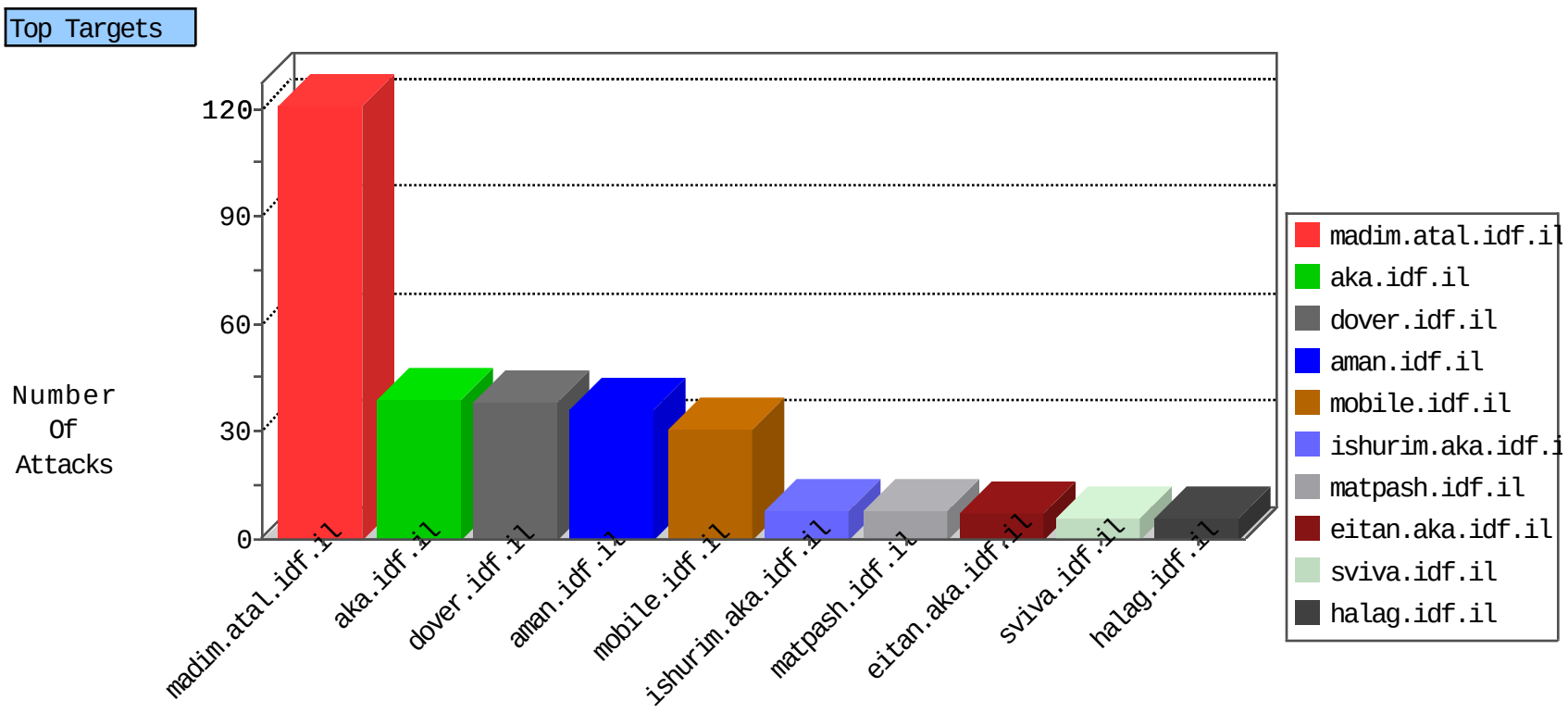
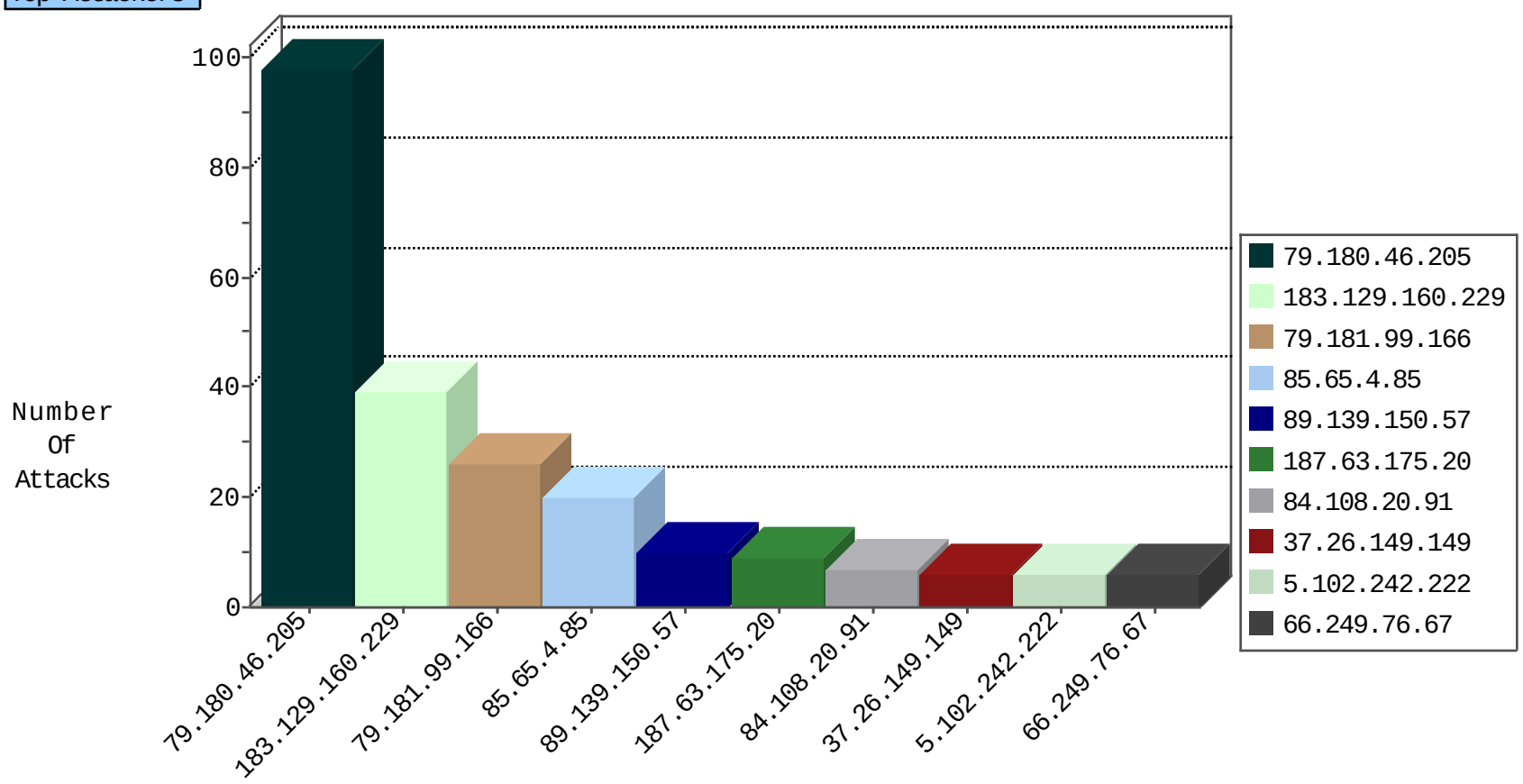
10-01-2016-08:04:08 to 10-01-2016-09:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-01-2016-08:04:08 to 10-01-2016-09:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.34.175	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
204.42.253.132	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
93.158.200.66	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
93.158.200.126	Netherlands	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1

10-01-2016-08:04:08 to 10-01-2016-09:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-01-2016-08:04:08 to 10-01-2016-09:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.0.34	Israel	tikshuv.idf.il	Xenu Link Sleuth User Agent	2
187.140.219.59	147.237.77.216	Mexico	dover.idf.il	Xenu Link Sleuth User Agent	2
14.152.59.11	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.79.224	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
208.100.26.228	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.65.51	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
187.63.175.20	147.237.77.235	Brazil	sviva.idf.il	ET SCAN Potential SSH Scan	1
62.210.243.100	147.237.0.19	France	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
187.63.175.20	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
187.63.175.20	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
187.63.175.20	147.237.76.86	Brazil	navy.idf.il	ET SCAN Potential SSH Scan	1
187.63.175.20	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
115.79.32.26	147.237.72.166	Vietnam	aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.76.119	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
66.249.65.21	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
187.63.175.20	147.237.77.234	Brazil	halag.idf.il	ET SCAN Potential SSH Scan	1
59.35.27.100	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
187.63.175.20	147.237.77.216	Brazil	dover.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
187.63.175.20	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
187.63.175.20	147.237.8.50	Brazil	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
40.68.159.134	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
183.10.79.34	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-01-2016-08:04:08 to 10-01-2016-09:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	8
84.108.20.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.253.128.182	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.3.147.188	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
89.139.150.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
