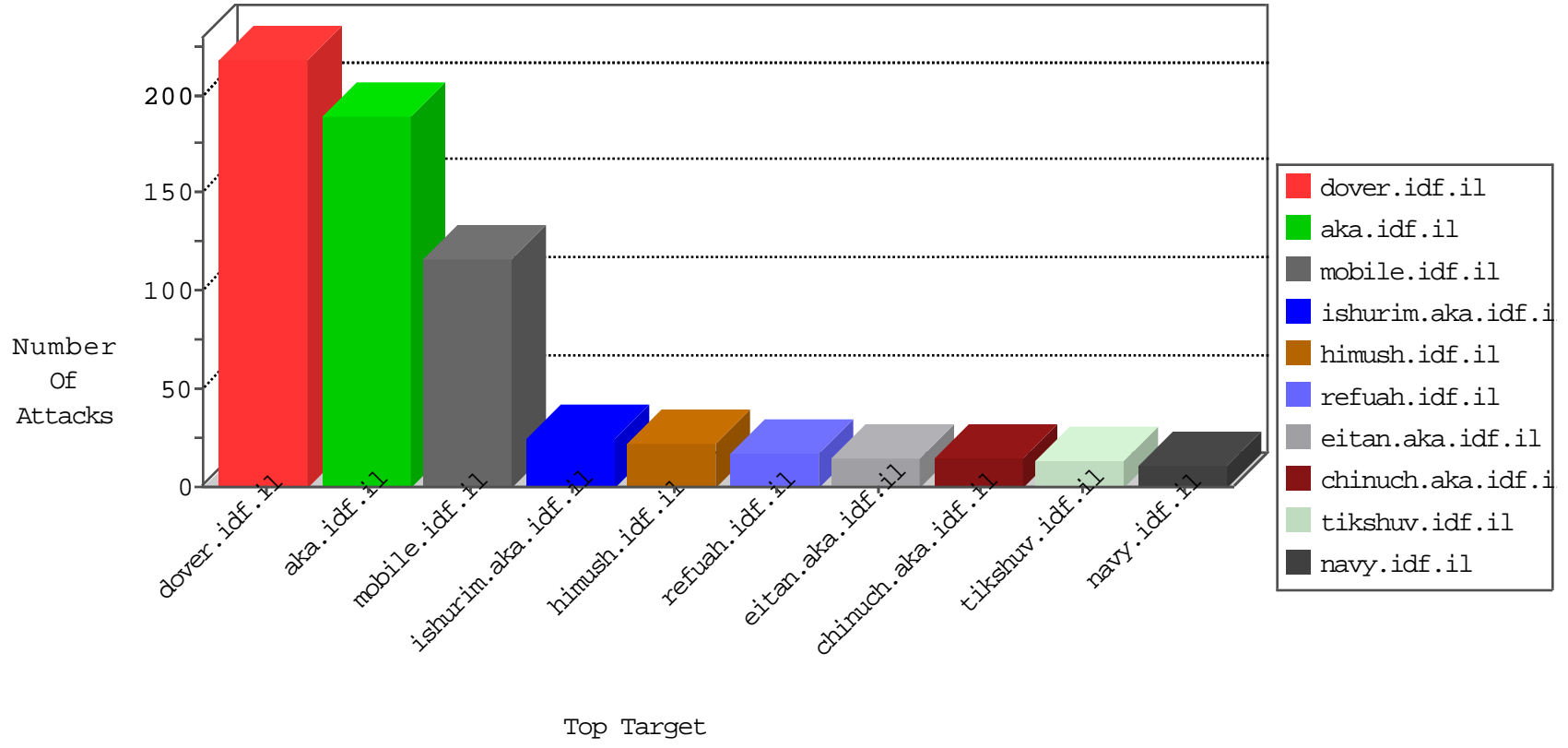


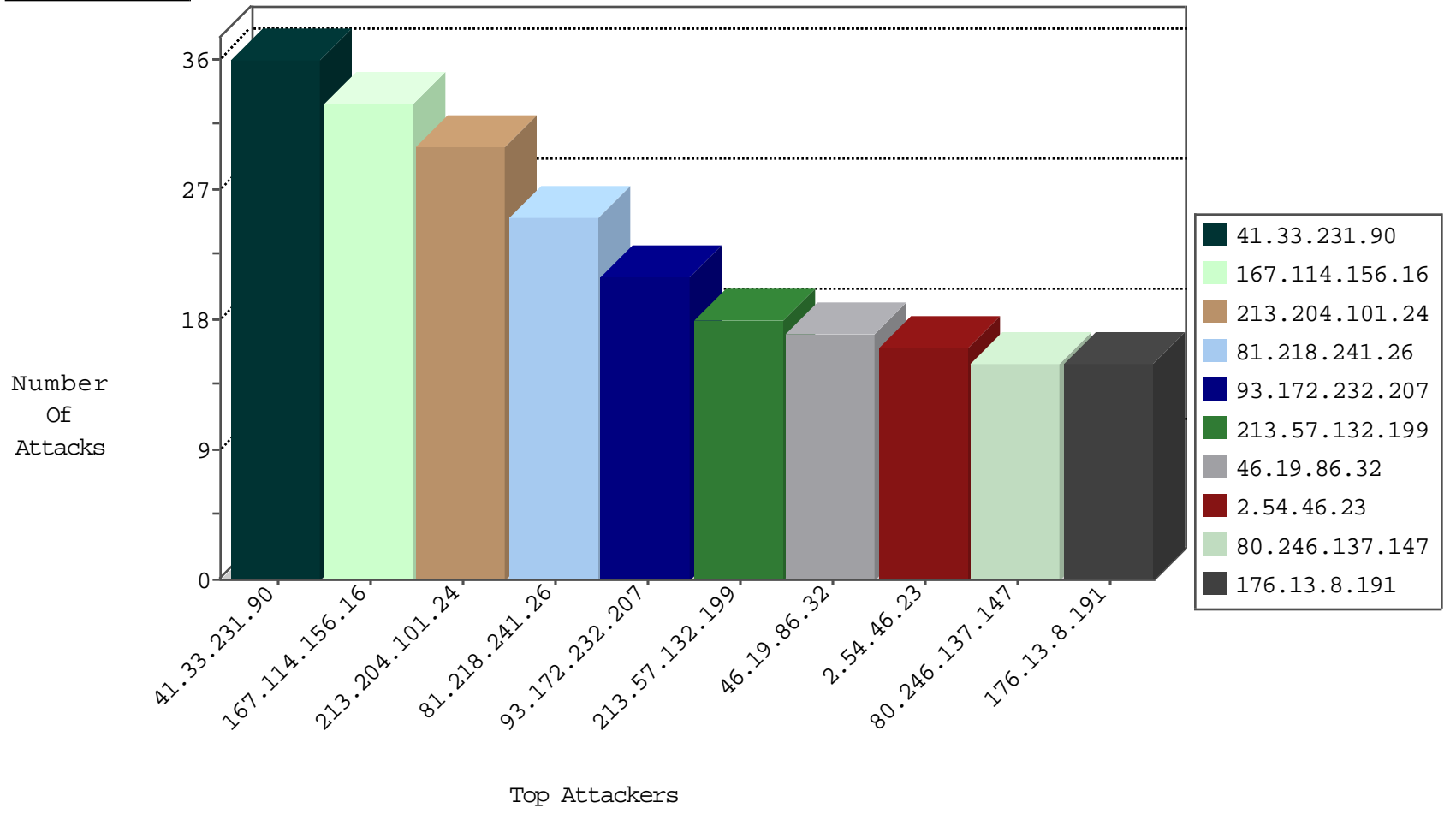
# IDF Under Attack Daily Report



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	570
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
42.116.225.2	Vietnam	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

12-29-2015-07:04:07 to 12-29-2015-08:04:07

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
151.217.178.88	147.237.77.74		law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
213.204.101.24	147.237.76.86	Lebanon	navy.idf.il	ET SCAN NMAP -sA (2)	1
146.185.30.93	147.237.76.30	United Kingdom	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
196.47.173.21	147.237.8.46	Cote D'Ivoire	e.chimuch.idf.il	ET SCAN NMAP -sS window 2048	1
131.109.15.15	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
115.182.17.13	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.77.243		mobile.idf.il	ET SCAN Potential SSH Scan	1
93.173.137.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	1
84.108.234.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
46.19.86.39	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.8.45		e.eitan.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.77.233		atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.76.42		refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
196.47.173.21	147.237.8.46	Cote D'Ivoire	e.chimuch.idf.il	ET SCAN NMAP -sS window 4096	1
131.109.15.15	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
196.47.173.21	147.237.8.46	Cote D'Ivoire	e.chimuch.idf.il	ET SCAN NMAP -f -sS	1
115.182.17.13	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 3072	1
192.115.162.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.141.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
46.62.132.118	147.237.76.39	Iran, Islamic Republic of	mobile.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.231	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.204.101.24	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
207.241.229.111	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	14
176.13.8.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.137.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
207.46.13.164	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
213.57.132.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
213.57.132.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
2.52.188.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.73.15.149	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.4.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
89.139.37.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.116.164.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.54.17.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.197.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.233.172.177	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.33.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.43.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.67.99.218	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.73.15.149	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.10.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.204.101.24	Lebanon	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.32	Israel	147.237.0.34	tikshuv.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
213.204.101.24	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.8.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.22.134.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.123.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
173.201.196.207	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.46.23	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.179.23.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.46.23	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack		reject	3
2.52.160.152	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.102.254.137	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.110.7.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.200.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.52.176.173	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.232.207	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	21
2.52.52.125	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
176.13.4.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.178.127.87	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
185.120.126.78		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
128.127.107.80	Netherlands	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.246.137.147	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.46	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.46	Block	2
2.52.43.240	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
138.134.102.16	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 138.134.102.16	Block	2
85.65.79.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	2
46.19.85.14	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
84.228.62.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.126.44		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.150.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.183.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.136.69	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.166.190.151	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
212.116.164.20	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 212.116.164.20	Block	1
89.139.37.108	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.154.145.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
180.76.15.11	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.136.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.17.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.140	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21915-ar/idfgdover.aspx	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
84.228.233.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.156.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.6.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.10.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9704-he/refuah.aspx	Block	1
66.220.146.23	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.143.172.93	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
91.227.51.14	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter id in www.aka.idf.il/iturim/asp/oneiturple.aspx	None	1
37.26.146.139	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.138	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.152.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.33.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
173.252.115.85	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.46	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/twitter.com/idfonline	Block	1
85.65.79.82	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.79.82	Block	1
46.117.65.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.163.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1