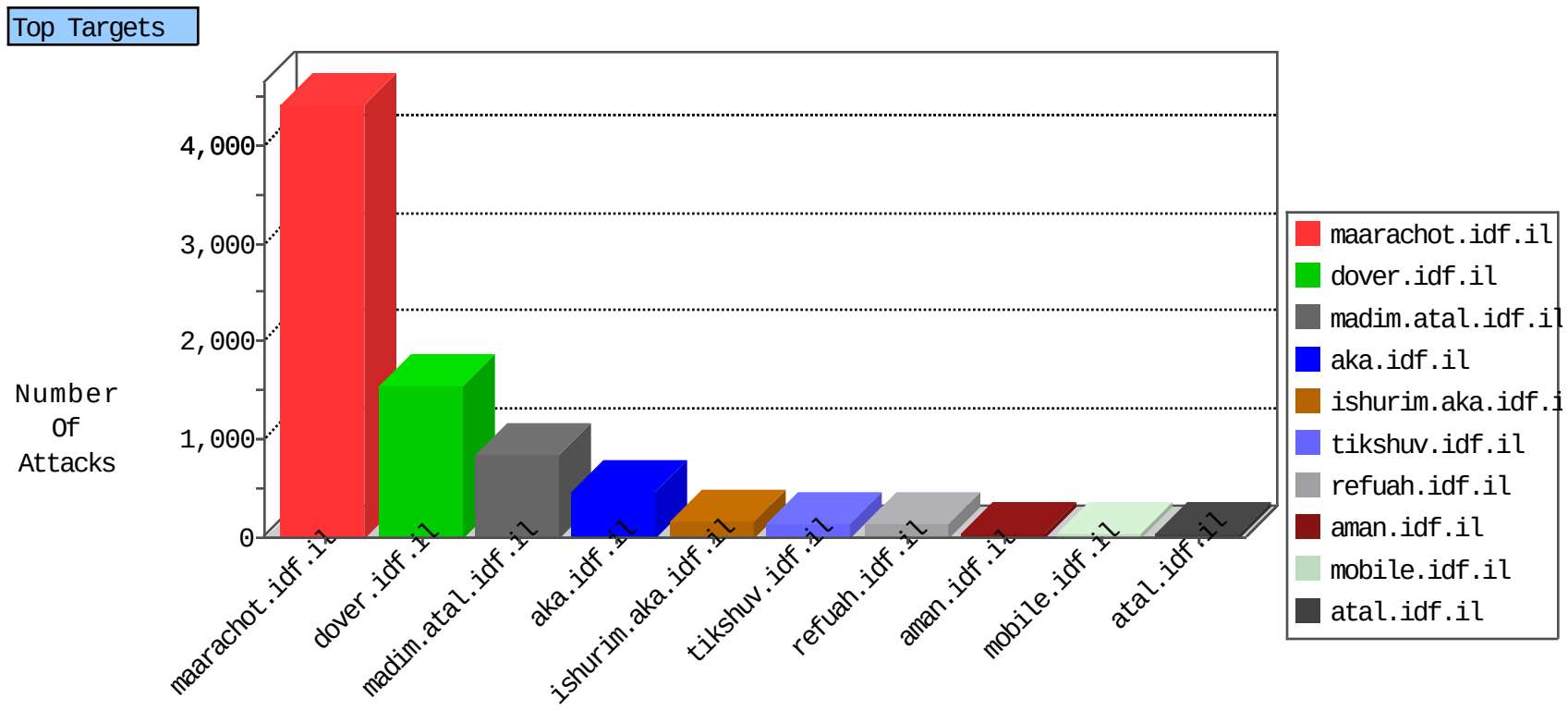
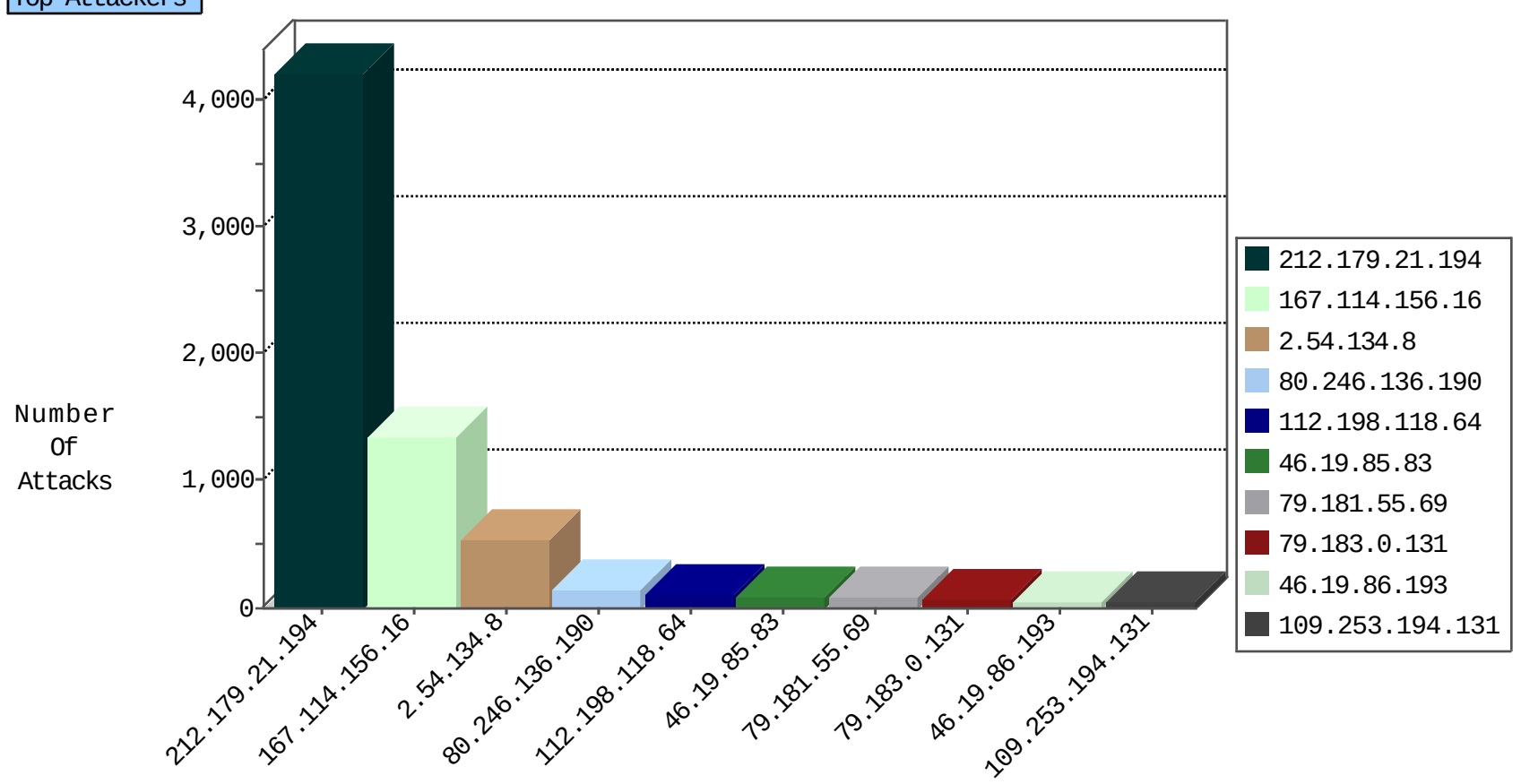
01-10-2016-11:04:02 to 01-10-2016-12:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-10-2016-11:04:02 to 01-10-2016-12:04:02

