45.56.90.49	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
45.56.90.49	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
45.56.90.49	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
46.19.86.225	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.123	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
45.56.90.49	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
37.26.148.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.139.105.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
45.56.90.49	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.243	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
104.207.144.185	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
5.29.94.49	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
2.54.88.113	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
5.29.94.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
109.253.130.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.17.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
193.106.52.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.105	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	5
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
213.8.118.14	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
193.106.52.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.117.150.188	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
213.8.118.14	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.181.155.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.110.54.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.69.87.85	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.180	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
176.13.17.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.85.193	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.246.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.218.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.179.114.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.17.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
80.179.114.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.61.62	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	3
2.53.5.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.199	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
66.249.76.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.19.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
77.211.44.4	Spain	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.2.147	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence		monitor	2

09-04-2016-14:04:09 to 09-04-2016-15:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.5.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
2.53.129.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
176.13.12.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
176.13.241.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
2.53.173.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
2.53.58.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
2.55.59.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
77.125.49.64	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	11
80.246.138.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
62.0.73.78	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	5
192.116.233.90	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
46.19.85.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
213.8.110.17	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/	Block	4
77.139.102.34	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
37.26.147.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
207.46.13.45	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
89.139.105.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.198.151.43	Block	3
2.55.61.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	3
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.25.216	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
162.216.224.38	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
132.74.145.215	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
77.139.208.160	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
37.26.147.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.135.36	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.26.148.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
62.0.73.78	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.0.73.78	Block	2
213.8.115.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general.aspx	Block	2
84.108.232.100	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.221	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.181.222.176	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.55.39.173	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
46.19.86.225	Israel	147.237.76.42	refuah.idf.il	Distributed Illegal HTTP Version	Block	1
95.59.136.118	Kazakstan	147.237.76.147	chinuch.aka.idf.i	Multiple Illegal Byte Code Character in Method from 95.59.136.118	Block	1
46.19.85.50	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
192.116.233.90	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
87.69.16.75	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
100.15.94.30	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
66.249.64.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	1
95.59.136.118	Kazakstan	147.237.76.147	chinuch.aka.idf.i	Illegal Byte Code Character in Header Name	Block	1
45.79.71.122	United States	147.237.77.234	halag.idf.il	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	1
188.120.148.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
79.182.115.34	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
77.125.49.64	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.49.64	Block	1

09-04-2016-14:04:09 to 09-04-2016-15:04:09