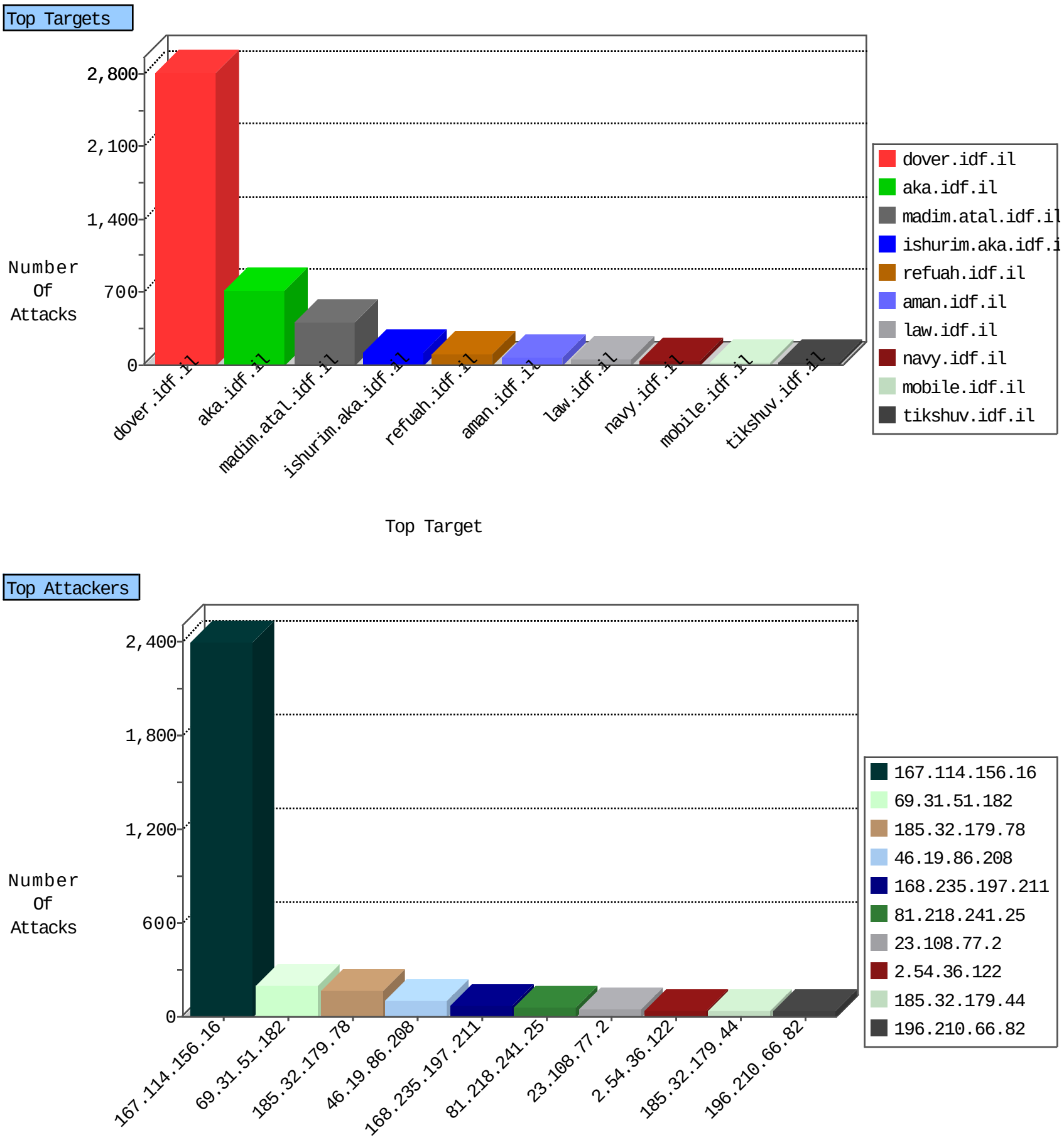
01-24-2016-10:04:03 to 01-24-2016-11:04:03

IDF Under Attack Daily Report



01-24-2016-10:04:03 to 01-24-2016-11:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3031
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	403
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
46.19.86.208	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	57
81.218.56.245	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
168.235.197.211	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
188.138.1.218	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-24-2016-10:04:03 to 01-24-2016-11:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.32.64.53		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
45.32.225.19		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-24-2016-10:04:03 to 01-24-2016-11:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.117.208.243	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
216.72.40.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.210.66.82	147.237.77.216	South Africa	dover.idf.il	portscan: TCP Distributed Portscan	1
23.101.3.156	147.237.8.45	Hong Kong	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
41.241.38.42	147.237.77.216	Sudan	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.112.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.101.3.156	147.237.77.216	Hong Kong	dover.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.52.154.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.13.173	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

01-24-2016-10:04:03 to 01-24-2016-11:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
69.31.51.182	Anonymous Proxy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	200
168.235.197.211	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	67
2.54.36.122	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	39
23.108.77.2	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
62.0.34.177	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	26
37.26.149.140	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
188.120.148.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
37.60.151.52	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	18
188.161.48.7	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
188.120.148.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
37.26.146.174	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.175	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.19.86.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
196.210.66.82	South Africa	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
79.180.254.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.254.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
37.26.149.140	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	10
79.180.254.104	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.52.51.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.95.211.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.241.38.42	Sudan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
138.134.192.10	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.175	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
196.210.66.82	South Africa	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.220	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
196.210.66.82	South Africa	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.71	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.171	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.199.154.194	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
5.135.165.184	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
40.77.167.11	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.161.48.7	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.183.175.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.186.189.174	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.34	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.255.253.38	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.197.117	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.135.165.184	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6

01-24-2016-10:04:03 to 01-24-2016-11:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
185.32.179.78	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 185.32.179.78	Block	54
185.32.179.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
2.54.186.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
176.13.6.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
80.246.137.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
109.253.139.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
5.29.83.3	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.83.3	Block	16
46.19.85.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
109.253.203.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
77.125.133.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
85.250.207.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	4
80.246.137.12	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 80.246.137.12	Block	4
185.32.179.78	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 185.32.179.78	Block	4
46.19.86.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
93.172.191.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.36.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
132.72.33.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
2.52.188.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
23.251.86.72	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	3
109.253.204.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
23.251.86.72	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	3
149.50.87.26	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.25.16	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	2
192.115.248.2	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.107	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.107	Block	2
2.54.155.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.128.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.107	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
46.19.86.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.205.50.218	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
217.194.202.17	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
132.72.33.242	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 132.72.33.242	Block	2
23.108.77.2	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.12.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.152.94	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	1
85.65.43.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
24.181.122.68	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
132.72.33.242	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
23.108.77.2	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 19	Block	1
109.67.164.218	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.180.58.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.83.3	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1

01-24-2016-10:04:03 to 01-24-2016-11:04:03