89.139.150.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.26.149.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.200.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.138.133.249	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
187.61.109.18	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
2.53.172.234	Israel	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
84.108.233.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.120.154.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.134.194	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.226.217.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.125.54.128	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
131.253.25.159	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
131.253.25.173	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
89.139.150.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
183.129.160.229	China	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
131.253.27.2	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.25	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.23	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.94	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.102.254.53	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
93.158.200.68	Netherlands	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
183.129.160.229	China	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.108.213.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.148	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.226.217.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.49	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.208.184	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
217.132.54.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
93.158.200.68	Netherlands	147.237.76.34	yohalan.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.46.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
5.102.242.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.138.65.184	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	5
37.26.149.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.174.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
141.226.217.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
183.129.160.229	China	147.237.77.226	www.chamatz.aka.idf.il	Multiple Malformed URL from 183.129.160.229	Block	1
183.129.160.229	China	147.237.77.74	law.idf.il	Multiple Malformed URL from 183.129.160.229	Block	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
183.129.160.229	China	147.237.77.234	halag.idf.il	Multiple Malformed HTTP Header Line from 183.129.160.229	Block	1
183.129.160.229	China	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 183.129.160.229	Block	1
2.53.149.136	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
183.129.160.229	China	147.237.72.167	ishurim.aka.idf.il	Malformed HTTP Header Line 1	Block	1
