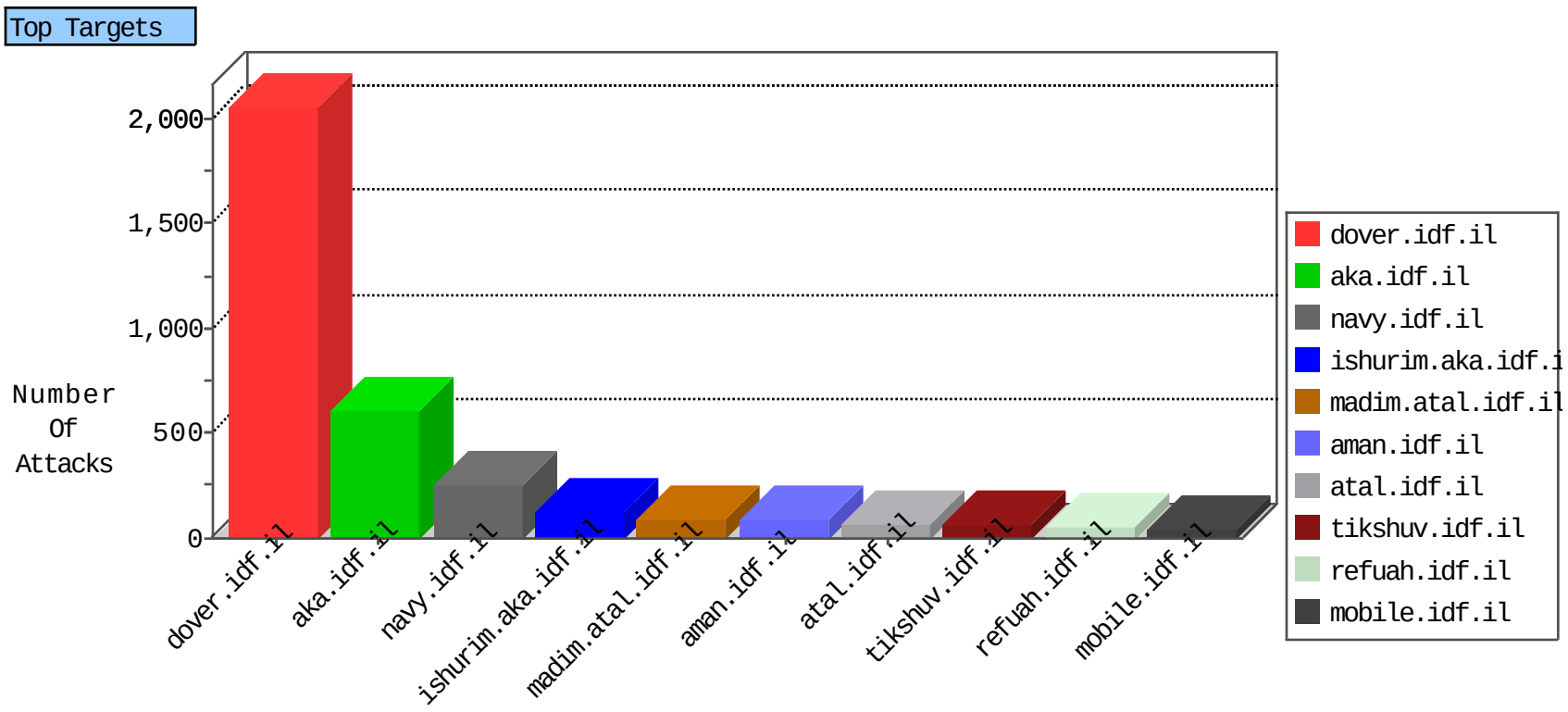
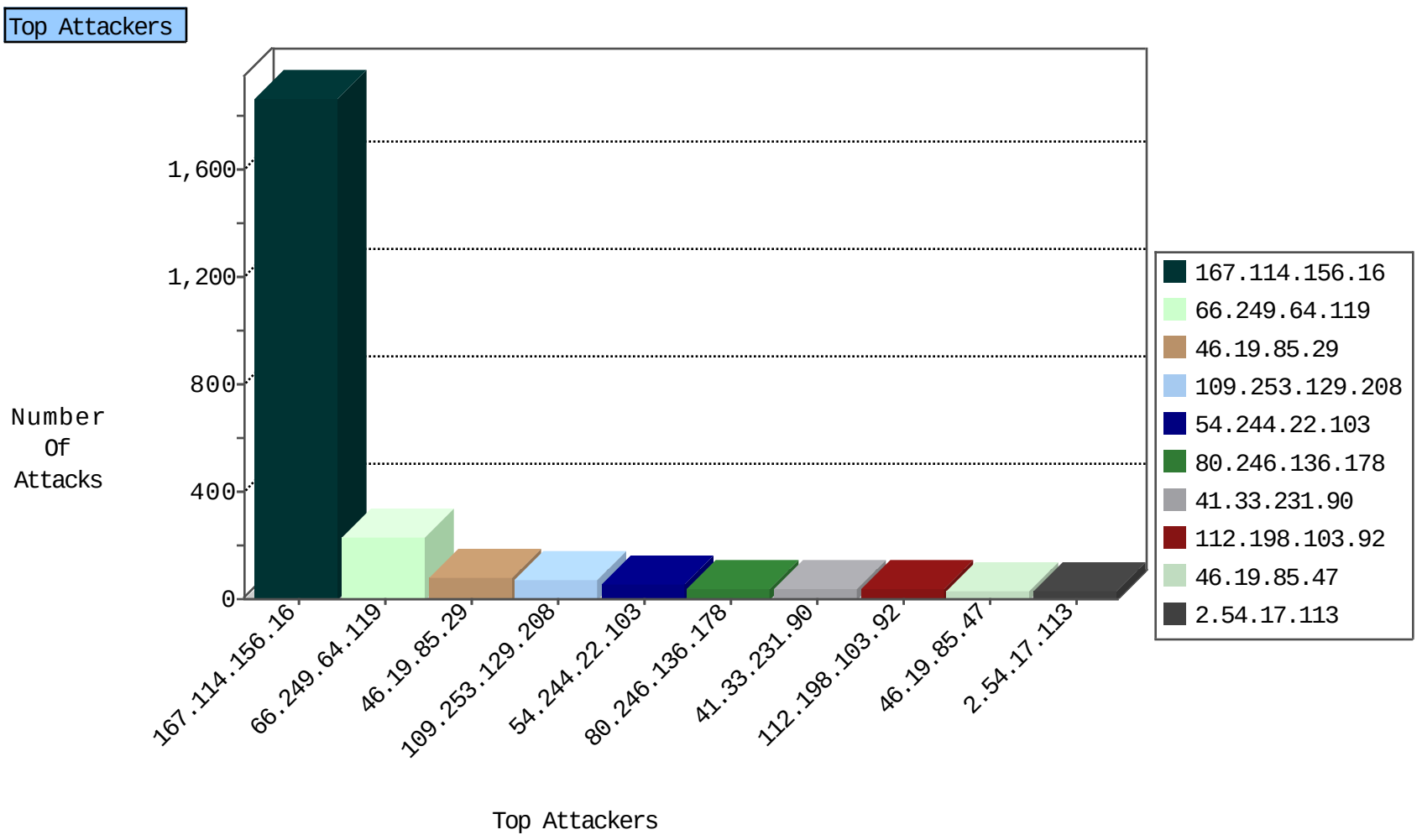
01-11-2016-17:04:03 to 01-11-2016-18:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-11-2016-17:04:03 to 01-11-2016-18:04:03

