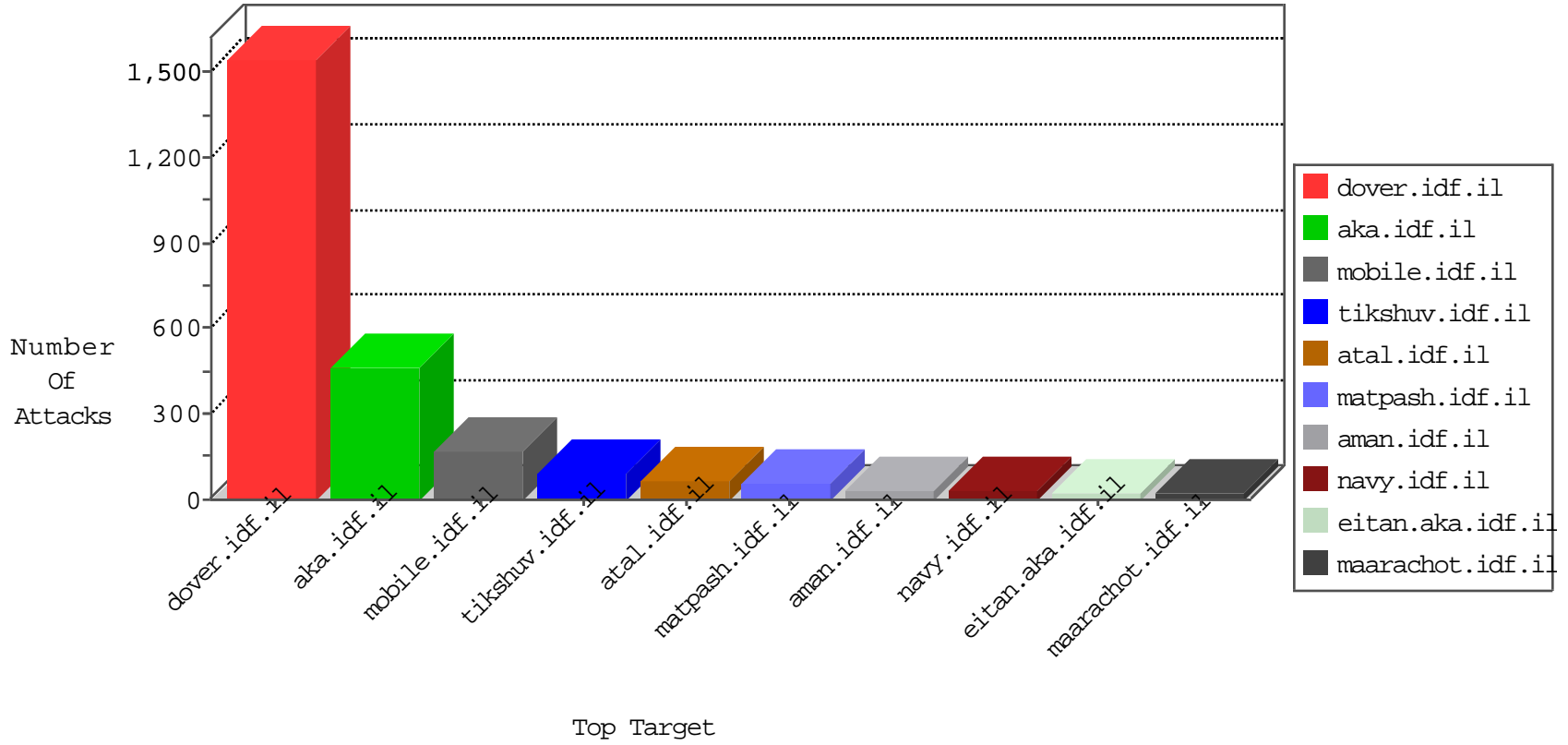




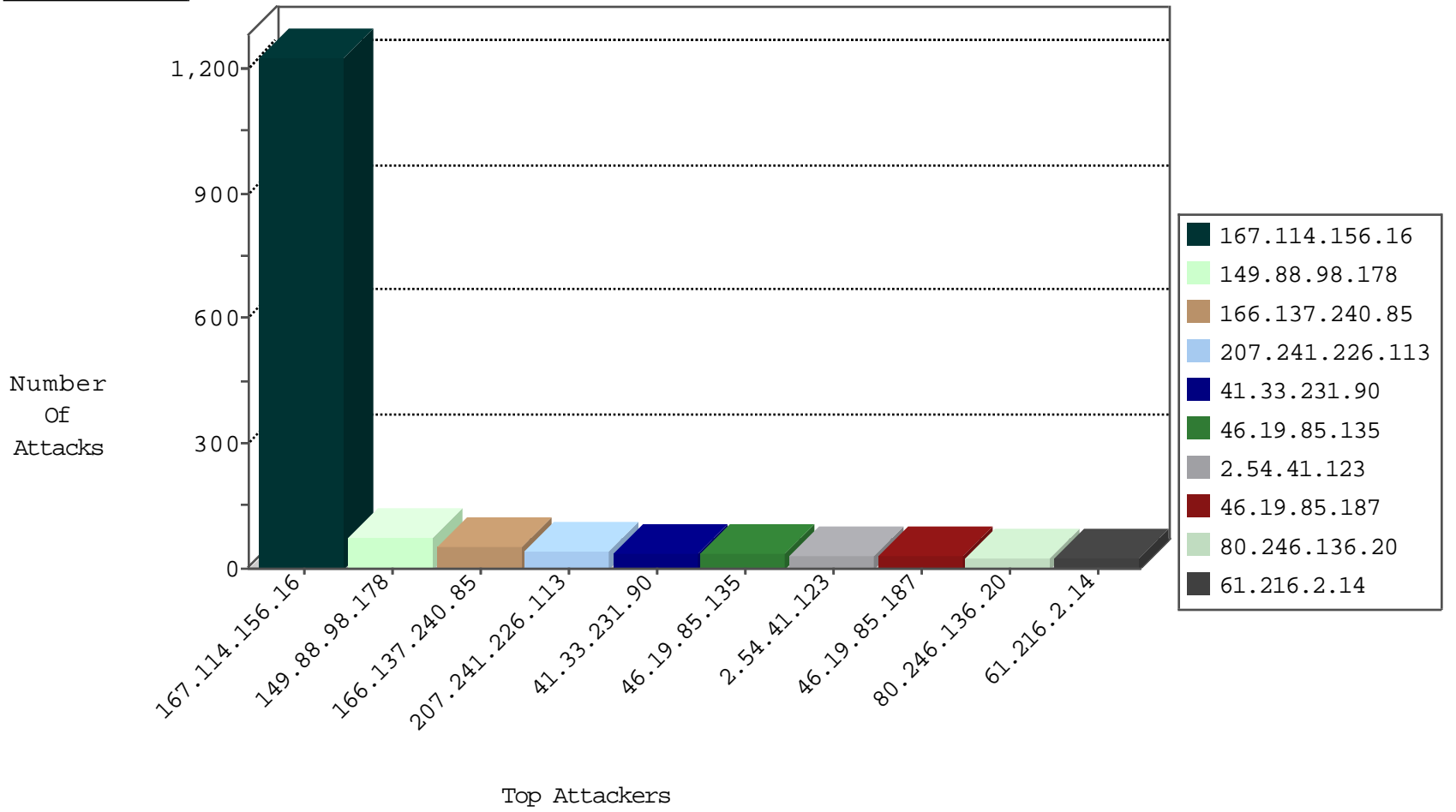
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3559
166.78.253.79	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
109.186.155.116	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
198.20.70.114	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
176.51.48.10	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
158.69.126.160	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.106.92.173		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-30-2015-17:04:04 to 12-30-2015-18:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
207.241.226.113	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.69	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
199.191.56.188	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
176.228.133.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.148	China	gocenter.aka.idf.il	ET SCAN Potential SSH Scan	1
162.248.160.18	147.237.8.50	Canada	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
149.78.19.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
134.222.104.250	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.13.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
111.84.195.245	147.237.77.216	Thailand	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.59.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.32.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.75.236.76	147.237.72.167	Germany	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.176	China	test.noore.idf.il	ET SCAN Potential SSH Scan	1
162.248.160.18	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
151.217.14.42	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
141.8.132.38	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
118.163.112.245	147.237.77.178	Taiwan	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.54.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.4.213	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
166.137.240.85	United States	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
207.241.226.113	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
46.19.85.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
2.54.41.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.187	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
80.246.136.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
163.247.46.239	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
109.64.210.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.135.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.4.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.52.22.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
176.13.4.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.179.118.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.54.13.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.81.23.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.179.9.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.54.148.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.46.39.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.65.140.113	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.136.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.14.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.135.102.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.149.201	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence		alert	6
2.54.146.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.175.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
61.216.2.14	Taiwan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
79.181.4.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.201	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence		monitor	6
79.181.32.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.87.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.212	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.139.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.57.134.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.65.140.113	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.179.9.7	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.253.150.32	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.149.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.179.28.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.98.178	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	72
149.78.50.74	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
109.186.18.110	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.186.18.110	Block	4
217.132.3.13	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
66.249.66.52	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.253.205.240	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	4
66.249.66.61	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
217.132.3.13	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtPersonalId in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	3
84.109.112.174	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
84.109.113.156	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.109.113.156	Block	3
107.167.113.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
176.13.21.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.102.241.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.146.3	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
84.109.112.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.173.43.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.205.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.102.228.59	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/horaot	Block	1
37.142.196.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.43.204	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.8.204.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
128.232.110.29	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
5.102.230.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.94.176.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.52.22.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.157	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
180.76.15.29	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.81.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.6.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.176.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.154	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
84.109.113.156	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site/spotting/spotting.asp	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1065-en/dover.aspx	Block	1
149.88.37.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.138.80	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
2.54.154.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.81.28.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
185.32.179.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.216.2.14	Taiwan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1