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	3126
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

01-10-2016-11:04:02 to 01-10-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	12
159.253.145.150	United States	147.237.72.166	aka.idf.il	C095: Suspicious Addresses MFA	Permit	6
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-10-2016-11:04:02 to 01-10-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
168.62.238.153	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.203	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.235.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.76.198	Moldova, Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.159.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.68.58.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-10-2016-11:04:02 to 01-10-2016-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3870
46.19.85.83	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	80
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
79.183.0.131	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	59
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
62.219.24.52	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
46.19.85.32	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
46.19.85.130	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
79.177.203.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
46.19.86.193	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
185.32.179.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.64.111.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.206.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.88.25.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.130	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
157.55.39.3	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.178.175.231	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
185.120.125.19		147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
40.77.167.69	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
147.236.34.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.135.25	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.180.116.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.32	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.228.180.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.14	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.218	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.23.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.132.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.9.185	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.141.102	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.108	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.194.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.207	Israel	147.237.77.216	dover.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
37.26.146.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.108	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.194.131	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.48.174	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.136	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
188.225.184.210	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
31.210.188.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.236	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.193	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.54.48.174	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.86.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

01-10-2016-11:04:02 to 01-10-2016-12:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.134.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	279
2.54.134.8	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.134.8	Block	139
2.54.134.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109
80.246.136.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
79.181.55.69	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.55.69	Block	76
80.246.136.190	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 80.246.136.190	Block	36
109.253.210.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
176.13.22.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.39.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
109.253.194.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
212.199.151.23	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
61.147.125.182	China	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	8
61.147.125.182	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 61.147.125.182	Block	7
176.13.14.171	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
2.52.174.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
176.13.5.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
192.117.12.65	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.mag.idf.il/508-he/patzar.aspx	Block	3
2.54.165.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 112.198.118.64	Block	3
109.253.157.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
165.225.76.55	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 165.225.76.55	Block	3
81.218.190.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	3
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 112.198.118.64	Block	3
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed URL from 112.198.118.64	Block	3
46.210.175.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.194.131	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	3
2.54.158.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 112.198.118.64	Block	3
176.13.6.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 112.198.118.64	Block	3
2.52.38.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.140.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
62.219.198.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
109.253.205.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
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	2
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 112.198.118.64	Block	2
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
134.191.232.70	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	2
87.68.166.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.39.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.28.158.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 112.198.118.64	Block	2
89.139.182.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
134.191.232.70	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/	Block	2
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 112.198.118.64	Block	2
79.181.36.80	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	2
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 112.198.118.64	Block	2

01-10-2016-11:04:02 to 01-10-2016-12:04:02