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	3216
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
185.120.125.13		147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	12
107.170.119.178	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
151.77.1.59	Italy	147.237.77.243	mobile.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
185.130.5.228		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

01-11-2016-17:04:03 to 01-11-2016-18:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.217.46.69	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

01-11-2016-17:04:03 to 01-11-2016-18:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.66.143.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
90.198.218.240	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
78.193.2.8	147.237.76.176	France	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.175.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.155	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.185.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
191.43.18.155	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
184.106.153.141	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
93.172.244.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.78.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
64.233.173.151	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.47.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
184.106.153.141	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

01-11-2016-17:04:03 to 01-11-2016-18:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.64.119	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	224
46.19.85.29	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	82
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	35
46.19.86.23	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	27
46.19.85.47	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
112.198.103.92	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	23
141.0.8.157	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
73.176.233.87	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
185.120.125.32		147.237.72.156	aman.idf.il	drop	SAM rule	drop	16
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
79.183.120.251	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
109.65.22.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.109.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
79.182.109.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.251	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.176.202.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.127.199.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
77.127.199.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.246.136.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.69.211.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.228.171.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.120.21.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.54.49.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
81.218.245.1	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
77.218.243.179	Sweden	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
80.246.136.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.241.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.17.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.246.136.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.198	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
2.54.17.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.131.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.17.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.178	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.85.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.17.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
80.246.136.178	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.142.68.80	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.116.170.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.120.125.13		147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.17.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6

01-11-2016-17:04:03 to 01-11-2016-18:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.129.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
84.111.233.31	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
212.150.192.18	Israel	147.237.77.74	law.idf.il	Parameter Type Violation prefixText in www.mag.idf.il/webservices/wscity.asmx/getcities	Block	11
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	6
109.7.69.34	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
80.246.136.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.83.4.168	Belgium	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
31.168.23.60	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.168.23.60	Block	3
79.179.199.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
109.253.138.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.199.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
77.127.199.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.28.177.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.234.172	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
81.218.195.72	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
153.1.50.213	Finland	147.237.77.176	matpash.idf.il	Distributed Parameter Type Violation on www.cogat.idf.il/938-en/cogat.aspx parameter SearchText	Block	2
46.120.21.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.21.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.64.119	Block	1
141.212.122.81	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Malformed URL	Block	1
87.69.125.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
112.198.103.92	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method nÃ _Â´ÂŠbb	Block	1
82.80.30.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.116.170.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
37.26.148.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.134.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.192	United States	147.237.76.30	himush.idf.il	Unknown Parameter v in www.chimush.atal.idf.il/ez/sitedesign/css/standard.css	None	1
2.54.159.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.238.136	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
217.132.146.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.98.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
112.198.103.92	Philippines	147.237.72.166	aka.idf.il	NULL Character in Header Name at (Â VNÂ‡Â^Â¬[[#18]]yÂ¬Ã‹iÂ¹Ã„[[#8]]sÂ“[[#0]]>Â–Ã–[[#19]][[#29]][[#11]]2Â©%Â‹Ã¡[[#16]]~}[[#1]]Ã‘[[#6]]=Ã‘	Block	1
41.207.201.129	Cote D'Ivoire	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
109.253.220.206	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl67 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.66.103.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
149.78.133.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	1
87.69.211.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.231	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
112.198.103.92	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL Â¯Ö²[[#16]][[#21]]×²qÖ±[[#2]]Â ×ª=×›w	Block	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.114.105.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.20.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-11-2016-17:04:03 to 01-11-2016-18:04:03