183.129.160.229	China	147.237.77.235	sviva.idf.il	Malformed URL	Block	1
66.249.65.10	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1732	Block	1
183.129.160.229	China	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unknown HTTP Request Method from 183.129.160.229	Block	1
183.129.160.229	China	147.237.77.74	law.idf.il	Multiple Unknown HTTP Request Method from 183.129.160.229	Block	1
84.108.20.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
183.129.160.229	China	147.237.77.234	halag.idf.il	Multiple Malformed URL from 183.129.160.229	Block	1
183.129.160.229	China	147.237.77.216	dover.idf.il	Multiple Malformed URL from 183.129.160.229	Block	1
183.129.160.229	China	147.237.72.167	ishurim.aka.idf.il	Malformed URL	Block	1
183.129.160.229	China	147.237.77.235	sviva.idf.il	Unknown HTTP Request Method test in URL	Block	1
77.139.20.94	France	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
183.129.160.229	China	147.237.77.233	atal.idf.il	Malformed HTTP Header Line 1	Block	1
183.129.160.229	China	147.237.77.176	matpash.idf.il	Malformed HTTP Header Line 1	Block	1
85.65.74.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
183.129.160.229	China	147.237.77.234	halag.idf.il	Multiple Unknown HTTP Request Method from 183.129.160.229	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8910-he/refuah.aspx	Block	1
183.129.160.229	China	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 183.129.160.229	Block	1
31.154.81.16	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
183.129.160.229	China	147.237.72.167	ishurim.aka.idf.il	Unknown HTTP Request Method test in URL	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13713-ar	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
183.129.160.229	China	147.237.77.233	atal.idf.il	Malformed URL	Block	1
183.129.160.229	China	147.237.77.176	matpash.idf.il	Malformed URL	Block	1
183.129.160.229	China	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
183.129.160.229	China	147.237.77.226	www.chamatz.aka.idf.il	Multiple Malformed HTTP Header Line from 183.129.160.229	Block	1
31.154.81.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
183.129.160.229	China	147.237.77.74	law.idf.il	Multiple Malformed HTTP Header Line from 183.129.160.229	Block	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.181.99.166 (Open Mode)	None	1
213.57.178.106	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.52	Block	1
183.129.160.229	China	147.237.77.233	atal.idf.il	Unknown HTTP Request Method test in URL	Block	1
183.129.160.229	China	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method test in URL	Block	1
183.129.160.229	China	147.237.77.235	sviva.idf.il	Malformed HTTP Header Line 1	Block	1
66.249.76.119	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1