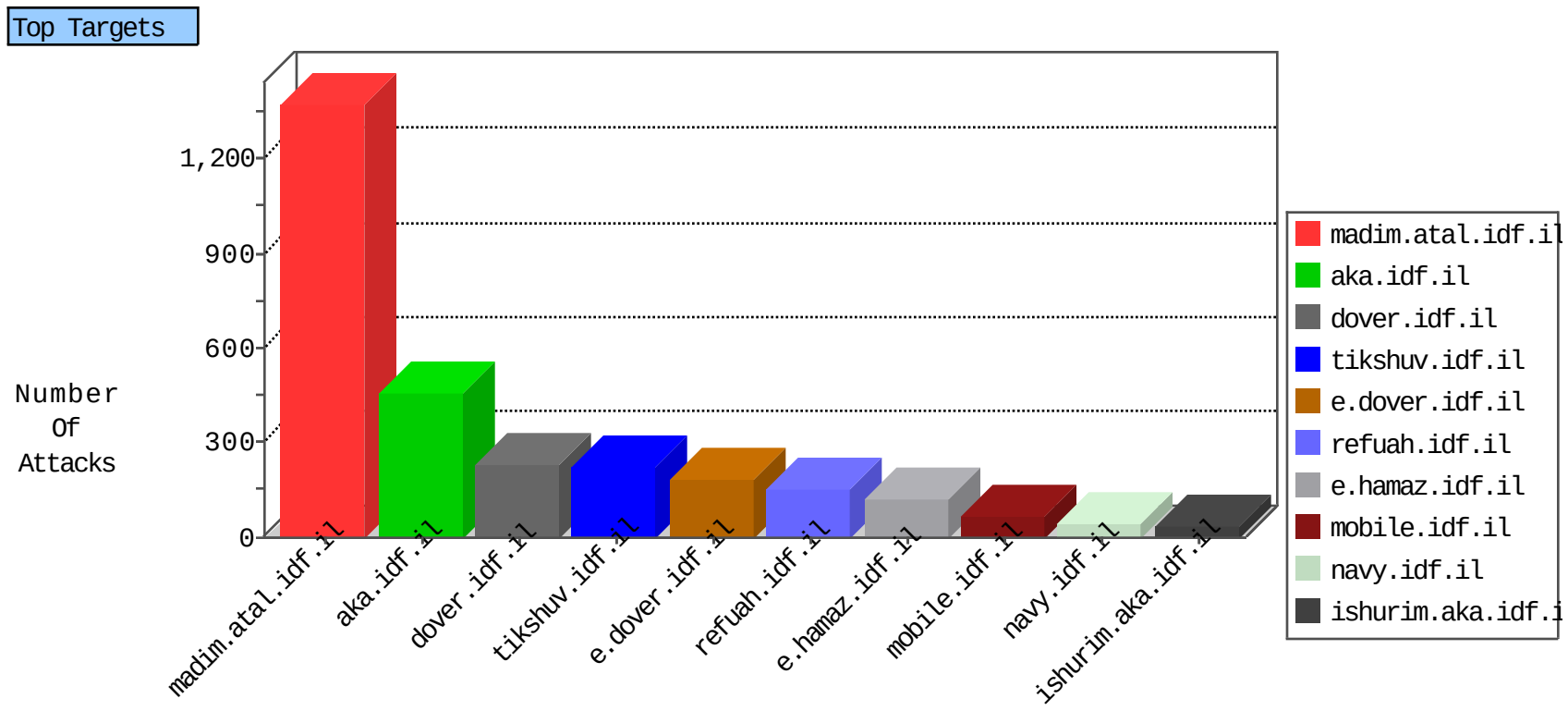
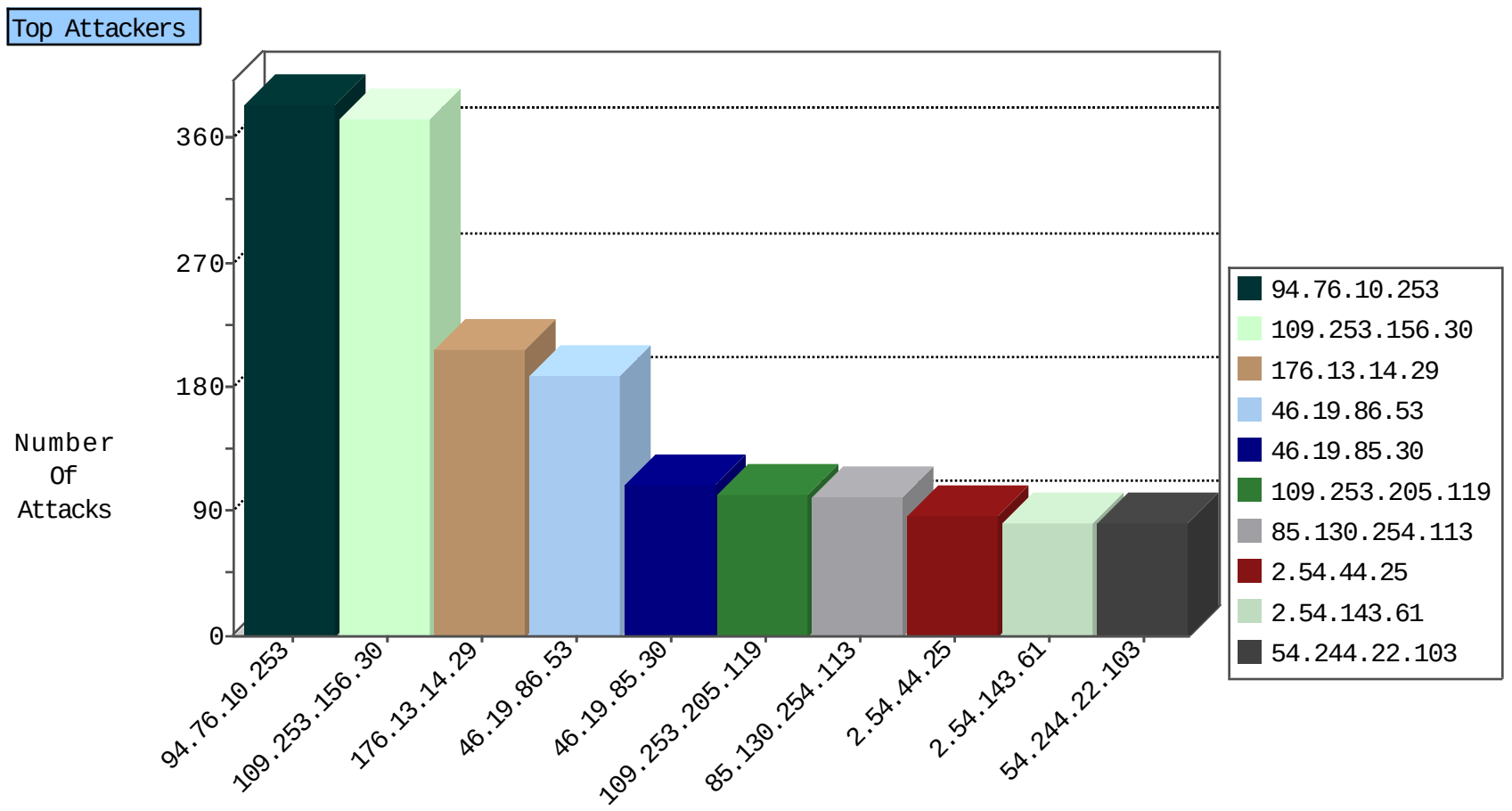
01-26-2016-11:04:04 to 01-26-2016-12:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-26-2016-11:04:04 to 01-26-2016-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.160	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1247
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	248
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
79.178.121.234	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
192.118.132.185	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
94.76.10.253	Bahrain	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
94.76.10.253	Bahrain	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
94.76.10.253	Bahrain	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
80.82.78.39	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
94.76.10.253	Bahrain	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.212	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
80.82.78.39	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
94.76.10.253	Bahrain	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.58	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1

