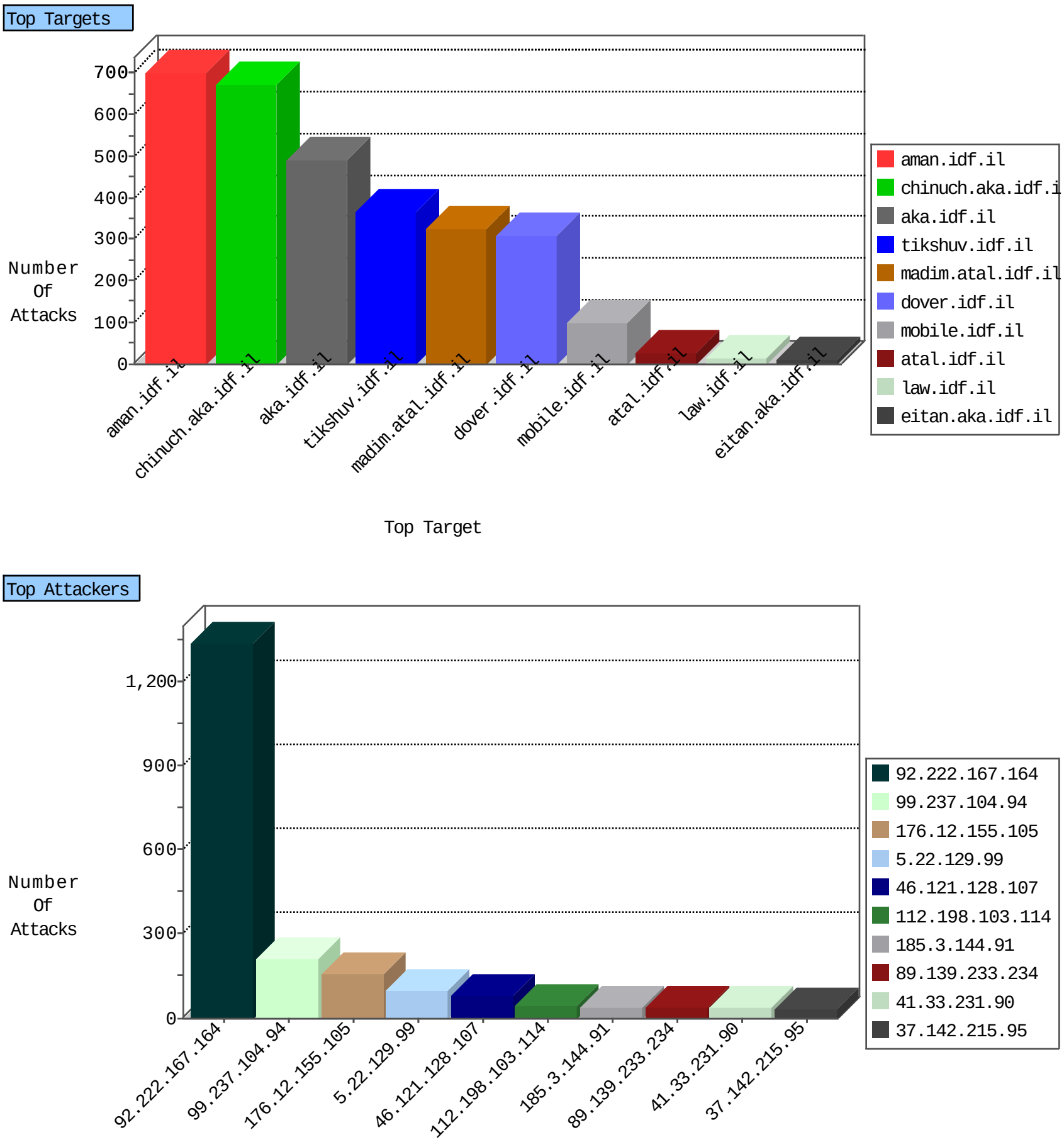
02-02-2016-19:04:06 to 02-02-2016-20:04:06

IDF Under Attack
Daily Report



02-02-2016-19:04:06 to 02-02-2016-20:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	26
109.67.26.72	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
79.181.56.211	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
109.66.135.112	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
200.53.9.113	Brazil	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
74.91.28.58	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
74.91.28.62	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
142.54.169.165	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
82.166.184.140	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

02-02-2016-19:04:06 to 02-02-2016-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.169.180.90	Romania	147.237.77.216	dover.idf.il	12715: HTTP: Blind SQL Injection in URI	Block	3

02-02-2016-19:04:06 to 02-02-2016-20:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
52.35.178.67	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
209.126.116.147	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
188.120.148.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.155.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.19.22.223	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.204.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
111.180.80.143	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.148.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.213.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.36.77.11	147.237.76.31	India	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.43.197.178	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.202.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.234.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
194.187.249.120	147.237.76.198	Europe	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
185.3.144.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.155.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.195.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.119.164.1	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.116.9.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.73.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.185.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.160.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.82.83	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.44.123	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.230.7.173	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

02-02-2016-19:04:06 to 02-02-2016-20:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
92.222.167.164	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	666
92.222.167.164	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	444
92.222.167.164	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	207
99.237.104.94	Canada	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	70
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
185.3.144.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.160.168.246	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
92.222.167.164	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.121.128.107	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.64.220.244	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
109.160.224.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
109.160.224.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.65.41.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.69.144.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
5.22.129.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.12.154.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.121	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
5.22.129.99	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
31.210.187.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.71.5.9	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
87.71.5.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
176.12.154.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.105.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.246.136.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
5.22.135.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.24.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.165.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.34.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.248.214	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.46.39.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.129.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.73	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.129.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.22.129.99	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.136.217	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.136.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
99.237.104.94	Canada	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	144
176.12.155.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
176.12.155.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
46.121.128.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
5.22.129.99	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
89.139.233.234	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.233.234	Block	35
2.54.171.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
37.142.215.95	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
176.12.155.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
212.199.205.68	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
85.250.108.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
176.12.154.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
213.151.49.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	3
79.176.160.58	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	3
109.66.1.62	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
37.26.146.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.233.69	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	3
79.176.160.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
195.154.71.139	France	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	2
195.154.71.139	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	2
195.154.71.139	France	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	2
195.154.71.139	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
176.12.154.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
195.154.71.139	France	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	2
37.46.38.190	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
84.108.105.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
195.154.71.139	France	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	2
195.154.71.139	France	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	2
149.78.34.20	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
213.57.172.65	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.116.137.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
195.154.71.139	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	2
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	1
37.239.8.28	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
188.143.232.35	Russian Federation	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1454-he/refuah.aspx	Block	1
93.172.167.199	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
176.12.154.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.128.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.160.58	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.176.160.58	Block	1
195.154.71.139	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Too Many Headers per Request - 66 Headers	Block	1
109.64.220.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
31.168.13.78	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Open Mode	None	1
176.12.155.143	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	1
176.12.154.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
80.246.137.247	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$hiddenUpdateEmail in www.aka.idf.il/main/giyus/faq.aspx	None	1
212.76.103.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/67780.pdf&sa=u&ved=0ahukewjl95asynnkahxeea8khru5bskqfggtmaq&usg=afqjcnehgkvpezkwekkpkakqhswkanlfuq	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name [[#3]]m	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-ar/cogat.aspx	Block	1