01-26-2016-11:04:04 to 01-26-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.76.10.253	Bahrain	147.237.77.205	prisha.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	4
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
216.249.107.200	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

01-26-2016-11:04:04 to 01-26-2016-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.86.49	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
46.19.86.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.76.10.253	147.237.77.205	Bahrain	prisha.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
46.19.85.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.76.10.253	147.237.76.200	Bahrain	eitan.aka.idf.i	ET SCAN NMAP -sS window 1024	1
5.22.134.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.76.10.253	147.237.76.197	Bahrain	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.14.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.130.254.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.190.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.241.156	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	1
176.106.230.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.114.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.208.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.230.242.162	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.56.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
94.76.10.253	147.237.77.216	Bahrain	dover.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.10.253	147.237.76.202	Bahrain	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
23.227.183.203	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
94.76.10.253	147.237.76.198	Bahrain	e.yohalan.idf.i	ET SCAN NMAP -sS window 1024	1
2.54.48.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.183.201.2	147.237.76.30	Ukraine	himush.idf.il	ET SCAN Potential SSH Scan	1
85.65.24.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
191.240.136.5	147.237.77.227	Brazil	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
82.118.226.189	147.237.72.156	Bulgaria	aman.idf.il	OS-OTHER Cisco IOS HTTP configuration attempt	1
149.78.215.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.124.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.160.191.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.162.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.65.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-26-2016-11:04:04 to 01-26-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.76.10.253	Bahrain	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	182
94.76.10.253	Bahrain	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	115
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	74
85.130.254.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
85.130.254.113	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
94.76.10.253	Bahrain	147.237.77.235	sviva.idf.il	drop	First packet isn't SYN	drop	22
79.179.9.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.19.86.49	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
105.157.172.127	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
85.158.139.228	United Kingdom	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	13
94.230.86.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.160	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
192.115.177.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
85.64.241.156	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
176.13.13.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
213.57.182.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.54.45.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.149.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.2.217	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
94.76.10.253	Bahrain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.204.128.94	Netherlands	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.51.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
213.8.98.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.142.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.172.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.186.80.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.250	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.115.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.186.80.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.21.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
155.56.40.47	Germany	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.242.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.200.205.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.16.98	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.126.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

01-26-2016-11:04:04 to 01-26-2016-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.156.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	182
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	115
176.13.14.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
46.19.85.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
109.253.156.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
109.253.156.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	89
176.13.14.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	86
2.54.44.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
2.54.143.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
109.253.205.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
213.151.35.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
31.168.197.195	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
132.74.244.183	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
2.54.161.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
194.90.88.105	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
109.253.193.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
109.253.205.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	20
176.13.14.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	11
109.253.146.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
213.151.35.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
176.13.9.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
37.26.146.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.207.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.52.169.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.22.70	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	4
176.13.17.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
37.26.149.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.18.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.179.50.230	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	3
37.26.146.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.179.50.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/style/shared/	Block	3
37.26.148.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.161.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.199.57.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.167.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.147.248	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
79.178.125.165	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtID in www.refua.atal.idf.il/926-he/refuah.aspx	Block	2
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.143.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.21.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.127.77.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.182.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	2
176.13.13.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.126.236.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl42$ctl02$ctl03$ddlQuestion in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
176.13.6.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1

01-26-2016-11:04:04 to 01-26-2016-12:04:04